IBM WebSphere eXtreme Scale
Versão 8.6

Guia de Programação

Novembro de 2012

8.6 Esta edição se aplica à versão 8, liberação 6, de WebSphere eXtreme Scale e a todas as liberações e modificações subsequentes até que seja indicado de outra forma em novas edições.

Índice

Figuras

Tabelas

Sobre o *Guia de Programação*

O conjunto da documentação do WebSphere eXtreme Scale inclui três volumes que fornecem as informações necessárias para utilizar, programar e administrar o produto WebSphere eXtreme Scale.

Biblioteca do WebSphere eXtreme Scale

A biblioteca do WebSphere eXtreme Scale contém os seguintes livros:

- O *Visão Geral do Produto* contém um visualização de alto nível dos conceitos do WebSphere eXtreme Scale, incluindo cenários de caso de uso e tutoriais.
- O *Guia de Instalação* descreve como instalar topologias comuns do WebSphere eXtreme Scale.
- O *Guia de Administração* contém as informações necessárias para os administradores de sistema, incluindo como planejar implementações do aplicativo, planejar capacidade, instalar e configurar o produto, iniciar e parar servidores, monitorar o ambiente e proteger o ambiente.
- O *Guia de Programação* contém informações para desenvolvedores de aplicativos sobre como desenvolver aplicativos para o WebSphere eXtreme Scale utilizando as informações da API incluídas.

Para fazer download dos manuais, vá para a Página da Biblioteca do WebSphere eXtreme Scale.

Também é possível acessar as mesmas informações nessa biblioteca no .

Usando Manuais Off-line

Todos os manuais na biblioteca do WebSphere eXtreme Scale contêm links para o centro de informações, com a URL raiz a seguir: . Esses links levam diretamente para as informações relacionadas. No entanto, se estiver trabalhando off-line e encontrar um desses links, será possível procurar pelo título do link nos outros manuais na biblioteca. A documentação da API, o glossário e a referência de mensagens não estão disponíveis em manuais PDF.

Quem Deve Utilizar este Manual

Este manual é destinado principalmente a desenvolvedores de aplicativos.

Obtendo Atualizações para este Manual

É possível obter as atualizações para esse manual ao fazer download da versão mais recente da Página da Biblioteca do WebSphere eXtreme Scale.

Como Enviar Seus Comentários

Entre em contato com a equipe de documentação. Você localizou o que precisava? O conteúdo era exato e completo? Envie seus comentários sobre esta documentação por e-mail para wasdoc@us.ibm.com.

Capítulo 1. Tutoriais

Os tutoriais podem ser usados para ajudar a entender os cenários de uso do produto, incluindo o gerenciador, consultas e segurança da entidade.

Tutorial: Consultando uma Grade de Dados na Memória Local

Java

É possível desenvolver um ObjectGrid na memória local que pode armazenar informações de pedido para um website e usar a API do ObjectQuery para consultar a grade de dados.

Antes de Iniciar

Certifique-se de ter o arquivo `objectgrid.jar` em seu caminho de classe.

Sobre Esta Tarefa

Cada etapa no tutorial é construída na etapa anterior. Siga cada uma das etapas para construir um aplicativo Java™ Platform, Standard Edition Versão 5 ou posterior simples que usa uma grade de dados locais na memória.

Tutorial do ObjectQuery - Etapa 1

Java

Com as seguintes etapas, você poderá continuar desenvolvendo um ObjectGrid local de memória que armazena informações de pedidos para uma loja varejista on-line usando as APIs do ObjectMap. Defina um esquema para o mapa e execute uma consulta em relação ao mapa.

Procedimento

1. Crie um ObjectGrid com um esquema de mapa.

   Crie um ObjectGrid com um esquema de mapa para o mapa; em seguida, insira um objeto no cache e recupere-o posteriormente, utilizando uma consulta simples.

   OrderBean.java

   ```
   public class OrderBean implements Serializable {
       String orderNumber;
       java.util.Date date;
       String customerName;
       String itemName;
       int quantity;
       double price;
   }
   ```

2. Defina a chave principal.

   O código anterior mostra um objeto OrderBean. Este objeto implementa a interface java.io.Serializable porque todos os objetos no cache devem (por padrão) ser Serializáveis.

O atributo orderNumber é a chave principal do objeto. O programa de exemplo a seguir pode ser executado no modo independente. É necessário seguir esse tutorial em um projeto Eclipse Java que tenha o arquivo `objectgrid.jar` incluído no caminho de classe.

Application.java

```
package querytutorial.basic.step1;

import java.util.Iterator;

import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
import com.ibm.websphere.objectgrid.ObjectMap;
import com.ibm.websphere.objectgrid.Session;
import com.ibm.websphere.objectgrid.config.QueryConfig;
import com.ibm.websphere.objectgrid.config.QueryMapping;
import com.ibm.websphere.objectgrid.query.ObjectQuery;

public class Application
{

    static public void main(String [] args) throws Exception
    {
        ObjectGrid og = ObjectGridManagerFactory.getObjectGridManager().createObjectGrid();
        og.defineMap("Order");

        // Definir o esquema
        QueryConfig queryCfg = new QueryConfig();
        queryCfg.addQueryMapping(new QueryMapping("Order", OrderBean.class.getName(), "orderNumber",
QueryMapping.FIELD_ACCESS));
        og.setQueryConfig(queryCfg);

        Session s = og.getSession();
        ObjectMap orderMap = s.getMap("Order");

        s.begin();
        OrderBean o = new OrderBean();
        o.customerName = "John Smith";
        o.date = new java.util.Date(System.currentTimeMillis());
        o.itemName = "Widget";
        o.orderNumber = "1";
        o.price = 99.99;
        o.quantity = 1;
        orderMap.put(o.orderNumber, o);
        s.commit();

        s.begin();
        ObjectQuery query = s.createObjectQuery("SELECT o FROM Order o WHERE o.itemName='Widget'");
        Iterator result = query.getResultIterator();
        o = (OrderBean) result.next();
        System.out.println("Found order for customer: " + o.customerName);
        s.commit();
 // Close the session (optional in Version 7.1.1 and later) for improved performance
 s.close();
}
}
```

Esse aplicativo eXtreme Scale primeiro inicializa um ObjectGrid local com um nome gerado automaticamente. Em seguida, o aplicativo cria um BackingMap e um QueryConfig que definem qual tipo Java está associado ao mapa, o nome do campo que é a chave principal para o mapa e como acessar os dados no objeto. A seguir, você obtém uma Sessão para adquirir a instância do ObjectMap e inserir um objeto OrderBean no mapa em uma transação.

Depois que os dados forem confirmados no cache, será possível usar o ObjectQuery para localizar o OrderBean usando qualquer um dos campos persistentes na classe. Campos persistentes são aqueles que não possuem o modificador temporário. Como nenhum índice foi definido no BackingMap, o ObjectQuery deverá varrer cada objeto no mapa usando o reflexo Java.

O que Fazer Depois

O “Tutorial do ObjectQuery - Etapa 2” demonstra como um índice pode ser usado para otimizar a consulta.

Tutorial do ObjectQuery - Etapa 2

Java

Nas seguintes etapas, você continuará criando um ObjectGrid com um mapa e um índice, junto com um esquema para o mapa. Em seguida, você poderá inserir um objeto no cache e, mais tarde, recuperá-lo utilizando uma consulta simples.

Antes de Iniciar

Certifique-se de ter concluído o "Tutorial do ObjectQuery - Etapa 1" na página 1 antes de continuar com esta etapa do tutorial.

Procedimento

Esquema e índice

Application.java

```
// Create an index
    HashIndex idx= new HashIndex();
    idx.setName("theItemName");
    idx.setAttributeName("itemName");
    idx.setRangeIndex(true);
    idx.setFieldAccessAttribute(true);
    orderBMap.addMapIndexPlugin(idx);
}
```

O índice deve ser uma instância com.ibm.websphere.objectgrid.plugins.index.HashIndex com as seguintes configurações:

- O Nome é arbitrário, mas deve ser exclusivo para um BackingMap fornecido.
- O AttributeName é o nome do campo ou propriedade do bean que o mecanismo de indexação utiliza para examinar a classe. Neste caso, este é o nome do campo para o qual você criará um índice.
- RangeIndex deve ser sempre verdadeiro.
- FieldAccessAttribute deve corresponder ao conjunto de valores no objeto QueryMapping quando o esquema de consulta foi criado. Nesse caso, o objeto Java é acessado usando os campos diretamente.

Quando uma consulta executa esses filtros no campo itemName, o mecanismo de consulta automaticamente usa o índice definido. Usar o índice permite que a consulta seja executada muito mais rapidamente e uma varredura de mapa não é necessária. A próxima etapa demonstra como um índice pode ser utilizado para otimizar a consulta.
Próxima etapa

Tutorial do ObjectQuery - Etapa 3

Java

Na etapa a seguir, você criará um ObjectGrid com dois mapas e um esquema para os mapas com um relacionamento e, em seguida, inserirá os objetos no cache e posteriormente irá recuperá-los utilizando uma consulta simples.

Antes de Iniciar

Certifique-se de ter concluído o "Tutorial do ObjectQuery - Etapa 2" na página 2 antes de continuar com esta etapa.

Sobre Esta Tarefa

Neste exemplo, há dois mapas, cada um com um tipo único Java mapeado para ele. O mapa Order possui objetos OrderBean e o mapa Customer contém objetos CustomerBean.

Procedimento

Defina mapas com um relacionamento.

OrderBean.java

```
public class OrderBean implements Serializable {
    String orderNumber;
    java.util.Date date;
    String customerId;
    String itemName;
    int quantity;
    double price;
}
```

O OrderBean não contém mais o customerName. Ao invés disso, ele contém o customerId, que é a chave principal para o objeto CustomerBean e o mapa Customer.

CustomerBean.java

```
public class CustomerBean implements Serializable{
    private static final long serialVersionUID = 1L;
    String id;
    String firstName;
    String surname;
    String address;
    String phoneNumber;
}
```

O relacionamento entre os dois tipos ou Mapas é:

Application.java

```
public class Application
{

    static public void main(String [] args)
        throws Exception
    {
        ObjectGrid og = ObjectGridManagerFactory.getObjectGridManager().createObjectGrid();
        og.defineMap("Order");
        og.defineMap("Customer");

        // Definir o esquema
        QueryConfig queryCfg = new QueryConfig();
        queryCfg.addQueryMapping(new QueryMapping(
            "Order", OrderBean.class.getName(), "orderNumber",
QueryMapping.FIELD_ACCESS));
        queryCfg.addQueryMapping(new QueryMapping(
            "Customer", CustomerBean.class.getName(), "id",
QueryMapping.FIELD_ACCESS));
        queryCfg.addQueryRelationship(new QueryRelationship(
             OrderBean.class.getName(), CustomerBean.class.getName(), "customerId", null));
        og.setQueryConfig(queryCfg);

        Session s = og.getSession();
        ObjectMap orderMap = s.getMap("Order");
        ObjectMap custMap = s.getMap("Customer");

        s.begin();
        CustomerBean cust = new CustomerBean();
        cust.address = "Main Street";
        cust.firstName = "John";
        cust.surname = "Smith";
        cust.id = "C001";
        cust.phoneNumber = "5555551212";
```

```
        custMap.insert(cust.id, cust);

        OrderBean o = new OrderBean();
        o.customerId = cust.id;
        o.date = new java.util.Date();
        o.itemName = "Widget";
        o.orderNumber = "1";
        o.price = 99.99;
        o.quantity = 1;
        orderMap.insert(o.orderNumber, o);
        s.commit();

        s.begin();
        ObjectQuery query = s.createObjectQuery(
            "SELECT c FROM Order o JOIN o.customerId as c WHERE o.itemName='Widget'");
        Iterator result = query.getResultIterator();
        cust = (CustomerBean) result.next();
        System.out.println("Found order for customer: " + cust.firstName + " " + cust.surname);
 s.commit();
   // Close the session (optional in Version 7.1.1 and later) for improved performance
 s.close();
    }
}
```

O XML equivalente no descritor de implementação do ObjectGrid é:

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
xmlns="http://ibm.com/ws/objectgrid/config">
  <objectGrids>
    <objectGrid name="CompanyGrid">
      <backingMap name="Order"/>
      <backingMap name="Customer"/>

      <querySchema>
         <mapSchemas>
           <mapSchema
             mapName="Order"
             valueClass="com.mycompany.OrderBean"
             primaryKeyField="orderNumber"
             accessType="FIELD"/>
           <mapSchema
             mapName="Customer"
             valueClass="com.mycompany.CustomerBean"
             primaryKeyField="id"
             accessType="FIELD"/>
         </mapSchemas>
         <relationships>
           <relationship
             source="com.mycompany.OrderBean"
             target="com.mycompany.CustomerBean"
             relationField="customerId"/>
         </relationships>
      </querySchema>
    </objectGrid>
  </objectGrids>
</objectGridConfig>
```

O que Fazer Depois

O “Tutorial do ObjectQuery - Etapa 4” expande a etapa atual ao incluir um campo, objetos de acesso da propriedade e relacionamentos adicionais.

Tutorial do ObjectQuery - Etapa 4

Java

A etapa a seguir mostra como criar um ObjectGrid com quatro mapas e um esquema para os mapas. Alguns dos mapas mantêm um relacionamento um-para-um (unidirecional) e um relacionamento um-para-muitos (bidirecional).

Após criar os mapas, é possível então executar o programa de amostra `Application.java` para inserir objetos no cache e executar consultas para recuperar esses objetos.

Antes de Iniciar

Certifique-se de ter concluído o "Tutorial do ObjectQuery - Etapa 3" na página 3 antes de continuar com a etapa atual.

Sobre Esta Tarefa

Será solicitado que você crie quatro classes JAVA. Elas serão os mapas para o ObjectGrid:

- OrderBean.java
- OrderLineBean.java
- CustomerBean.java
- ItemBean.java

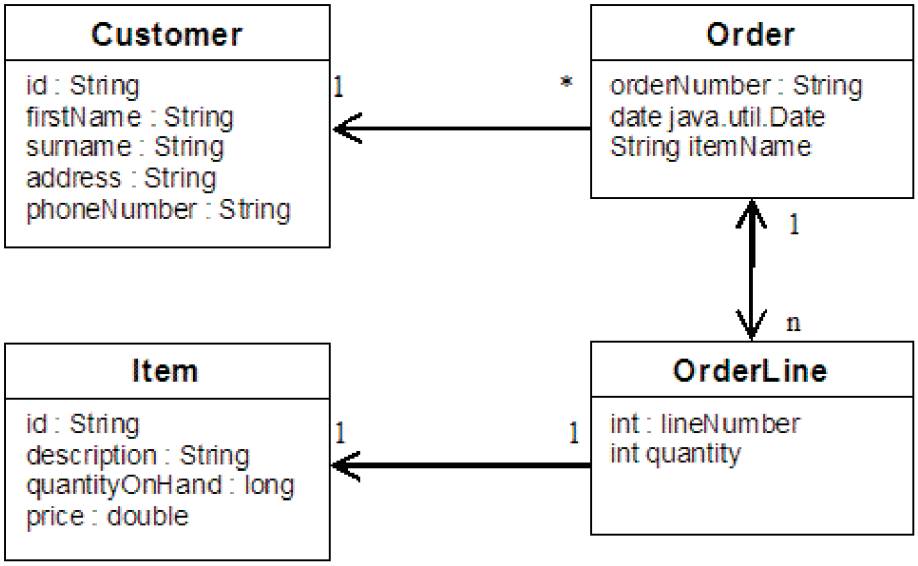


Figura 1. Esquema de Ordem. Um Esquema de Ordem tem um relacionamento um-para-um com o Cliente e um relacionamento um-para-muitos com o OrderLine. O mapa OrderLine tem um relacionamento um-para-um com o Item e inclui a quantidade pedida.

Após criar essas classes JAVA com esses relacionamentos, é possível executar o programa de amostra `Application.java`. Esse programa permite que você insira objetos no cache e os recupere usando várias consultas.

Procedimento

1. Crie as classes JAVA a seguir:

   `OrderBean.java`

   ```
   public class OrderBean implements Serializable {
      String orderNumber;
      java.util.Date date;
   ```

```
   String customerId;
   String itemName;
   List<Integer> orderLines;
}
```

OrderLineBean.java

```
public class OrderLineBean implements Serializable {
  int lineNumber;
  int quantity;
  String orderNumber;
  String itemId;
}
```

CustomerBean.java

```
public class CustomerBean implements Serializable{
  String id;
  String firstName;
  String surname;
  String address;
  String phoneNumber;
}
```

ItemBean.java

```
public class ItemBean implements Serializable {
  String id;
  String description;
  long quantityOnHand;
  double price;
}
```

2. Após criar as classes, é possível executar a amostra `Application.java`:

Application.java

```
  public class Application static public void main(String [] args)throws Exception
        // Configure programatically
     objectGrid og = ObjectGridManagerFactory.getObjectGridManager().createObjectGrid();
        og.defineMap("Order");
        og.defineMap("Customer");
        og.defineMap("OrderLine");
        og.defineMap("Item");

        // Definir o esquema
        QueryConfig queryCfg = new QueryConfig();
        queryCfg.addQueryMapping(new QueryMapping("Order", OrderBean.class.getName(), "orderNumber",
QueryMapping.FIELD_ACCESS));
        queryCfg.addQueryMapping(new QueryMapping("Customer", CustomerBean.class.getName(), "id",
QueryMapping.FIELD_ACCESS));
        queryCfg.addQueryMapping(new QueryMapping("OrderLine", OrderLineBean.class.getName(), "lineNumber",
QueryMapping.FIELD_ACCESS));
        queryCfg.addQueryMapping(new QueryMapping("Item", ItemBean.class.getName(), "id",
QueryMapping.FIELD_ACCESS));
        queryCfg.addQueryRelationship(new QueryRelationship(OrderBean.class.getName(), CustomerBean.class.getName(), "customerId", null));
        queryCfg.addQueryRelationship(new QueryRelationship(OrderBean.class.getName(), OrderLineBean.class.getName(),
    "orderLines", "lineNumber"));
        queryCfg.addQueryRelationship(new QueryRelationship(OrderLineBean.class.getName(), ItemBean.class.getName(), "itemId", null));
        og.setQueryConfig(queryCfg);

        // Get session and maps;
        Session s = og.getSession();
        ObjectMap orderMap = s.getMap("Order");
        ObjectMap custMap = s.getMap("Customer");
        ObjectMap itemMap = s.getMap("Item");
        ObjectMap orderLineMap = s.getMap("OrderLine");

        // Add data
        s.begin();
        CustomerBean aCustomer = new CustomerBean();
        aCustomer.address = "Main Street";
        aCustomer.firstName = "John";
        aCustomer.surname = "Smith";
        aCustomer.id = "C001";
        aCustomer.phoneNumber = "5555551212";
        custMap.insert(aCustomer.id, aCustomer);

        // Insert an order with a reference to the customer, but without any OrderLines yet.
        // Because we are using CopyMode.COPY_ON_READ_AND_COMMIT, the
        // insert won't be copied into the backing map until commit time, so
```

```
        // the reference is still good.

    OrderBean anOrder = new OrderBean();
    anOrder.customerId = aCustomer.id;
    anOrder.date = new java.util.Date();
    anOrder.itemName = "Widget";
    anOrder.orderNumber = "1";
    anOrder.orderLines = new ArrayList();
    orderMap.insert(anOrder.orderNumber, anOrder);

        ItemBean anItem = new ItemBean();
        anItem.id = "AC0001";
        anItem.description = "Description of widget";
        anItem.quantityOnHand = 100;
        anItem.price = 1000.0;
        itemMap.insert(anItem.id, anItem);

    // Create the OrderLines and add the reference to the Order
        OrderLineBean anOrderLine = new OrderLineBean();
        anOrderLine.lineNumber = 99;
        anOrderLine.itemId = anItem.id;
        anOrderLine.orderNumber = anOrder.orderNumber;
        anOrderLine.quantity = 500;
        orderLineMap.insert(anOrderLine.lineNumber, anOrderLine);
        anOrder.orderLines.add(Integer.valueOf(anOrderLine.lineNumber));

    anOrderLine = new OrderLineBean();
        anOrderLine.lineNumber = 100;
        anOrderLine.itemId = anItem.id;
        anOrderLine.orderNumber = anOrder.orderNumber;
        anOrderLine.quantity = 501;
        orderLineMap.insert(anOrderLine.lineNumber, anOrderLine);
        anOrder.orderLines.add(Integer.valueOf(anOrderLine.lineNumber));
        s.commit();

    s.begin();
        // Find all customers who have ordered a specific item.
        ObjectQuery query = s.createObjectQuery("SELECT c FROM Order o JOIN o.customerId as c WHERE o.itemName='Widget'");
        Iterator result = query.getResultIterator();
        aCustomer = (CustomerBean) result.next();
        System.out.println("Found order for customer: " + aCustomer.firstName + " " + aCustomer.surname);
        s.commit();

    s.begin();
        // Find all OrderLines for customer C001.
        // The query joins are expressed on the foreign keys.
        query = s.createObjectQuery("SELECT ol FROM Order o JOIN o.customerId as c JOIN o.orderLines as ol WHERE c.id='C001'");
        result = query.getResultIterator();
        System.out.println("Found OrderLines:");
        while(result.hasNext()) {
            anOrderLine = (OrderLineBean) result.next();
            System.out.println(anOrderLine.lineNumber + ", qty=" + anOrderLine.quantity);
        }
 // Close the session (optional in Version 7.1.1 and later) for improved performance
 s.close();
   }
}
```

3. Utilizar a configuração XML abaixo (no descritor de implementação ObjectGrid) é equivalente à abordagem programática acima.

```
<?xml version="1.0" encoding="UTF-8"?><objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://ibm.com/ws/objectgrid/config
../objectGrid.xsd"xmlns="http://ibm.com/ws/objectgrid/config">
<objectGrids>
  <objectGrid name="CompanyGrid">
  <backingMap name="Order"/>
  <backingMap name="Customer"/>
  <backingMap name="OrderLine" />
  <backingMap name="Item" />

<querySchema>
 <mapSchemas>
  <mapSchema
  mapName="Order"
  valueClass="com.mycompany.OrderBean"
  primaryKeyField="orderNumber"
  accessType="FIELD"/>
  <mapSchema
  mapName="Customer"
  valueClass="com.mycompany.CustomerBean"
  primaryKeyField="id"
  accessType="FIELD"/>
  <mapSchema
  mapName="OrderLine"
  valueClass="com.mycompany.OrderLineBean"
  primaryKeyField="
  lineNumber"
  accessType="FIELD"/>
  <mapSchema
```

```
  mapName="Item"
  valueClass="com.mycompany.ItemBean"
  primaryKeyField="id"
  accessType="FIELD"/>
  </mapSchemas>

<relationships>
 <relationship
  source="com.mycompany.OrderBean"
  target="com.mycompany.CustomerBean"
  relationField="customerId"/>
 <relationship
  source="com.mycompany.OrderBean"
  target="com.mycompany.OrderLineBean"
  relationField="orderLines"
  invRelationField="lineNumber"/>
 <relationship
  source="com.mycompany.OrderLineBean"
  target="com.mycompany.ItemBean"
  relationField="itemId"/>
    </relationships>
   </querySchema>
  </objectGrid>
 </objectGrids>
</objectGridConfig>
```

Tutorial: Armazenando Informações de Pedido nas Entidades

Java

Este tutorial do gerenciador de entidade mostra como utilizar o WebSphere eXtreme Scale para armazenar informações de pedido em um Web site. É possível criar um aplicativo Java Platform, Standard Edition 5 simples que utiliza um eXtreme Scale local e de memória. As entidades utilizam anotações e genéricos do Java SE 5.

Antes de Iniciar

Certifique-se de atender aos seguintes requisitos antes de começar o tutorial:

- É necessário ter o Java SE 5.
- É necessário ter o arquivo `objectgrid.jar` em seu caminho de classe.

Conceitos relacionados:

"Objetos de Armazenamento em Cache sem Relacionamentos Envolvidos (API ObjectMap)" na página 372
Os ObjectMaps são como Mapas Java que permitem que os dados sejam armazenados como pares chave-valor. Os ObjectMaps apresentam uma abordagem simples e intuitiva para o aplicativo que armazenará os dados. Um ObjectMap é ideal para o armazenamento em cache de objetos que não tenham nenhum relacionamento envolvido. Se os relacionamentos de objetos estiverem envolvidos, então você deve usar a API EntityManager.

Java "Ajustando o Desempenho da Interface EntityManager" na página 760
A interface EntityManager separa aplicativos do estado de suspensão no armazenamento de dados da grade do servidor.

Java "Objetos de Armazenamento em Cache e seus Relacionamentos (API EntityManager)" na página 388
A maioria dos produtos de cache utiliza APIs baseadas em mapa para armazenar dados como pares de chave-valor. A API ObjectMap e o cache dinâmico no WebSphere Application Server, entre outros, usam essa abordagem. Entretanto, APIs baseadas em mapas têm limitações. A API EntityManager simplifica a interação com a grade de dados ao fornecer uma maneira fácil de declarar e interagir com um gráfico complexo de objetos relacionados.

Java "Entity Manager em um Ambiente Distribuído" na página 401
É possível usar a API EntityManager com um ObjectGrid local ou em um ambiente distribuído do eXtreme Scale . A principal diferença é como você se conecta a esse ambiente remoto. Após você estabelecer uma conexão, não existe diferença entre o uso de um objeto Session ou uma API do EntityManager.

Java "Interagindo com EntityManager" na página 405
Geralmente os aplicativos primeiro obtêm uma referência do ObjectGrid e, depois, uma Sessão dessa referência para cada encadeamento. As sessões não podem ser compartilhadas entre encadeamentos. Um método extra em Session, o método getEntityManager, está disponível. Este método retorna uma referência para um gerenciador de entidades para uso para este encadeamento. A interface de EntityManager pode substituir as interfaces de Session e ObjectMap para todos os aplicativos. É possível utilizar essas APIs de EntityManager se o cliente tiver acesso às classes de entidade definidas.

Java "Suporte ao Plano de Carregamento do EntityManager" na página 417
Um FetchPlan é a estratégia que o gerenciador de entidade usa para recuperar objetos associados se o aplicativo precisar acessar relacionamentos.

Java "Filas de Consulta da Entidade" na página 421
Filas de consulte permitem que aplicativos criem uma fila qualificada por uma consulta no lado do servidor ou eXtreme Scale local sobre uma entidade. As entidades do resultado da consulta são armazenadas nesta fila. Atualmente, a fila de consulta é suportada apenas em um mapa que está utilizando a estratégia de bloqueio pessimista.

Referências relacionadas:

Java "Agente de Instrumentação de Desempenho da Entidade" na página 762
É possível melhorar o desempenho de entidades de acesso ao campo ativando o agente de instrumentação do WebSphere eXtreme Scale ao usar o Java Development Kit (JDK) Versão 6 ou posterior.

Java "Definindo um Esquema de Entidade" na página 391
Um ObjectGrid pode ter inúmeros esquemas de entidade lógicos. As entidades são definidas usando as classes Java anotadas, o XML ou uma combinação de classes

XML e Java. Entidades definidas são registradas com um servidor eXtreme Scale e ligadas a BackingMaps, índices e outros plug-ins.

Java "Listeners de Entidade e Métodos de Retorno de Chamada" na página 408
Os aplicativos podem ser notificados quando o estado de uma entidade é alterado de estado para estado. Dois mecanismos de retorno de chamada existem para os eventos de mudança de estado: os métodos de retorno de chamada do ciclo de vida que são definidos em uma classe de entidade e são chamados sempre que o estado da entidade é alterado e os listeners de entidade, que são mais gerais porque o listener da entidade pode ser registrado em várias entidades.

Java "Exemplos do Listener de Entidade" na página 414
É possível gravar EntityListeners com base em seus requisitos. Veja a seguir vários scripts de exemplo.

Java "Interface EntityTransaction" na página 426
É possível utilizar a interface EntityTransaction para demarcar transações.

Informações relacionadas:

Documentação da API

"Tutorial de Introdução - Lição 2.1: Criando um Aplicativo de Cliente Java" na página 238
Para inserir, excluir, atualizar e recuperar dados de sua grade de dados, você deverá gravar um aplicativo cliente. A amostra de introdução inclui um aplicativo de cliente Java que pode ser usado para aprender sobre como criar seu próprio aplicativo cliente.

Tutorial do Entity Manager: Criando uma Classe de Entidade

Java

Crie um ObjectGrid local com uma entidade criando uma classe Entity, registrando o tipo de entidade e armazenando uma instância da entidade no cache.

Procedimento

1. Crie o objeto Order. Para identificar o objeto como uma entidade ObjectGrid, inclua a anotação @Entity. Ao incluir esta anotação, todos os atributos serializáveis no objeto são automaticamente persistidos no eXtreme Scale, a menos que você utilize anotações nos atributos para substituí-los. O atributo **orderNumber** é anotado com `@Id` para indicar que este atributo é a chave primária. A seguir, está um exemplo de um objeto Order:

   Order.java

   ```
   @Entity
   public class Order {
       @Id String orderNumber;
       Date date;
       String customerName;
       String itemName;
       int quantity;
       double price;
   }
   ```

2. Execute o aplicativo eXtreme Scale Hello World para demonstrar as operações entity. O programa de exemplo a seguir pode ser emitido no modo independente para demonstrar as operações entity. Use esse programa em um projeto Eclipse Java que tenha o arquivo `objectgrid.jar` incluído no caminho de classe. A seguir, está um exemplo de um aplicativo Hello world simples que utiliza o eXtreme Scale:

Application.java

```
package emtutorial.basic.step1;

import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
import com.ibm.websphere.objectgrid.Session;
import com.ibm.websphere.objectgrid.em.EntityManager;

public class Application
{

    static public void main(String [] args)
        throws Exception
    {
        ObjectGrid og =
    ObjectGridManagerFactory.getObjectGridManager().createObjectGrid();
        og.registerEntities(new Class[] {Order.class});

        Session s = og.getSession();
        EntityManager em = s.getEntityManager();

        em.getTransaction().begin();

        Order o = new Order();
        o.customerName = "John Smith";
        o.date = new java.util.Date(System.currentTimeMillis());
        o.itemName = "Widget";
        o.orderNumber = "1";
        o.price = 99.99;
        o.quantity = 1;

        em.persist(o);
        em.getTransaction().commit();

        em.getTransaction().begin();
        o = (Order)em.find(Order.class, "1");
        System.out.println("Found order for customer: " + o.customerName);
        em.getTransaction().commit();
    }
}
```

Este aplicativo de exemplo executa as seguintes operações:

a. Inicializa um eXtreme Scale local com um nome gerado automaticamente.
b. Registra as classes entity com o aplicativo utilizando a API do registerEntities, embora utilizar a API do registerEntities não seja sempre necessário.
c. Recupera um objeto Session e uma referência para o entity manager para Session.
d. Associa cada objeto Session do eXtreme Scale com um EntityManager e EntityTransaction únicos. O EntityManager agora é utilizado.
e. O método registerEntities cria um objeto BackingMap que é chamado Order e associa os metadados para o objeto Order com o objeto BackingMap. Esses metadados incluem os atributos chave e não-chave, juntamente com os tipos e nomes de atributo.
f. Uma transação inicia e cria uma instância Order. A transação é preenchida com alguns valores. A transação é, então, persistida usando o método EntityManager.persist, que identifica a entidade como aguardando para ser incluída no mapa associado.
g. A transação é, então, confirmada, e a entidade é incluída na instância de ObjectMap.
h. Uma outra transação é feita e o objeto Order é recuperado usando a chave 1. O cast de tipo no método EntityManager.find é necessário. A capacidade do Java SE 5 não é usada para assegurar que o arquivo `objectgrid.jar` funciona em um Java SE Versão 5 e Java Virtual Machine posterior.

Tutorial do Entity Manager: Formando Relacionamentos de Entidades

Java

Crie um relacionamento simples entre entidades criando duas classes de entidades com um relacionamento, registrando as entidades com o ObjectGrid e armazenamento as instâncias da entidade no cache.

Procedimento

1. Crie a entidade customer, que é usada para armazenar detalhes do cliente independentemente do objeto Order. Um exemplo da entidade customer é apresentado a seguir:

   Customer.java

   ```
   @Entity
   public class Customer
   {
       @Id String id;
       String firstName;
       String surname;
       String address;
       String phoneNumber;
   }
   ```

   Esta classe inclui informações sobre o cliente, tais como nome, endereço e número de telefone.

2. Crie o objeto Order, que é semelhante ao objeto Order no tópico do "Tutorial do Entity Manager: Criando uma Classe de Entidade" na página 11. A seguir, está um exemplo do objeto order:

   Order.java

   ```
   @Entity
   public class Order {
       @Id String orderNumber;
       Date date;
       @ManyToOne(cascade=CascadeType.PERSIST) Customer customer;
       String itemName;
       int quantity;
       double price;
   }
   ```

   Neste exemplo, uma referência para um objeto Customer substitui o atributo customerName. A referência possui uma anotação que indica uma relação muitos-para-um. Um relacionamento muitos-para-um indica que cada pedido possui um cliente, mas vários pedidos podem fazer referência ao mesmo cliente. O modificador de anotação em cascata indica que, se o gerenciador de entidade persistir o objeto Order, ele também deverá persistir o objeto Customer. Se você decidir não definir a opção de persistência em cascata, que é a opção padrão, deve persistir manualmente o objeto Customer com o objeto Order.

3. Utilizando as entidades, defina os mapas para a instância do ObjectGrid. Cada mapa é definido para uma entidade específica e uma entidade é denominada Order e a outra é denominada Customer. O aplicativo de exemplo a seguir ilustra como armazenar e recuperar um pedido do cliente:

   Application.java

   ```
   public class Application
   {
       static public void main(String [] args)
           throws Exception
       {
           ObjectGrid og =
        ObjectGridManagerFactory.getObjectGridManager().createObjectGrid();
           og.registerEntities(new Class[] {Order.class});

           Session s = og.getSession();
           EntityManager em = s.getEntityManager();
   ```

```
        em.getTransaction().begin();

        Customer cust = new Customer();
        cust.address = "Main Street";
        cust.firstName = "John";
        cust.surname = "Smith";
        cust.id = "C001";
        cust.phoneNumber = "5555551212";

        Order o = new Order();
        o.customer = cust;
        o.date = new java.util.Date();
        o.itemName = "Widget";
        o.orderNumber = "1";
        o.price = 99.99;
        o.quantity = 1;

        em.persist(o);
        em.getTransaction().commit();

        em.getTransaction().begin();
        o = (Order)em.find(Order.class, "1");
        System.out.println("Found order for customer: "
    + o.customer.firstName + " " + o.customer.surname);
        em.getTransaction().commit();
 // Close the session (optional in Version 7.1.1 and later) for improved performance
 s.close();
    }
}
```

Este aplicativo é semelhante ao aplicativo de exemplo que está na etapa anterior. No exemplo anterior, apenas uma única classe Order é registrada. O WebSphere eXtreme Scale detecta e automaticamente inclui a referência na entidade Customer e uma instância Customer para `John Smith` é criada e referenciada a partir do novo objeto Order. Como resultado, o novo cliente é persistido automaticamente, porque o relacionamento entre duas ordens inclui o modificador em cascata, que requer que cada objeto seja persistido. Quando o objeto Order é localizado, o entity manager automaticamente localiza o objeto Customer associado e insere uma referência no objeto.

Tutorial do Entity Manager: Esquema da Entidade Order

Java

Crie quatro classes de entidade utilizando relacionamentos únicos e bidirecionais, listas ordenadas e relacionamentos de chave estrangeira. As APIs do EntityManager são utilizadas para persistir e localizar as entidades. Com base nas entidades Order e Customer que estão nas partes anteriores do tutorial, esta etapa do tutorial inclui mais duas entidades: as entidades Item e OrderLine.

Sobre Esta Tarefa

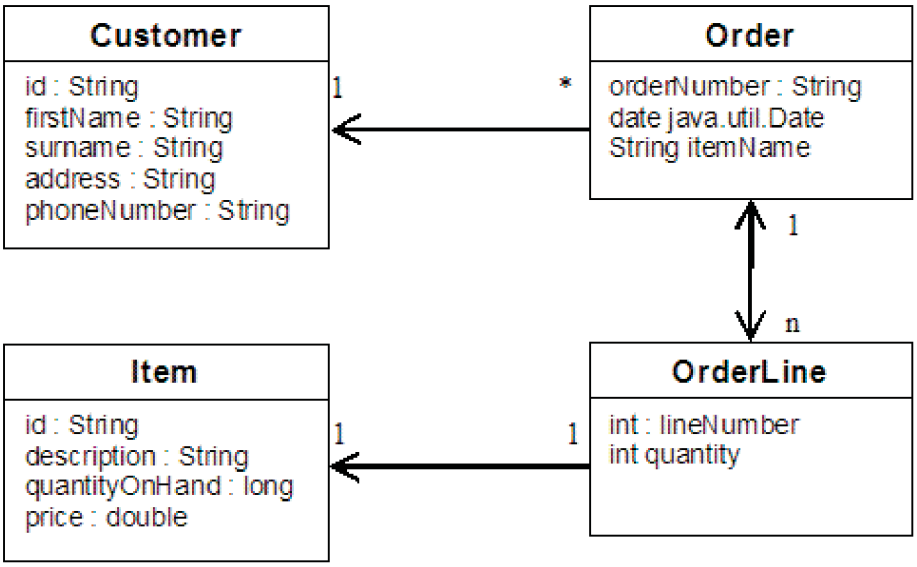


Figura 2. Esquema da Entidade Order. Uma entidade Order possui uma referência para um cliente e zero ou mais OrderLines. Cada entidade OrderLine possui uma referência para um único item e inclui a quantidade solicitada.

Procedimento

1. Crie a entidade customer, que é semelhante aos exemplos anteriores.

   Customer.java
   ```
   @Entity
   public class Customer
   {
       @Id String id;
       String firstName;
       String surname;
       String address;
       String phoneNumber;
   }
   ```

2. Crie a entidade Item, que contém informações sobre um produto que está incluído no inventário da loja, como a descrição do produto, a quantidade e o preço.

   Item.java
   ```
   @Entity
   public class Item
   {
       @Id String id;
       String description;
       long quantityOnHand;
       double price;
   }
   ```

3. Crie a entidade OrderLine. Cada Order possui zero ou mais OrderLines, que identificam a quantidade de cada item no pedido. A chave para a OrderLine é uma chave composta que consiste no Order que possui o OrderLine e um número inteiro que designa um número para a linha do pedido. Inclua o modificador de persistência em cascata em cada relacionamento em suas entidades.

   OrderLine.java
   ```
   @Entity
   public class OrderLine
   ```

```
{
    @Id @ManyToOne(cascade=CascadeType.PERSIST) Order order;
    @Id int lineNumber;
    @OneToOne(cascade=CascadeType.PERSIST) Item item;
    int quantity;
    double price;
}
```

4. Criar o Order Object final, que possui uma referência ao Customer para a ordem e uma coleta de objetos OrderLine.

   Order.java
   ```
   @Entity
   public class Order {
       @Id String orderNumber;
       java.util.Date date;
       @ManyToOne(cascade=CascadeType.PERSIST) Customer customer;
       @OneToMany(cascade=CascadeType.ALL, mappedBy="order")
      @OrderBy("lineNumber") List<OrderLine> lines;  }
   ```

   ALL em cascata é utilizado como o modificador para as linhas. Esse modificador sinaliza o EntityManager para exibir em cascata a operação PERSIST e a operação REMOVE. Por exemplo, se a entidade Order for persistida ou removida, então, todas as entidades OrderLine também são persistidas ou removidas.

   Se uma entidade OrderLine for removida da lista de linhas no objeto de Pedido, a referência então será quebrada. No entanto, a entidade OrderLine não será removida do cache. Você deve utilizar a API de remoção do EntityManager para remover entidades do cache. A operação REMOVE não é utilizada na entidade do cliente ou na entidade de item de OrderLine. Como resultado, a entidade do cliente permanece mesmo que o item ou o item seja removido quando a OrderLine for removida.

   O modificador mappedBy indica um relacionamento inverso com a entidade de destino. O modificador identifica qual atributo na entidade de destino refere-se à entidade de origem, e o lado pertencente de um relacionamento um para um ou muitos para muitos. Geralmente, é possível omitir o modificador. Entretanto, um erro é exibido para indicar que ele deve ser especificado se WebSphere eXtreme Scale não puder descobrí-lo automaticamente. Uma entidade OrderLine que contém dois tipos de atributos Order em uma relacionamento muitos para um normalmente causa o erro.

   A anotação @OrderBy especifica a ordem na qual cada entidade OrderLine deve estar na lista de linhas. Se a anotação não for especificada, então, as linhas são exibida em uma ordem arbitrária. Embora as linhas sejam incluídas na entidade Order emitindo ArrayList, o que preserva o pedido, o EntityManager não necessariamente reconhecerá a pedido. Quando você emite o método de localização para recuperar o objeto Order do cache, o objeto de lista não é um objeto ArrayList.

5. Crie o aplicativo. O exemplo a seguir ilustra o objeto Order final, que possui uma referência para o Customer para o pedido e uma coleta de objetos OrderLine.
   a. Encontre os Itens a serem ordenados, que podem se tornar entidades Gerenciadas.
   b. Crie a OrderLine e anexe-a a cada Item.
   c. Crie o Pedido e associe-o a cada OrderLine e ao cliente.
   d. Persista o pedido, que persiste automaticamente cada OrderLine.
   e. Confirme a transação, que desconecta cada entidade e sincroniza o estado das entidades com o cache.

f. Imprima as informações do pedido. As entidades OrderLine são armazenadas automaticamente pelo ID da OrderLine.

Application.java

```
static public void main(String [] args)
        throws Exception
    {
        ...

        // Add some items to our inventory.
        em.getTransaction().begin();
        createItems(em);
        em.getTransaction().commit();

        // Create a new customer with the items in his cart.
        em.getTransaction().begin();
        Customer cust = createCustomer();
        em.persist(cust);

        // Create a new order and add an order line for each item.
        // Each line item is automatically persisted since the
    // Cascade=ALL option is set.
        Order order = createOrderFromItems(em, cust, "ORDER_1",
     new String[]{"1", "2"}, new int[]{1,3});
        em.persist(order);
        em.getTransaction().commit();

        // Print the order summary
        em.getTransaction().begin();
        order = (Order)em.find(Order.class, "ORDER_1");
        System.out.println(printOrderSummary(order));
        em.getTransaction().commit();
    }

    public static Customer createCustomer() {
        Customer cust = new Customer();
        cust.address = "Main Street";
        cust.firstName = "John";
        cust.surname = "Smith";
        cust.id = "C001";
        cust.phoneNumber = "5555551212";
        return cust;
    }

    public static void createItems(EntityManager em) {
        Item item1 = new Item();
        item1.id = "1";
        item1.price = 9.99;
        item1.description = "Widget 1";
        item1.quantityOnHand = 4000;
        em.persist(item1);

        Item item2 = new Item();
        item2.id = "2";
        item2.price = 15.99;
        item2.description = "Widget 2";
        item2.quantityOnHand = 225;
        em.persist(item2);

    }

    public static Order createOrderFromItems(EntityManager em,
   Customer cust, String orderId, String[] itemIds, int[] qty) {

        Item[] items = getItems(em, itemIds);
```

```
        Order order = new Order();
        order.customer = cust;
        order.date = new java.util.Date();
        order.orderNumber = orderId;
        order.lines = new ArrayList<OrderLine>(items.length);
    for(int i=0;i<items.length;i++){
      OrderLine line = new OrderLine();
            line.lineNumber = i+1;
            line.item = items[i];
            line.price = line.item.price;
            line.quantity = qty[i];
            line.order = order;
            order.lines.add(line);
        }
        return order;
    }

    public static Item[] getItems(EntityManager em, String[] itemIds) {
        Item[] items = new Item[itemIds.length];
        for(int i=0;i<items.length;i++){
    items[i] = (Item) em.find(Item.class, itemIds[i]);
        }
        return items;
    }
```

A próxima etapa é excluir uma entidade. A interface EntityManager possui um método de remoção que marca um objeto como excluído. O aplicativo deve remover a entidade de qualquer coleta de relacionamento antes de chamar o método de remoção. Edite as referências e emita o método de remoção ou em.remove(object), como uma etapa final.

Tutorial do Entity Manager: Atualizando Entradas

Java

Se você desejar alterar uma entidade, é possível localizar a instância, atualizar a instância e quaisquer entidades referenciadas, além de executar o commit da transação.

Antes de Iniciar

Procedimento

Entradas de atualização. O exemplo a seguir demonstra como localizar a instância Order, alterá-la e qualquer entidade mencionada, e confirmar a transação.

```
public static void updateCustomerOrder(EntityManager em) {
    em.getTransaction().begin();
    Order order = (Order) em.find(Order.class, "ORDER_1");
    processDiscount(order, 10);
    Customer cust = order.customer;
    cust.phoneNumber = "5075551234";
    em.getTransaction().commit();
}

public static void processDiscount(Order order, double discountPct) {
    for(OrderLine line : order.lines) {
        line.price = line.price * ((100-discountPct)/100);
    }
}
```

Executar o flushing da transação sincroniza todas as entidades gerenciadas com o cache. Quando ocorre o commit de uma transação, automaticamente ocorre um flush. Neste caso, Order se torna uma entidade gerenciada. Quaisquer entidades referenciadas de Order, Customer e OrderLine também se tornam entidades

gerenciadas. No flush da transação, cada entidade é verificada para determinar se foi modificada. As que foram modificadas são atualizadas no cache. Após a conclusão da transação, através de commit ou rollback, as entidades se separam e quaisquer alterações feitas nas entidades não são refletidas no cache.

Tutorial do Entity Manager: Atualizando e Removendo Entradas com um Índice

Java

É possível utilizar um índice para localizar, atualizar e remover entidades.

Procedimento

Atualize e remova entidades utilizando um índice. Utilize um índice para localizar, atualizar e remover entidades. Nos exemplos anteriores, a classe de entidade Order é atualizada para utilizar a anotação @Index. A anotação @Index sinaliza ao WebSphere eXtreme Scale para criar um índice de intervalo para um atributo. O nome do índice é o mesmo nome do atributo e é sempre um tipo de índice MapRangeIndex.

Order.java

```
@Entity
public class Order {
    @Id String orderNumber;
    @Index java.util.Date date;
    @OneToOne(cascade=CascadeType.PERSIST) Customer customer;
    @OneToMany(cascade=CascadeType.ALL, mappedBy="order")
    @OrderBy("lineNumber") List<OrderLine> lines;  }
```

O exemplo a seguir demonstra como cancelar todas os pedidos enviados no último minuto. Encontrar o pedido utilizando um índice, incluir os itens no pedido de volta no inventário e remover o pedido e os itens da linha associados do sistema.

```
public static void cancelOrdersUsingIndex(Session s)
  throws ObjectGridException {
    // Cancel all orders that were submitted 1 minute ago
    java.util.Date cancelTime = new
   java.util.Date(System.currentTimeMillis() - 60000);
    EntityManager em = s.getEntityManager();
    em.getTransaction().begin();
    MapRangeIndex dateIndex = (MapRangeIndex)
   s.getMap("Order").getIndex("date");
    Iterator<Tuple> orderKeys = dateIndex.findGreaterEqual(cancelTime);
  while(orderKeys.hasNext()) {
   Tuple orderKey = orderKeys.next();
   // Localizar o Pedido para que possamos removê-lo.
   Order curOrder = (Order) em.find(Order.class, orderKey);
   // Verificar se o pedido não foi atualizado por outra pessoa.
   if(curOrder != null && curOrder.date.getTime() >= cancelTime.getTime()) {
    for(OrderLine line : curOrder.lines) {
     // Incluir o item novamente no inventário.
     line.item.quantityOnHand += line.quantity;
     line.quantity = 0;
    }
   em.remove(curOrder);
   }
  }
 em.getTransaction().commit();
}
```

Tutorial do Entity Manager: Atualizando e Removendo Entradas Utilizando uma Consulta

Java

É possível atualizar e remover entidades utilizando uma consulta.

Procedimento

Atualize e remova entidades utilizando uma consulta.

Order.java

```
@Entity
public class Order {
    @Id String orderNumber;
    @Index java.util.Date date;
    @OneToOne(cascade=CascadeType.PERSIST) Customer customer;
    @OneToMany(cascade=CascadeType.ALL, mappedBy="order")
   @OrderBy("lineNumber") List<OrderLine> lines;  }
```

A classe de entidade order é a mesma que a do exemplo anterior. A classe ainda fornece a anotação @Index, porque a cadeia de consultas utiliza a data para localizar a entidade. O mecanismo de consulta utiliza índices quando eles podem ser utilizados.

```
public static void cancelOrdersUsingQuery(Session s) {
        // Cancel all orders that were submitted 1 minute ago
        java.util.Date cancelTime =
     new java.util.Date(System.currentTimeMillis() - 60000);
        EntityManager em = s.getEntityManager();
        em.getTransaction().begin();

        // Create a query that will find the order based on date.  Since
        // we have an index defined on the order date, the query
    // will automatically use it.
        Query query = em.createQuery("SELECT order FROM Order order
     WHERE order.date >= ?1");
        query.setParameter(1, cancelTime);
        Iterator<Order> orderIterator = query.getResultIterator();
    while(orderIterator.hasNext()) {
     Order order = orderIterator.next();
     // Verificar se o pedido não foi atualizado por outra pessoa.
     // Since the query used an index, there was no lock on the row.
     if(order != null && order.date.getTime() >= cancelTime.getTime()) {
       for(OrderLine line : order.lines) {
        // Incluir o item novamente no inventário.
        line.item.quantityOnHand += line.quantity;
        line.quantity = 0;
       }
       em.remove(order);
     }
   }
  em.getTransaction().commit();
}
```

Como o exemplo anterior, o método cancelOrdersUsingQuery é destinado a cancelar todos os pedidos que foram enviados no último minuto. Para cancelar o pedido, você o localiza utilizando uma consulta, inclui os itens no pedido de volta no inventário e remove o pedido e os itens de linha associados do sistema.

Tutorial: Configurando a Segurança do Java SE

Com o seguinte tutorial, é possível criar um ambiente eXtreme Scale distribuído em um ambiente Java Platform, Standard Edition.

Antes de Iniciar

Certifique-se de estar familiarizado com os conceitos básicos de uma configuração distribuída do eXtreme Scale.

Sobre Esta Tarefa

Utilize este tutorial quando tiver instalado o eXtreme Scale em um ambiente independente. Cada etapa no tutorial é baseada na anterior. Siga cada etapa para proteger um eXtreme Scale distribuído e a desenvolver um aplicativo simples Java SE para acessar o eXtreme Scale protegido.

Iniciar o tutorial

Tutorial de Segurança do Java SE - Etapa 1

Para trabalhar com o restante do tutorial, é necessário criar e fazer um pacote de um programa Java simples e dois arquivos XML. Esse conjunto de arquivos define uma configuração simples do ObjectGrid com uma instância ObjectGrid denominada `accounting` e um mapa `customer`. O arquivo `SimpleDP.xml` retrata uma política de implementação de um conjunto de mapas configurado com uma partição e réplicas com o mínimo de zero requeridas.

Procedimento

1. Em uma janela de linha de comandos, acesse o diretório *wxs_home*.
2. Crie um diretório chamado `applib`.
3. Assegure que seu ambiente de desenvolvimento contenha o arquivo `ogclient.jar` no caminho de classe. Para obter mais informações, consulte *Guia de Programação*.
4. Crie e compile a classe `SimpleApp.java` a seguir:

SimpleApp.java

```
// This sample program is provided AS IS and may be used, executed, copied and modified
// without royalty payment by customer
// (a) for its own instruction and study,
// (b) in order to develop applications designed to run with an IBM WebSphere product,
// either for customer's own internal use or for redistribution by customer, as part of such an
// application, in customer's own products.
// Licensed Materials - Property of IBM
// 5724-J34 (C) COPYRIGHT International Business Machines Corp. 2007-2009
package com.ibm.websphere.objectgrid.security.sample.guide;

import com.ibm.websphere.objectgrid.ClientClusterContext;
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.ObjectGridManager;
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
import com.ibm.websphere.objectgrid.ObjectMap;
import com.ibm.websphere.objectgrid.Session;

public class SimpleApp {

    public static void main(String[] args) throws Exception  {

        SimpleApp app = new SimpleApp();
        app.run(args);
    }

    /**
     * read and write the map
     * @throws Exception
     */
    protected void run(String[] args) throws Exception {
        ObjectGrid og = getObjectGrid(args);

        Session session = og.getSession();

        ObjectMap customerMap = session.getMap("customer");

        String customer = (String) customerMap.get("0001");
```

```
        if (customer == null) {
            customerMap.insert("0001", "fName lName");
        } else {
            customerMap.update("0001", "fName lName");
        }
        customer = (String) customerMap.get("0001");
 // Close the session (optional in Version 7.1.1 and later) for improved performance
 session.close();
        System.out.println("The customer name for ID 0001 is " + customer);
    }

    /**
     * Get the ObjectGrid
     * @return an ObjectGrid instance
     * @throws Exception
     */
    protected ObjectGrid getObjectGrid(String[] args) throws Exception {
        ObjectGridManager ogManager = ObjectGridManagerFactory.getObjectGridManager();

        // Create an ObjectGrid
        ClientClusterContext ccContext =
ogManager.connect("localhost:2809", null, null);
        ObjectGrid og = ogManager.getObjectGrid(ccContext, "accounting");

        return og;

    }

}
```

5. Compile o pacote com este arquivo e o nome de JAR `sec_sample.jar`.
6. Acesse o diretório *wxs_home* e crie um diretório denominado `xml`
7. No diretório *wxs_home*`/xml`, crie os arquivos de configuração a seguir:

   SimpleApp.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="accounting">
            <backingMap name="customer" readOnly="false" copyKey="true"/>
        </objectGrid>
    </objectGrids>
</objectGridConfig>
```

   O arquivo XML a seguir configura o ambiente de implementação.

   SimpleDP.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<deploymentPolicy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/deploymentPolicy ../deploymentPolicy.xsd"
 xmlns="http://ibm.com/ws/objectgrid/deploymentPolicy">

 <objectgridDeployment objectgridName="accounting">
  <mapSet name="mapSet1" numberOfPartitions="1" minSyncReplicas="0"
maxSyncReplicas="1" >"2" maxAsyncReplicas="1">
   <map ref="customer"/>
  </mapSet>
 </objectgridDeployment>
</deploymentPolicy>
```

Resultados

Esses arquivos criam uma configuração simples do ObjectGrid com um ObjectGrid e a instância `accounting` e um mapa `customer`.

Tutorial de Segurança do Java SE - Etapa 2

Antes que seja possível verificar se a amostra `SimpleApp.java` é executada, é necessário iniciar um servidor de catálogos e um servidor de contêiner. Após iniciar esses serviços com êxito, é possível então ativar o cliente e executar a

amostra. Recursos de segurança adicionais são incluídos de maneira incremental nas etapas do tutorial para aumentar a quantidade de segurança integrada que está disponível.

Antes de Iniciar

Para concluir essa etapa do tutorial com êxito, é necessário ter acesso aos arquivos a seguir:

- Ter acesso ao pacote `sec_sample.jar` compilado. Esse pacote contém o programa `SimpleApp.java`.
- Ter acesso aos arquivos de configuração necessários `SimpleApp.xml` e `SimpleDP.xml`.

Esses arquivos devem ter sido criados no "Tutorial de Segurança do Java SE - Etapa 1" na página 21 deste tutorial.

Você deve também saber como:

- Iniciar e parar servidores de catálogos e servidores de contêiner. Para obter informações adicionais, consulte Iniciando e Parando Servidores Independentes.

  Reprovado: 8.6+ Os comandos **startOgServer** e **stopOgServer** iniciam servidores que usam o mecanismo de transporte do Object Request Broker (ORB). O ORB foi descontinuado, mas você pode continuar utilizando esses scripts se estava utilizando o ORB em uma liberação anterior. O mecanismo de transporte do IBM eXtremeIO (XIO) substitui o ORB. Use os scripts **startXsServer** e **stopXsServer** para iniciar e parar os servidores que utilizam o transporte XIO.
- Execute o utilitário **xscmd** para verificar o tamanho do mapa inserido na grade de dados.

Procedimento

1. Em uma janela de linha de comandos, acesse o diretório *wxs_home*/bin e inicie o serviço de catálogo.
   - UNIX Linux `./startOgServer.sh catalogServer`
   - Windows `startOgServer.bat catalogServer`
   - UNIX Linux 8.6+ `./startXsServer.sh catalogServer`
   - Windows 8.6+ `startXsServer.bat catalogServer`
2. Inicie um serviço de contêiner denominado `c0`:
   - UNIX Linux
     ```
     ./startOgServer.sh c0 -objectGridFile
     ../xml/SimpleApp.xml -deploymentPolicyFile ../xml/SimpleDP.xml
     -catalogServiceEndPoints localhost:2809
     ```
   - Windows
     ```
     startOgServer.bat c0 -objectGridFile ..\xml\SimpleApp.xml -
     deploymentPolicyFile ..\xml\SimpleDP.xml  -catalogServiceEndPoints
     localhost:2809
     ```
   - UNIX Linux 8.6+
     ```
     ./startXsServer.sh c0 -objectGridFile
     ../xml/SimpleApp.xml -deploymentPolicyFile ../xml/SimpleDP.xml
     -catalogServiceEndPoints localhost:2809
     ```
   - Windows 8.6+
     ```
     startXsServer.bat c0 -objectGridFile
     ..\xml\SimpleApp.xml - deploymentPolicyFile ..\xml\SimpleDP.xml
     -catalogServiceEndPoints localhost:2809
     ```

3. Após o servidor de catálogos e o servidor de contêiner terem sido iniciados, execute a amostra `sec_sample.jar` da seguinte maneira: `java -classpath ../lib/objectgrid.jar:../applib/sec_sample.jar com.ibm.websphere.objectgrid.security.sample.guide.SimpleApp`

   `java -classpath ..\lib\objectgrid.jar;..\applib\sec_sample.jar com.ibm.websphere.objectgrid.security.sample.guide.SimpleApp` A saída da amostra é: `O nome do cliente para o ID 0001 é fName lName` O método getObjectGrid nesta classe obtém um ObjectGrid e o método de execução lê um registro do mapa do cliente e atualiza o valor na grade de contábil.
4. Verifique o tamanho do mapa de "cliente" inserido na grade "contábil", emitindo o utilitário de comando **xscmd** da seguinte maneira:
   - UNIX Linux `./xscmd.sh -c showMapSizes -g accounting -ms mapSet1`
   - Windows `xscmd.bat -c showMapSizes -g accounting -ms mapSet1`
5. Pare um servidor de contêiner denominado `c0` com um dos scripts a seguir:
   - UNIX Linux `./stopOgServer.sh c0 -catalogServiceEndPoints localhost:2809`
   - Windows `stopOgServer.bat c0 -catalogServiceEndPoints localhost:2809`
   - 8.6+ UNIX Linux `./stopXsServer.sh c0 -catalogServiceEndPoints localhost:2809`
   - 8.6+ Windows `stopXsServer.bat c0 -catalogServiceEndPoints localhost:2809`

   Se o servidor tiver sido interrompido com êxito, aparecerá a mensagem a seguir:

   `CWOBJ2512I: ObjectGrid server c0 stopped.`
6. Pare o servidor de catálogos com um dos scripts a seguir:
   - UNIX Linux `./stopOgServer.sh catalogServer -catalogServiceEndPoints localhost:2809`
   - Windows `stopOgServer.bat catalogServer -catalogServiceEndPoints localhost:2809`
   - 8.6+ UNIX Linux `./stopXsServer.sh catalogServer -catalogServiceEndPoints localhost:2809`
   - 8.6+ Windows `stopXsServer.bat catalogServer -catalogServiceEndPoints localhost:2809`

   Se o servidor tiver sido interrompido com êxito, aparecerá a mensagem a seguir:

   `CWOBJ2512I: ObjectGrid server catalogServer stopped.`

Tutorial de Segurança do Java SE - Etapa 3

O restante do tutorial demonstra como ativar a autenticação de cliente antes de se conectar a um servidor do eXtreme Scale. Para se preparar para a próxima etapa deste tutorial, é necessário empacotar o programa `SecureSimpleApp.java` em um JAR e criar um conjunto de arquivos de configuração, que inclui um arquivo `security.xml` e dois arquivos de configuração JAAS. O arquivo `security.xml`

permite que você grave a autenticação no ambiente e os arquivos de configuração JAAS fornecem o mecanismo de autenticação durante a conexão com o servidor.

Procedimento

1. Em uma janela de linha de comandos, acesse o diretório *wxs_home*/applib criado em "Tutorial de Segurança do Java SE - Etapa 1" na página 21.
2. Crie e compile a classe SecureSimpleApp.java a seguir:

SecureSimpleApp.java

```
package com.ibm.websphere.objectgrid.security.sample.guide;

import com.ibm.websphere.objectgrid.ClientClusterContext;
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.ObjectGridManager;
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
import com.ibm.websphere.objectgrid.security.config.ClientSecurityConfiguration;
import com.ibm.websphere.objectgrid.security.config.ClientSecurityConfigurationFactory;
import com.ibm.websphere.objectgrid.security.plugins.CredentialGenerator;
import com.ibm.websphere.objectgrid.security.plugins.builtins.UserPasswordCredentialGenerator;

public class SecureSimpleApp extends SimpleApp {

    public static void main(String[] args) throws Exception  {

        SecureSimpleApp app = new SecureSimpleApp();
        app.run(args);
    }

    /**
     * Get the ObjectGrid
     * @return an ObjectGrid instance
     * @throws Exception
     */
    protected ObjectGrid getObjectGrid(String[] args) throws Exception {
        ObjectGridManager ogManager = ObjectGridManagerFactory.getObjectGridManager();
        ogManager.setTraceFileName("logs/client.log");
        ogManager.setTraceSpecification("ObjectGrid*=all=enabled:ORBRas=all=enabled");

        // Creates a ClientSecurityConfiguration object using the specified file
        ClientSecurityConfiguration clientSC = ClientSecurityConfigurationFactory
                .getClientSecurityConfiguration(args[0]);

        // Creates a CredentialGenerator using the passed-in user and password.
        CredentialGenerator credGen = new UserPasswordCredentialGenerator(args[1], args[2]);
        clientSC.setCredentialGenerator(credGen);

        // Create an ObjectGrid by connecting to the catalog server
        ClientClusterContext ccContext =
ogManager.connect("localhost:2809", clientSC, null);
        ObjectGrid og = ogManager.getObjectGrid(ccContext, "accounting");

        return og;

    }

}
```

3. Assegure que seu ambiente de desenvolvimento contenha o arquivo ogclient.jar no caminho de classe. Para obter mais informações, consulte *Guia de Programação*.
4. Compile o pacote com estes arquivos e o nome de JAR sec_sample.jar.
5. Altere para o diretório *wxs_home*.
6. Crie um diretório chamado security.
7. Crie um arquivo de configuração chamado security.xml. As propriedades de segurança do servidor são especificadas neste arquivo. Essas propriedades são comuns para os servidores de catálogos e os servidores de contêiner.

security.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<securityConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config/security
../objectGridSecurity.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config/security">

 <security securityEnabled="true" loginSessionExpirationTime="300" >
```

```
        <authenticator className ="com.ibm.websphere.objectgrid.security.plugins.
builtins.KeyStoreLoginAuthenticator">
        </authenticator>
    </security>

</securityConfig>
```

Tutorial de Segurança do Java SE - Etapa 4

Baseado na etapa anterior, o tópico a seguir mostra como implementar a autenticação de cliente em um ambiente distribuído do eXtreme Scale.

Antes de Iniciar

Certifique-se de ter concluído o "Tutorial de Segurança do Java SE - Etapa 3" na página 24. Você precisa ter criado e confirmado a amostra `SecureSimpleApp.java` em um arquivo `sec_sample.jar` e criado um arquivo de configuração denominado`security.xml`.

Sobre Esta Tarefa

Com a autenticação de cliente ativada, um cliente é autenticado antes de conectar-se ao servidor eXtreme Scale. Esta seção demonstra como a autenticação de cliente pode ser feita em um ambiente do servidor eXtreme Scale, usando o `SecureSimpleApp.java` de amostra.

Credencial de cliente

A amostra `SecureSimpleApp.java` usa as duas implementações de plug-in a seguir para obter credenciais de cliente:

`com.ibm.websphere.objectgrid.security.plugins.builtins.UserPasswordCredential`

`com.ibm.websphere.objectgrid.security.plugins.builtins.UserPasswordCredentialGenerator`

Para obter mais informações sobre esses plug-ins, consulte o "Programação de Autenticação de Cliente" na página 809.

Autenticação do servidor

O exemplo usa uma implementação integrada do eXtreme Scale: `KeyStoreLoginAuthenticator`, que é para propósitos de teste e amostra (uma keystore é um registro do usuário simples e não deve ser usado para produção). Para obter mais informações, consulte o tópico sobre o plug-in do autenticador em "Programação de Autenticação de Cliente" na página 809.

Procedimento

1. Em uma janela de linha de comandos, acesse o diretório *wxs_home*.
2. Altere para o diretório *wxs_home*/`security` criado no "Tutorial de Segurança do Java SE - Etapa 3" na página 24.
3. Crie um arquivo de configuração JAAS que impinge um método de autenticação para o servidor, o `og_jaas.config`. O `KeyStoreLoginAuthenticator` mencionado no arquivo `security.xml` usa um keystore usando o módulo de login do JAAS, o "KeyStoreLogin". O keystore pode ser configurado como uma opção para a classe KeyStoreLoginModule.

   `og_jaas.config`
   ```
   KeyStoreLogin{
   com.ibm.websphere.objectgrid.security.plugins.builtins.KeyStoreLoginModule required
        keyStoreFile="../security/sampleKS.jks" debug = true;
   };
   ```

4. Altere para o diretório *java_home*/bin e execute o keytool.
5. Altere para o diretório *wxs_home* /security e crie dois usuários, "manager" e "cashier" com suas próprias senhas.
   a. Use o keytool para criar um usuário "manager" com a senha "manager1" no keystore sampleKS.jks.
      - UNIX Linux

        ```
        keytool -genkey -v -keystore sampleKS.jks -storepass sampleKS1 \
        -alias manager -keypass manager1 \
        -dname CN=manager,O=acme,OU=OGSample -validity 10000
        ```

      - Windows

        ```
        keytool -genkey -v -keystore sampleKS.jks -storepass sampleKS1 ^
        -alias manager -keypass manager1 ^
        -dname CN=manager,O=acme,OU=OGSample -validity 10000
        ```

   b. Use o keytool para criar um usuário "cashier" com a senha "cashier1" no keystore sampleKS.jks.
      - UNIX Linux

        ```
        keytool -genkey -v -keystore sampleKS.jks -storepass sampleKS1 \
        -alias cashier -keypass cashier1 \
        -dname CN=cashier,O=acme,OU=OGSample -validity 10000
        ```

      - Windows

        ```
        keytool -genkey -v -keystore sampleKS.jks -storepass sampleKS1 ^
        -alias cashier -keypass cashier1 ^
        -dname CN=cashier,O=acme,OU=OGSample -validity 10000
        ```

6. Faça uma cópia do arquivo sampleClient.properties localizado no wxs_home/properties directory em wxs_home/security/client.properties
   - UNIX Linux

     ```
     cp ../properties/sampleClient.properties client.properties
     ```

   - Windows

     ```
     copy ..\properties\sampleClient.properties client.properties
     ```

7. No diretório *wxs_home*/security, salve-o como client.properties

   Faça as mudanças a seguir no arquivo client.properties:
   a. **securityEnabled:** Configurar **securityEnabled** como verdadeiro (valor padrão) ativa a segurança do cliente, que inclui autenticação.
   b. **credentialAuthentication:** Configure **credentialAuthentication** como Suportado (valor padrão), o que significa que o cliente suporta autenticação de credencial.
   c. **transportType:** Configure o **transportType** como TCP/IP, o que significa que nenhum SSL será usado.
8. Copie o arquivo sampleServer.properties no diretório *wxs_home*/security e salve-o como server.properties.
   - UNIX Linux

     ```
     cp ../properties/sampleServer.properties server.properties
     ```

   - Windows

     ```
     copy ..\properties\sampleServer.properties server.properties
     ```

   Faça as seguintes alterações no arquivo server.properties:
   a. **securityEnabled:** Configure o atributo **securityEnabled** como true.
   b. **transportType:** Configure o atributo **transportType** como TCP/IP, o que significa que nenhum SSL será utilizado.

c. **secureTokenManagerType:** Configure o atributo **secureTokenManagerType** como none para não configurar o gerenciador de tokens seguros.

9. Acesse o diretório *wxs_home*/bin e, dependendo da plataforma, emita um dos comandos a seguir para iniciar um servidor de catálogos. É necessário emitir as opções de linha de comandos **-clusterFile** e **-serverProps** para passar nas propriedades de segurança:

   - UNIX Linux

     ```
     ./startOgServer.sh catalogServer -clusterSecurityFile ../security/security.xml
     -serverProps ../security/server.properties -jvmArgs
     -Djava.security.auth.login.config="../security/og_jaas.config"
     ```

   - Windows

     ```
     startOgServer.bat catalogServer -clusterSecurityFile ..\security\security.xml
     -serverProps ..\security\server.properties -jvmArgs
     -Djava.security.auth.login.config="..\security\og_jaas.config"
     ```

   - UNIX Linux 8.6+

     ```
     ./startXsServer.sh catalogServer -clusterSecurityFile ../security/security.xml
     -serverProps ../security/server.properties -jvmArgs
     -Djava.security.auth.login.config="../security/og_jaas.config"
     ```

   - Windows 8.6+

     ```
     startXsServer.bat catalogServer -clusterSecurityFile ..\security\security.xml
     -serverProps ..\security\server.properties -jvmArgs
     -Djava.security.auth.login.config="..\security\og_jaas.config"
     ```

10. Inicie um servidor de contêiner chamado c0 com um dos scripts a seguir. O arquivo de propriedades de servidor é passado ao emitir o **-serverProps**.

    a.

    - UNIX Linux

      ```
      ./startOgServer.sh c0 -objectgridFile ../xml/SimpleApp.xml
      -deploymentPolicyFile ../xml/SimpleDP.xml
      -catalogServiceEndPoints localhost:2809
      -serverProps ../security/server.properties
      -jvmArgs -Djava.security.auth.login.config="../security/og_jaas.config"
      ```

    - Windows

      ```
      startOgServer.bat c0 -objectgridFile ..\xml\SimpleApp.xml
      -deploymentPolicyFile ..\xml\SimpleDP.xml
      -catalogServiceEndPoints localhost:2809
      -serverProps ..\security\server.properties
      -jvmArgs -Djava.security.auth.login.config="..\security\og_jaas.config"
      ```

    - UNIX Linux 8.6+

      ```
      ./startXsServer.sh c0 -objectgridFile ../xml/SimpleApp.xml
      -deploymentPolicyFile ../xml/SimpleDP.xml
      -catalogServiceEndPoints localhost:2809
      -serverProps ../security/server.properties
      -jvmArgs -Djava.security.auth.login.config="../security/og_jaas.config"
      ```

    - Windows 8.6+

      ```
      startXsServer.bat c0 -objectgridFile ..\xml\SimpleApp.xml
      -deploymentPolicyFile ..\xml\SimpleDP.xml
      -catalogServiceEndPoints localhost:2809
      -serverProps ..\security\server.properties
      -jvmArgs -Djava.security.auth.login.config="..\security\og_jaas.config"
      ```

11. Após o servidor de catálogos e o servidor de contêiner terem sido iniciados, execute a amostra sec_sample.jar da seguinte maneira:

    - UNIX Linux

      ```
      java -classpath ../lib/objectgrid.jar:../applib/sec_sample.jar
        com.ibm.websphere.objectgrid.security.sample.guide.SecureSimpleApp
        ../security/client.properties manager manager1
      ```

    - Windows

```
java -classpath ..\lib\objectgrid.jar;..\applib\sec_sample.jar
  com.ibm.websphere.objectgrid.security.sample.guide.SecureSimpleApp
  ..\security\client.properties manager manager1
```

Linux Utilize dois pontos (:) para o separador de caminho de classe em vez de usar ponto e vírgula (;), como no exemplo anterior.

Após executar a classe, o resultado é a seguinte saída:

O nome do cliente para o `ID 0001` é `fName lName`.

12. Verifique o tamanho do mapa de "cliente" inserido na grade "contábil", emitindo o utilitário de comando **xscmd** da seguinte maneira:
    - UNIX Linux `./xscmd.sh -c showMapSizes -g accounting -m customer -username manager -password manager1`
    - Windows `xscmd.bat -c showMapSizes -g accounting -m customer -username manager -password manager1`
13. Opcional: Para parar os servidores de contêineres ou de catálogos, é possível usar o comando **stopOgServer** ou **stopXsServer**. Porém, é necessário fornecer um arquivo de configuração de segurança. O arquivo de propriedades do cliente de amostra define as seguintes duas propriedades para gerar uma credencial userID/password (manager/manager1).

```
credentialGeneratorClass=com.ibm.websphere.objectgrid.security.plugins.builtins.UserPasswordCredentialGenerator
credentialGeneratorProps=manager manager1
```

Pare o contêiner `c0` com o comando a seguir.

- UNIX Linux `./stopOgServer.sh c0 -catalogServiceEndPoints localhost:2809 -clientSecurityFile ../security/client.properties`
- Windows `stopOgServer.bat c0 -catalogServiceEndPoints localhost:2809 -clientSecurityFile ..\security\client.properties`
- UNIX Linux 8.6+ `./stopXsServer.sh c0 -catalogServiceEndPoints localhost:2809 -clientSecurityFile ../security/client.properties`
- Windows 8.6+ `stopXsServer.bat c0 -catalogServiceEndPoints localhost:2809 -clientSecurityFile ..\security\client.properties`

Se a opção **-clientSecurityFile** não for fornecida, uma exceção será exibida com a seguinte mensagem.

```
>> SERVER (id=39132c79, host=9.10.86.47) TRACE START:

>> org.omg.CORBA.NO_PERMISSION: O servidor requer uma autenticação de
credencial mas não há nenhum contexto de segurança a partir do cliente.
Isso geralmente acontece quando o cliente não transmite uma credencial
para o servidor.

vmcid: 0x0

código secundário: 0

completed: No
```

Também é possível encerrar o servidor de catálogos usando o seguinte comando. Porém, se você desejar continuar tentando a próxima etapa do tutorial, poderá deixar que o servidor de catálogo permaneça em execução.

- UNIX Linux `./stopOgServer.sh catalogServer -catalogServiceEndPoints localhost:2809 -clientSecurityFile ../security/client.properties`
- Windows `stopOgServer.bat catalogServer -catalogServiceEndPoints localhost:2809 -clientSecurityFile ..\security\client.properties`

- UNIX Linux 8.6+ `./stopXsServer.sh -catalogServiceEndPoints localhost:2809 -clientSecurityFile ../security/client.properties`
- Windows 8.6+ `stopXsServer.bat -catalogServiceEndPoints localhost:2809 -clientSecurityFile ..\security\client.properties`

Se você encerrar o servidor de catálogos, a seguinte saída será exibida.

```
CWOBJ2512I: ObjectGrid server catalogServer stopped
```

Agora, você tornou seu sistema parcialmente seguro com sucesso, ativando a autenticação. Você configurou o servidor para conexão no registro do usuário, configurou o cliente para fornecer credenciais do cliente e alterou o arquivo de propriedades do cliente e o arquivo XML do cluster para ativar autenticação.

Se você fornecer uma senha inválida, verá uma exceção que informa que o nome de usuário ou a senha não está correto.

Para obter mais detalhes sobre a autenticação do cliente, consulte "Autenticando Aplicativos Clientes" na página 772.

Próxima etapa do tutorial

Tutorial de Segurança do Java SE - Etapa 5

Após autenticar um cliente, na etapa anterior, você pode fornecer privilégios de segurança através dos mecanismos de autorização do eXtreme Scale.

Antes de Iniciar

Certifique-se de ter concluído o "Tutorial de Segurança do Java SE - Etapa 4" na página 26 antes de continuar com esta tarefa.

Sobre Esta Tarefa

A etapa anterior deste tutorial demonstrou como ativar a autenticação em uma grade do eXtreme Scale. Como resultado, nenhum cliente não autenticado pode se conectar a seu servidor e submeter pedidos para seu sistema. Entretanto, todo cliente autenticado tem a mesma permissão ou privilégios para o servidor, como de leitura, gravação ou exclusão de dados armazenados nos mapas do ObjectGrid. Os clientes também podem emitir qualquer tipo de consulta. Esta seção demonstra como utilizar a autorização do eXtreme Scale para conceder vários privilégios de usuário autenticado.

Semelhante a vários outros sistemas, o eXtreme Scale adota um mecanismo de autorização baseado em permissão. WebSphere eXtreme Scale tem categorias de permissão diferentes que são representadas por diferentes classes de permissão. Este tópico descreve o MapPermission. Para a categoria completa de permissões, consulte o "Programação de Autorização de Cliente" na página 827.

No WebSphere eXtreme Scale, a classe com.ibm.websphere.objectgrid.security.MapPermission representa permissões para os recursos do eXtreme Scale, especificamente os métodos das interfaces ObjectMap ou JavaMap. O WebSphere eXtreme Scale define as seguintes cadeias de permissões para acesso aos métodos de ObjectMap e JavaMap:

- read: Concede permissão para ler os dados do mapa.
- write: Concede permissão para atualizar os dados no mapa.
- insert: Concede permissão para inserir os dados no mapa.
- remove: Concede permissão para remover os dados do mapa.
- invalidate: Concede permissão para invalidar os dados do mapa.

- all: Concede todas as permissões para ler, gravar, inserir, remover e invalidar.

A autorização ocorre quando um cliente chama um método de ObjectMap ou JavaMap. O ambiente de tempo de execução do eXtreme Scale verifica diferentes permissões de mapa para diferentes métodos. Se as permissões requeridas não forem concedidas ao cliente, isso resultará em um AccessControlException.

Este tutorial demonstra como utilizar a autorização Java Authentication and Authorization Service (JAAS) para conceder acessos do mapa de autorização para diferentes usuários.

Procedimento

1. **Ative a autorização do eXtreme Scale**. Para ativar a autorização no ObjectGrid, você precisa configurar o atributo securityEnabled como `true` para esse ObjectGrid específico no arquivo XML. A ativação da segurança no ObjectGrid significa que você está ativando a autorização. Utilize os seguintes comandos para criar um novo arquivo XML do ObjectGrid com a segurança ativada.
   a. Navegue até o diretório `xml`.
      ```
      cd objectgridRoot/xml
      ```
   b. Copie o arquivo `SimpleApp.xml` no arquivo `SecureSimpleApp.xml`.
      - UNIX Linux
        ```
        cp SimpleApp.xml SecureSimpleApp.xml
        ```
      - Windows
        ```
        copy SimpleApp.xml SecureSimpleApp.xml
        ```
   c. Abra o arquivo `SecureSimpleApp.xml` e inclua `securityEnabled="true"` no nível do ObjectGrid como mostra o seguinte XML:
      ```
      <?xml version="1.0" encoding="UTF-8"?>
      <objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
         xmlns="http://ibm.com/ws/objectgrid/config">
          <objectGrids>
              <objectGrid name="accounting" securityEnabled="true">
                  <backingMap name="customer" readOnly="false" copyKey="true"/>
              </objectGrid>
          </objectGrids>
      </objectGridConfig>
      ```
2. **Defina a política de autorização.** No tópico de autenticação de cliente anterior, você criou os usuários, cashier e manager, no keystore. Neste exemplo, o usuário "cashier" só tem permissões de leitura a todos os mapas, e o usuário "manager" tem todas as permissões. A autorização JAAS é usada neste exemplo. Você deve criar um arquivo de política de autorização JAAS para conceder permissões aos principais. Crie o arquivo `og_auth.policy` a seguir no diretório `objectgridRoot/security`:
   og_auth.policy
   ```
   grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
       principal javax.security.auth.x500.X500Principal "CN=cashier,O=acme,OU=OGSample" {
       permission com.ibm.websphere.objectgrid.security.MapPermission "accounting.*", "read ";
   };

   grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
       principal javax.security.auth.x500.X500Principal "CN=manager,O=acme,OU=OGSample" {
       permission com.ibm.websphere.objectgrid.security.MapPermission "accounting.*", "all";
   };
   ```

   Nota:
   - `codebase "http://www.ibm.com/com/ibm/ws/objectgridRoot/security/PrivilegedAction"` é uma URL especialmente reservada para o ObjectGrid. Todas as permissões do ObjectGrid concedidas a principals devem utilizar esse código base especial.

- A primeira instrução de concessão concede permissão de mapa "read" ao principal `"CN=cashier,O=acme,OU=OGSample"`, de modo que cashier tenha apenas permissão de leitura ao mapa para todos os mapas na contabilidade do ObjectGrid.
- A segunda instrução de concessão concede permissão de mapa "all" ao principal `"CN=manager,O=acme,OU=OGSample"`, de modo que manager tenha todas as permissões para os mapas na contabilidade do ObjectGrid.

Agora você pode ativar um servidor com uma política de autorização. O arquivo de políticas de autorização de JAAS pode ser configurado usando a propriedade -D padrão: `-Djava.security.policy=../security/og_auth.policy`

3. **Execute o aplicativo.**

   Depois de criar os arquivos acima, será possível executar o aplicativo.

   Utilize os seguintes comandos para iniciar o servidor de catálogos. Para obter mais informações sobre como iniciar o serviço de catálogo, consulte o Iniciando um Serviço de Catálogo Independente que Utiliza o Transporte ORB.

   a. Navegue até o diretório bin: `cd objectgridRoot/bin`

   b. Inicie o servidor de catálogos.

   - UNIX Linux

     ```
     ./startOgServer.sh catalogServer
     -clusterSecurityFile ../security/security.xml
     -serverProps ../security/server.properties
     -jvmArgs -Djava.security.auth.login.config="../security/og_jaas.config"
     ```

   - Windows

     ```
     startOgServer.bat catalogServer
     -clusterSecurityFile ..\security\security.xml
     -serverProps ..\security\server.properties
     -jvmArgs -Djava.security.auth.login.config="..\security\og_jaas.config"
     ```

   - 8.6+ UNIX Linux

     ```
     ./startXsServer.sh catalogServer
     -clusterSecurityFile ../security/security.xml
     -serverProps ../security/server.properties
     -jvmArgs -Djava.security.auth.login.config="../security/og_jaas.config"
     ```

   - 8.6+ Windows

     ```
     startXsServer.bat catalogServer
     -clusterSecurityFile ..\security\security.xml
     -serverProps ..\security\server.properties
     -jvmArgs -Djava.security.auth.login.config="..\security\og_jaas.config"
     ```

     Os arquivos `security.xml` e `server.properties` foram criados na etapa anterior deste tutorial.

   c. É possível iniciar um servidor de contêiner seguro utilizando o seguinte script. Execute o seguinte script a partir do diretório bin:

   - UNIX Linux

     ```
     ./startOgServer.sh c0 -objectGridFile ../xml/SecureSimpleApp.xml
     -deploymentPolicyFile ../xml/SimpleDP.xml
     -catalogServiceEndPoints localhost:2809
     -serverProps ../security/server.properties
     -jvmArgs -Djava.security.auth.login.config="../security/og_jaas.config"
     -Djava.security.policy="../security/og_auth.policy"
     ```

   - Windows

     ```
     startOgServer.bat c0 -objectGridFile ..\xml\SecureSimpleApp.xml
     -deploymentPolicyFile ..\xml\SimpleDP.xml
     -catalogServiceEndPoints localhost:2809
     ```

```
-serverProps ..\security\server.properties
-jvmArgs -Djava.security.auth.login.config="..\security\og_jaas.config"
-Djava.security.policy="..\security\og_auth.policy"
```

- 8.6+ UNIX Linux

```
./startXsServer.sh c0 -objectGridFile ../xml/SecureSimpleApp.xml
-deploymentPolicyFile ../xml/SimpleDP.xml
-catalogServiceEndPoints localhost:2809
-serverProps ../security/server.properties
-jvmArgs -Djava.security.auth.login.config="../security/og_jaas.config"
-Djava.security.policy="../security/og_auth.policy"
```

- 8.6+ Windows

```
startXsServer.bat c0 -objectGridFile ..\xml\SecureSimpleApp.xml
-deploymentPolicyFile ..\xml\SimpleDP.xml
-catalogServiceEndPoints localhost:2809
-serverProps ..\security\server.properties
-jvmArgs -Djava.security.auth.login.config="..\security\og_jaas.config"
-Djava.security.policy="..\security\og_auth.policy"
```

Observe as seguintes diferenças do comando para iniciar o servidor de contêiner anterior:

- Utilize o arquivo `SecureSimpleApp.xml` em vez de o arquivo `SimpleApp.xml`.
- Inclua outro argumento `-Djava.security.policy` para configurar o arquivo de políticas de autorização de JAAS para o processo do servidor de contêiner.

Utilize o mesmo comando da etapa anterior do tutorial:

a. Navegue até o diretório bin.

- UNIX Linux

```
java -classpath ../lib/objectgrid.jar:../applib/sec_sample.jar com.ibm.websphere.objectgrid.security.sample.guide.SecureSimpleApp
../security/client.properties manager manager1
```

- Windows

```
java -classpath ..\lib\objectgrid.jar;..\applib\sec_sample.jar com.ibm.websphere.objectgrid.security.sample.guide.SecureSimpleApp
 ..\security\client.properties manager manager1
```

b. Como o usuário "manager" possui todas as permissões para mapas no ObjectGrid de contabilidade, o aplicativo é executado apropriadamente.

Agora, em vez de utilizar o usuário "manager", utilize o usuário "cashier" para ativar o aplicativo cliente.

c. Navegue até o diretório bin.

- UNIX Linux

```
java -classpath ../lib/objectgrid.jar:../applib/sec_sample.jar com.ibm.ws.objectgrid.security.sample.guide.SecureSimpleApp
../security/client.properties cashier cashier1
```

- Windows

```
java -classpath ..\lib\objectgrid.jar;..\applib\sec_sample.jar com.ibm.ws.objectgrid.security.sample.guide.SecureSimpleApp
..\security\client.properties cashier cashier1
```

Resulta na seguinte exceção:

```
Exception in thread "P=387313:O=0:CT" com.ibm.websphere.objectgrid.TransactionException:
rolling back transaction, see caused by exception
 at com.ibm.ws.objectgrid.SessionImpl.rollbackPMapChanges(SessionImpl.java:1422)
  at com.ibm.ws.objectgrid.SessionImpl.commit(SessionImpl.java:1149)
  at com.ibm.ws.objectgrid.SessionImpl.mapPostInvoke(SessionImpl.java:2260)
  at com.ibm.ws.objectgrid.ObjectMapImpl.update(ObjectMapImpl.java:1062)
  at com.ibm.ws.objectgrid.security.sample.guide.SimpleApp.run(SimpleApp.java:42)
 at com.ibm.ws.objectgrid.security.sample.guide.SecureSimpleApp.main(SecureSimpleApp.java:27)
Caused by: com.ibm.websphere.objectgrid.ClientServerTransactionCallbackException:
   Client Services - received exception from remote server:
     com.ibm.websphere.objectgrid.TransactionException: transaction rolled back, see caused by Throwable
        at com.ibm.ws.objectgrid.client.RemoteTransactionCallbackImpl.processReadWriteResponse(
            RemoteTransactionCallbackImpl.java:1399)
        at com.ibm.ws.objectgrid.client.RemoteTransactionCallbackImpl.processReadWriteRequestAndResponse(
            RemoteTransactionCallbackImpl.java:2333)
```

```
        at com.ibm.ws.objectgrid.client.RemoteTransactionCallbackImpl.commit(RemoteTransactionCallbackImpl.java:557)
        at com.ibm.ws.objectgrid.SessionImpl.commit(SessionImpl.java:1079)
        ... 4 more
Caused by: com.ibm.websphere.objectgrid.TransactionException: transaction rolled back, see caused by Throwable
        at com.ibm.ws.objectgrid.ServerCoreEventProcessor.processLogSequence(ServerCoreEventProcessor.java:1133)
        at com.ibm.ws.objectgrid.ServerCoreEventProcessor.processReadWriteTransactionRequest(ServerCoreEventProcessor.java:910)
        at com.ibm.ws.objectgrid.ServerCoreEventProcessor.processClientServerRequest(ServerCoreEventProcessor.java:1285)

        at com.ibm.ws.objectgrid.ShardImpl.processMessage(ShardImpl.java:515)
        at com.ibm.ws.objectgrid.partition.IDLShardPOA._invoke(IDLShardPOA.java:154)
        at com.ibm.CORBA.poa.POAServerDelegate.dispatchToServant(POAServerDelegate.java:396)
        at com.ibm.CORBA.poa.POAServerDelegate.internalDispatch(POAServerDelegate.java:331)
        at com.ibm.CORBA.poa.POAServerDelegate.dispatch(POAServerDelegate.java:253)
        at com.ibm.rmi.iiop.ORB.process(ORB.java:503)
        at com.ibm.CORBA.iiop.ORB.process(ORB.java:1553)
        at com.ibm.rmi.iiop.Connection.respondTo(Connection.java:2680)
        at com.ibm.rmi.iiop.Connection.doWork(Connection.java:2554)
        at com.ibm.rmi.iiop.WorkUnitImpl.doWork(WorkUnitImpl.java:62)
        at com.ibm.rmi.iiop.WorkerThread.run(ThreadPoolImpl.java:202)
        at java.lang.Thread.run(Thread.java:803)
Caused by: java.security.AccessControlException: Access denied (
   com.ibm.websphere.objectgrid.security.MapPermission accounting.customer write)
        at java.security.AccessControlContext.checkPermission(AccessControlContext.java:155)
        at com.ibm.ws.objectgrid.security.MapPermissionCheckAction.run(MapPermissionCheckAction.java:141)
        at java.security.AccessController.doPrivileged(AccessController.java:275)
        at javax.security.auth.Subject.doAsPrivileged(Subject.java:727)
        at com.ibm.ws.objectgrid.security.MapAuthorizer$1.run(MapAuthorizer.java:76)
        em java.security.AccessController.doPrivileged(AccessController.java:242)
        at com.ibm.ws.objectgrid.security.MapAuthorizer.check(MapAuthorizer.java:66)
        at com.ibm.ws.objectgrid.security.SecuredObjectMapImpl.checkMapAuthorization(SecuredObjectMapImpl.java:429)
        at com.ibm.ws.objectgrid.security.SecuredObjectMapImpl.update(SecuredObjectMapImpl.java:490)
        at com.ibm.ws.objectgrid.SessionImpl.processLogSequence(SessionImpl.java:1913)
        at com.ibm.ws.objectgrid.SessionImpl.processLogSequence(SessionImpl.java:1805)
        at com.ibm.ws.objectgrid.ServerCoreEventProcessor.processLogSequence(ServerCoreEventProcessor.java:1011)
        ... 14 more
```

Essa exceção ocorre porque o usuário "cashier" não tem permissão de gravação, portanto, ele não pode atualizar o cliente do mapa.

Agora, o seu sistema suporta autorização. É possível definir políticas de autorização para conceder diferentes permissões a diferentes usuários. Para obter mais informações sobre autorização, consulte “Autorizando Aplicativos Clientes” na página 774.

O que Fazer Depois

Conclua a próxima etapa do tutorial. Consulte “Tutorial de Segurança do Java SE - Etapa 6”.

Tutorial de Segurança do Java SE - Etapa 6

A seguinte etapa explica como uma camada de segurança pode ser ativada para comunicação entre os terminais do ambiente.

Antes de Iniciar

Certifique-se de ter concluído do “Tutorial de Segurança do Java SE - Etapa 5” na página 30 antes de continuar com esta tarefa.

Sobre Esta Tarefa

A topologia do eXtreme Scale suporta Transport Layer Security/Secure Sockets Layer (TLS/SSL) para comunicação segura entre terminais do ObjectGrid (cliente, servidores de contêineres e servidores de catálogos). Esta etapa do tutorial é baseada nas etapas anteriores para ativar a segurança do transporte.

Procedimento

1. **Crie chaves TLS/SSL e keystores**

Para ativar a segurança do transporte, você deve criar um keystore e um armazenamento confiável. Este exercício cria apenas um par de chave e trust-store. Estes armazéns são utilizados para clientes do ObjectGrid, servidores de contêineres e servidores de catálogos, e são criados com o JDK keytool.

- *Criar uma chave privada no keystore*

  ```
  keytool -genkey -alias ogsample -keystore key.jks -storetype JKS
  -keyalg rsa -dname "CN=ogsample, OU=OGSample, O=acme, L=Your City,
  S=Your State, C=Your Country" -storepass ogpass -keypass ogpass
  -validity 3650
  ```

  Utilizando este comando, um keystore key.jks é criado com uma chave "ogsample" armazenada nele. Este keystore key.jks será usado como o keystore SSL.

- *Exportar o certificado público*

  ```
  keytool -export -alias ogsample -keystore key.jks -file temp.key
  -storepass ogpass
  ```

  Utilizando este comando, o certificado público da chave "ogsample" é extraído e armazenado no arquivo temp.key.

- *Importar o certificado público do cliente para o trust store*

  ```
  keytool -import -noprompt -alias ogsamplepublic -keystore trust.jks
  -file temp.key -storepass ogpass
  ```

  Usando este comando, o certificado público foi incluído no keystore trust.jks. Este trust.jks é utilizado como o trust store SSL.

2. **Configurando arquivos de propriedades do ObjectGrid**

   Neste etapa, é necessário configurar os arquivos de propriedades do ObjectGrid para ativar a segurança do transporte.

   Primeiro, copie os arquivos key.jks e trust.jks no diretório objectgridRoot/security.

   Configure as seguintes propriedades nos arquivos `client.properties` e `server.properties`.

   ```
   transportType=SSL-Required

   alias=ogsample
   contextProvider=IBMJSSE2
   protocol=SSL
   keyStoreType=JKS
   keyStore=../security/key.jks
   keyStorePassword=ogpass
   trustStoreType=JKS
   trustStore=../security/trust.jks
   trustStorePassword=ogpass
   ```

   transportType: O valor de transportType é configurado como "SSL-Required", o que significa que o transporte requer SSL. Assim, todos os terminais do ObjectGrid (clientes, servidores de catálogos e servidores de contêineres) devem ter a configuração SSL definida e toda a comunicação de transporte será criptografada.

   As outras propriedades são utilizadas para definir as configurações SSL. Consulte o “Transport Layer Security e Secure Sockets Layer” na página 785 para obter uma explicação detalhada. Certifique-se de seguir as seguintes instruções neste tópico para atualizar o arquivo `orb.properties`.

   Certifique-se de seguir essa página para atualizar o arquivo `orb.properties`.

No arquivo `server.properties`, é necessário incluir uma propriedade adicional clientAuthentication e configurá-la para false. No lado do servidor, não é necessário confiar o cliente.

```
clientAuthentication=false
```

3. **Execute o aplicativo**

   Os comandos são os mesmos que os comandos no tópico "Tutorial de Segurança do Java SE - Etapa 3" na página 24.

   Utilize os seguintes comandos para iniciar um servidor de catálogos.

   a. Navegue até o diretório bin: `cd objectgridRoot/bin`

   b. Inicie o servidor de catálogos:

   - Linux UNIX

```
./startOgServer.sh catalogServer -clusterSecurityFile ../security/security.xml
-serverProps ../security/server.properties -JMXServicePort 11001
-jvmArgs -Djava.security.auth.login.config="../security/og_jaas.config"
```

   - Windows

```
startOgServer.bat catalogServer -clusterSecurityFile ..\security\security.xml
-serverProps ..\security\server.properties -JMXServicePort 11001 -jvmArgs
-Djava.security.auth.login.config="..\security\og_jaas.config"
```

   - Linux UNIX 8.6+

```
./startXsServer.sh catalogServer -clusterSecurityFile ../security/security.xml
-serverProps ../security/server.properties -JMXServicePort 11001
-jvmArgs -Djava.security.auth.login.config="../security/og_jaas.config"
```

   - Windows 8.6+

```
startXsServer.bat catalogServer -clusterSecurityFile ..\security\security.xml
-serverProps ..\security\server.properties -JMXServicePort 11001 -jvmArgs
-Djava.security.auth.login.config="..\security\og_jaas.config"
```

   Os arquivos `security.xml` e `server.properties` foram criados na página "Tutorial de Segurança do Java SE - Etapa 2" na página 22.

   Use a opção **`-JMXServicePort`** para especificar explicitamente a porta JMX para o servidor. Essa opção é necessária para usar o comando **`xscmd`**.

   Execute um servidor de contêiner ObjectGrid:

   c. Navegue até o diretório bin novamente: `cd objectgridRoot/bin`

   d.

   - Linux UNIX

```
./startOgServer.sh c0 -objectGridFile ../xml/SecureSimpleApp.xml
-deploymentPolicyFile ../xml/SimpleDP.xml -catalogServiceEndPoints
localhost:2809 -serverProps ../security/server.properties
-JMXServicePort 11002 -jvmArgs
-Djava.security.auth.login.config="../security/og_jaas.config"
-Djava.security.policy="../security/og_auth.policy"
```

   - Windows

```
startOgServer.bat c0 -objectGridFile ..\xml\SecureSimpleApp.xml
-deploymentPolicyFile ..\xml\SimpleDP.xml -catalogServiceEndPoints localhost:2809
-serverProps ..\security\server.properties -JMXServicePort 11002
-jvmArgs -Djava.security.auth.login.config="..\security\og_jaas.config"
-Djava.security.policy="..\security\og_auth.policy"
```

   - Linux UNIX 8.6+

```
./startXsServer.sh c0 -objectGridFile ../xml/SecureSimpleApp.xml
-deploymentPolicyFile ../xml/SimpleDP.xml -catalogServiceEndPoints
localhost:2809 -serverProps ../security/server.properties
-JMXServicePort 11002 -jvmArgs
-Djava.security.auth.login.config="../security/og_jaas.config"
-Djava.security.policy="../security/og_auth.policy"
```

   - Windows 8.6+

```
startXsServer.bat c0 -objectGridFile ..\xml\SecureSimpleApp.xml
-deploymentPolicyFile ..\xml\SimpleDP.xml -catalogServiceEndPoints localhost:2809
-serverProps ..\security\server.properties -JMXServicePort 11002
-jvmArgs -Djava.security.auth.login.config="..\security\og_jaas.config"
-Djava.security.policy="..\security\og_auth.policy"
```

Observe as seguintes diferenças do comando para iniciar o servidor de contêiner anterior:

- Use a propriedade `SecureSimpleApp.xml` em vez dos arquivos `SimpleApp.xml`.
- Inclua outro -Djava.security.policy para configurar o arquivo de políticas de autorização de JAAS para o processo do servidor de contêiner.

Execute o seguinte comando para autenticação de cliente:

a. `cd objectgridRoot/bin`

   - UNIX Linux

     ```
     javaHome/java -classpath ../lib/objectgrid.jar:../applib/sec_sample.jar
     com.ibm.websphere.objectgrid.security.sample.guide.SecureSimpleApp
     ../security/client.properties manager manager1
     ```

   - Windows

     ```
     javaHome\java -classpath ..\lib\objectgrid.jar;..\applib\sec_sample.jar
     com.ibm.websphere.objectgrid.security.sample.guide.SecureSimpleApp
     ..\security\client.properties manager manager1
     ```

b. Como o usuário "manager" tem permissão para todos os mapas no ObjectGrid de contabilidade, o aplicativo é executado com êxito.

Também é possível usar o utilitário **xscmd** para mostrar os tamanhos de mapa da grade "accounting".

- Navegue até o diretório `objectgridRoot/bin`
- Use o comando **xscmd** para mostrar os tamanhos de mapa:
  - UNIX Linux

    ```
    ./xscmd.sh -c showMapsizes -g accounting -m customer -prot SSL
    -ts ../security/trust.jks -tsp ogpass -tst jks
    -user manager -pwd manager1 -ks ../security/key.jks -ksp ogpass -kst JKS
    -cxpv IBMJSSE2 -tt SSL-Required
    ```

  - Windows

    ```
    xscmd.bat -c showMapsizes -g accounting -m customer -prot SSL
    -ts ..\security\trust.jks -tsp ogpass -tst jks
    -user manager -pwd manager1 -ks ..\security\key.jks -ksp ogpass -kst JKS
    -cxpv IBMJSSE2 -tt SSL-Required
    ```

  Observe que especificamos a porta JMX do serviço de catálogo usando -p 11001 aqui.

  A seguinte saída será exibida.

```
This administrative utility is provided as a sample only and is not to
be considered a fully supported component of the WebSphere eXtreme Scale product.
Connecting to Catalog service at localhost:1099
********** Displaying Results for Grid - accounting, MapSet - customer **********
*** Listing Maps for c0 ***
Map Name: customer Partition #: 0 Map Size: 1 Shard Type: Primary
Server Total: 1
Total Domain Count: 1
```

Executando o aplicativo com um keystore incorreto

Se seu armazenamento confiável não contiver o certificado público da chave privada no keystore, uma exceção de que a chave não pode ser confiável ocorre.

Para mostrar esta exceção, crie um outro keystore `key2.jks`.

```
keytool -genkey -alias ogsample -keystore key2.jks -storetype JKS
-keyalg rsa -dname
"CN=ogsample, OU=Your Organizational Unit, O=Your Organization, L=Your
City, S=Your State, C=Your Country" -storepass ogpass -keypass ogpass
-validity 3650
```

Em seguida, modifique o arquivo `server.properties` para criar o ponto de keyStore neste novo keystore `key2.jks`:

```
keyStore=../security/key2.jks
```

Execute o seguintes comando para iniciar o servidor de catálogos:

a. Navegue até o bin: `cd objectgridRoot/bin`

b. Inicie o servidor de catálogos:

- Linux UNIX

```
./startOgServer.sh c0 -objectGridFile ../xml/SecureSimpleApp.xml
-deploymentPolicyFile ../xml/SimpleDP.xml -catalogServiceEndPoints localhost:2809
-serverProps ../security/server.properties -jvmArgs
-Djava.security.auth.login.config="../security/og_jaas.config"
-Djava.security.policy="../security/og_auth.policy"
```

- Windows

```
startOgServer.bat c0 -objectGridFile ..\xml\SecureSimpleApp.xml
-deploymentPolicyFile ..\xml/SimpleDP.xml -catalogServiceEndPoints localhost:2809
 -serverProps ..\security\server.properties -jvmArgs
-Djava.security.auth.login.config="..\security\og_jaas.config"
-Djava.security.policy="..\security\og_auth.policy"
```

- 8.6+

  Linux UNIX

```
./startXsServer.sh c0 -objectGridFile ../xml/SecureSimpleApp.xml
-deploymentPolicyFile ../xml/SimpleDP.xml -catalogServiceEndPoints localhost:2809
-serverProps ../security/server.properties -jvmArgs
-Djava.security.auth.login.config="../security/og_jaas.config"
-Djava.security.policy="../security/og_auth.policy"
```

- 8.6+

  Windows

```
startXsServer.bat c0 -objectGridFile ..\xml\SecureSimpleApp.xml
-deploymentPolicyFile ..\xml/SimpleDP.xml -catalogServiceEndPoints localhost:2809
 -serverProps ..\security\server.properties -jvmArgs
-Djava.security.auth.login.config="..\security\og_jaas.config"
-Djava.security.policy="..\security\og_auth.policy"
```

A seguinte exceção será exibida:

```
Caused by: com.ibm.websphere.objectgrid.ObjectGridRPCException:
    com.ibm.websphere.objectgrid.ObjectGridRuntimeException:
        SSL connection fails and plain socket cannot be used.
```

Por fim, altere o arquivo `server.properties` de volta para usar o arquivo `key.jks`.

Tutorial: Executar os Clientes e Servidores eXtreme Scale no Perfil do Liberty

É possível executar o WebSphere eXtreme Scale como um cliente no perfil do Liberty que o WebSphere Application Server fornece.

Objetivos do aprendizado

Neste tutorial, você pode esperar concluir os seguintes objetivos do aprendizado:

- Instalar o perfil do Liberty.
- Criar um servidor de aplicativos da web no Liberty.
- Incluir o recurso da web para o aplicativo da web.
- Configurar clientes para usar APIs do cliente no perfil do Liberty.
- Executar a grade de dados dentro do perfil do Liberty.

Tempo Necessário

Esse tutorial demora aproximadamente 60 minutos para ser concluído. Se você explorar outros conceitos relacionados a este tutorial, ele poderá demorar mais tempo para ser concluído.

Pré-requisitos

Para concluir este tutorial, você deve instalar os produtos a seguir:

- IBM® Installation Manager
- WebSphere eXtreme Scale

Perfil do Liberty

O Perfil do Liberty é um ambiente de tempo de execução do servidor de aplicativos dinâmico de alta possibilidade de composição e de rápida inicialização.

Instale o perfil do Liberty ao instalar o WebSphere eXtreme Scale com o WebSphere Application Server Versão 8.5. Em razão de um perfil do Liberty não incluir um Java Runtime Environment (JRE), é necessário instalar um JRE fornecido pelo Oracle ou IBM.

Para obter informações adicionais sobre os ambientes e locais suportados do Java, consulte Níveis mínimos suportados do Java no Centro de Informações do WebSphere Application Server.

Esse servidor suporta dois modelos de implementação do aplicativo:

- Implementa um aplicativo descartando-o no diretório `dropins`.
- Implementa um aplicativo incluindo-o na configuração do servidor.

O perfil do Liberty suporta um subconjunto das partes a seguir do modelo de programação do WebSphere Application Server:

- Aplicativos da Web
- Aplicativos OSGi
- Java Persistence API (JPA)

Os serviços associados, como transações e segurança, são suportados apenas até onde for requerido por esses tipos de aplicativo e pelo JPA.

Os recursos são as unidades de recurso pelas quais você controla as partes do ambiente de tempo de execução que são carregadas em um servidor específico. O perfil do Liberty inclui os principais recursos a seguir:

- Validação de bean
- Blueprint
- API de Java para Serviços da web RESTful
- JDBC (Java Database Connectivity)
- Java Naming and Directory Interface
- Java Persistence API (JPA)
- JavaServer Faces (JSF)
- JSP (JavaServer Pages)
- LDAP (Lightweight Directory Access Protocol)
- Conector local (para clientes do Java Management Extensions (JMX)
- Monitoramento
- JPA de OSGi (suporte a JPA para aplicativos OSGi)
- Conector remoto (para clientes JMX)
- SSL (Secure Sockets Layer)
- Segurança

- servlet
- Persistência de sessão
- Transação
- Web Application Bundle (WAB)
- Segurança z/OS
- Gerenciamento de transações z/OS
- Gerenciamento de carga de trabalho z/OS

É possível trabalhar com o ambiente de tempo de execução diretamente ou usar o WebSphere Application Server Developer Tools for Eclipse.

Nas plataformas distribuídas, o perfil do Liberty fornece um ambiente de desenvolvimento e de operações. No Mac, ele fornece um ambiente de desenvolvimento.

Nos sistemas z/OS, o perfil do Liberty fornece um ambiente de operações. É possível trabalhar com este ambiente de forma nativa, usando o console do MVS. Para o desenvolvimento de aplicativo, considere o uso das ferramentas do desenvolvedor baseado em Eclipse em um sistema distribuído, no Mac OS ou em um shell do Linux no z/OS.

Executando o Perfil do Liberty com um JRE de Terceiros

Ao usar um JRE que a Oracle fornece, devem ser feitas considerações especiais para executar o WebSphere eXtreme Scale com o perfil do Liberty.

Conflito do carregador de classes

Pode ocorrer um conflito do carregador de classe que teve uma solução alternativa com o uso das configurações do JVM_ARGS. Se ocorrer um conflito na lógica do BundleLoader, inclua os argumentos a seguir:

```
export JVM_ARGS="$JVM_ARGS -XX:+UnlockDiagnosticVMOptions -XX:+UnsyncloadClass"
```

IBM ORB

O WebSphere eXtreme Scale requer que você use o IBM ORB, que está incluído em uma instalação do WebSphere Application Server, mas não no perfil do Liberty. Você deve configurar os diretórios endossados usando a propriedade de sistema Java, `java.endorsed.dirs`, para incluir o diretório que contém os arquivos Java archive (JAR) do IBM ORB. Os arquivos JAR do IBM ORB estão incluídos na instalação do eXtreme Scale no diretório `wlp\wxs\lib\endorsed`.

Referências relacionadas:

Propriedades do Servidor de Perfis do Liberty
Utilize as opções do arquivo de propriedades do servidor para configurar os servidoresWebSphere eXtreme Scale que são executados no Perfil do Liberty.

Informações relacionadas:

"Lição 5.1: Configurar Servidores eXtreme Scale para Utilizar o Perfil do Liberty" na página 44
Para executar a grade de dados em um perfil do Liberty, você deve incluir o recurso do servidor para configurar servidores WebSphere eXtreme Scale que usam arquivos de configuração de perfil do Liberty.

Módulo 1: Instalar o Perfil do Liberty

Você deve instalar o WebSphere Application Server Versão 8.5 para obter o perfil do Liberty.

Para instalar o perfil do Liberty, você deve usar o IBM Installation Manager para instalar o WebSphere Application Server Versão 8.5 com o WebSphere eXtreme Scale ou pode instalar o Perfil do Liberty executando um arquivo JAR fornecido. É possível fazer download e instalar o ambiente de serviço do aplicativo Perfil do Liberty e o arquivo JAR incluído a partir da Página de Downloads da Comunidade WASdev.

Objetivos do aprendizado

Após concluir as lições neste módulo, você saberá como:

- Instalar o perfil do Liberty.

Pré-requisitos

Instale o WebSphere eXtreme Scale.

Módulo 2: Criar um Servidor de Aplicativos da Web no Perfil do Liberty

Você deve criar um diretório do servidor e o arquivo `server.xml` para desenvolver a definição de servidor para o perfil do Liberty.

Objetivos do aprendizado

Após concluir a lição neste módulo, você saberá como:

- Definir um servidor para executar no perfil do Liberty.

Pré-requisitos

Para concluir este módulo, você deve instalar o perfil do Liberty.

Lição 2.1: Definir um Servidor para Executar no Perfil do Liberty

Crie um diretório do servidor e o arquivo de definição de servidor para executar no perfil do Liberty.

Para criar a definição do servidor para o servidor de aplicativos da Web, insira o seguinte comando a partir do diretório `bin`:

wlp_home`/bin/server create `*your_server_name*

Para verificar se você criou o arquivo de definição do servidor, procure o arquivo XML no seguinte diretório: *wlp_home*`/usr/servers/`*your_server_name*.

É possível localizar o arquivo `server.xml` em sua definição de servidor e abrir o arquivo em um editor. Uma sub-rotina do gerenciador de recurso comentada existe no `server.xml`. No próximo módulo, você incluirá o recurso da web para essa sub-rotina da definição do servidor.

Módulo 3: Incluir o Recurso da Web do Liberty no Perfil do Liberty

Inclua o recurso da web em sua definição de servidor para identificar aplicativos baseados na web e incluir funções, tal como a replicação de sessão.

Objetivos do aprendizado

Após concluir a lição neste módulo, você saberá como:

- Definir um aplicativo da web para execução no perfil do Liberty.

Pré-requisitos

Para concluir este módulo, você deve concluir os seguintes módulos primeiro

- Instalar o perfil do Liberty.
- Criar um servidor de aplicativos da web no perfil do Liberty.

.

Lição 3.1: Definir um Aplicativo da Web para Execução no Perfil do Liberty

Defina o recurso da web para sua definição de servidor para ativar funções de aplicativo, tal como uma replicação de sessão.

 O recurso da web foi descontinuado. Use o recurso webApp quando desejar replicar os dados da sessão HTTP para tolerância a falhas.

O recurso webApp tem propriedades de metatipo que podem ser configuradas no elemento `xsWebApp` do arquivo`server.xml`. Para obter informações adicionais, consulte "Ativando o Recurso webApp do eXtreme Scale no Perfil do Liberty" na página 207

Inclua o recurso da web a seguir no arquivo Perfil do Liberty `server.xml`. O recurso da web inclui o recurso cliente; entretanto, ele não inclui o recurso do servidor. Você provavelmente deseja separar seus aplicativos da web a partir das grades de dados. Por exemplo, você tem um servidor Perfil do Liberty para seus aplicativos da web e um servidor Perfil do Liberty diferente para hospedar a grade de dados.

```
<featureManager>
<feature>eXtremeScale_web-1.0</feature>
</featureManager>
```

Seus aplicativos da web agora podem persistir seus dados de sessão em uma grade do WebSphere eXtreme Scale.

Consulte o exemplo a seguir de um arquivo `server.xml`, que contém o recurso da web que você utiliza ao se conectar à grade de dados remotamente.

```
<server description="Airport Entry eXtremeScale Getting Started Client Web Server">
<!--
 This sample program is provided AS IS and may be used, executed, copied and modified
 without royalty payment by customer
 (a) for its own instruction and study,
 (b) in order to develop applications designed to run with an IBM WebSphere product,
 either for customer's own internal use or for redistribution by customer, as part of such an
 application, in customer's own products.
 Licensed Materials - Property of IBM
 5724-X67, 5655-V66 (C) COPYRIGHT International Business Machines Corp. 2012
-->
    <!-- Enable features -->
    <featureManager>
        <feature>servlet-3.0</feature>
        <feature>jsp-2.2</feature>
        <feature>eXtremeScale.web-1.1</feature>
    </featureManager>

    <httpEndpoint id="defaultHttpEndpoint"
```

```
        host="*"
        httpPort="${default.http.port}"
        httpsPort="${default.https.port}" />

    <xsWebAppV85 objectGridType="REMOTE" objectGridName="session" catalogHostPort="remoteHost:2809" securityEnabled="false" />

</server>
```

Módulo 4: Configurar Clientes para Usar APIs do Cliente no Perfil do Liberty

É possível configurar seus clientes WebSphere eXtreme Scale para execução no perfil do Liberty.

Objetivos do aprendizado

Após concluir a lição neste módulo, você saberá como:

- Configurar o perfil do Liberty para execução com clientes eXtreme Scale.

Pré-requisitos

Para concluir este módulo, você deve concluir os seguintes módulos primeiro:

- Instalar o perfil do Liberty.
- Criar um servidor de aplicativos da web no perfil do Liberty.
- Incluir o Recurso da Web do Liberty no aplicativo da web.

Lição 4.1: Configurar o Perfil do Liberty para Executar com Clientes do eXtreme Scale

Utilize o recurso cliente do WebSphere eXtreme Scale para executar o perfil do Liberty com clientes do eXtreme Scale.

Esta configuração fornece apenas a funcionalidade do cliente. Neste aplicativo, a função do servidor é executada em outro processo. A inclusão do recurso do cliente permite que seu aplicativo acesse as APIs do eXtreme Scale e se conecte a uma grade remota.

Esta configuração do cliente fornece um processo único que inclui o que você precisa para teste de unidade de um aplicativo da web utilizando uma grade de dados do eXtreme Scale. Quando você inclui o recurso do cliente, ele inicia um servidor de catálogo e um servidor de contêiner quando a configuração é implementada no diretório da grade. Além disso, após você incluir o recurso cliente, o aplicativo pode gravar nas APIs do eXtreme Scale.

1. Inclua o recurso cliente no servidor do Liberty. Inclua o seguinte código no servidor do Liberty: **8.6+**

```
<server description="eXtreme Scale Container Server">

<featureManager>
<feature>eXtremeScale.client-1.1</feature>
</featureManager>


</server>
```

2. (Opcional) Como alternativa, você pode utilizar o recurso do servidor eXtreme Scale para fazer referência à configuração do cliente. Ao incluir a configuração do servidor a seguir, a funcionalidade do cliente é automaticamente incluída: **8.6+**

```
<server description="eXtreme Scale Container Server">

<featureManager>
<feature>eXtremeScale.server-1.1</feature>
</featureManager>


</server>
```

3. (Opcional) Para configurar a segurança para seus clientes, use o arquivo `client.xml` para especificar o caminho para o arquivo de propriedades de servidor, que contém todas as configurações de segurança. Para obter mais informações, consulte Configurando a Segurança do Cliente em um Domínio de Serviço de Catálogo.

Você configurou o perfil do Liberty incluindo o recurso do cliente no servidor do Liberty.

Módulo 5: Executar a Grade de Dados Dentro do Perfil do Liberty

Depois de incluir as configurações do cliente e do servidor no perfil do Liberty, é possível executar WebSphere eXtreme Scale no perfil do Liberty.

Objetivos do aprendizado

Após concluir as lições neste módulo, você saberá como concluir as tarefas a seguir:

- Configurar servidores eXtreme Scale para usar o perfil do Liberty.
- Configurar um servidor de aplicativos da web do perfil do Liberty para usar o eXtreme Scale para replicação de sessão..

Pré-requisitos

Para concluir este módulo, você deve concluir os módulos a seguir neste tutorial:

- Instalar o perfil do Liberty.
- Criar um servidor de aplicativos da web no Liberty.
- Incluir o recurso da web do perfil do Liberty no aplicativo da web.
- Configurar clientes para usar APIs do cliente no perfil do Liberty.

Lição 5.1: Configurar Servidores eXtreme Scale para Utilizar o Perfil do Liberty

Para executar a grade de dados em um perfil do Liberty, você deve incluir o recurso do servidor para configurar servidores WebSphere eXtreme Scale que usam arquivos de configuração de perfil do Liberty.

1. Configure um servidor de catálogos com as configurações padrão usando os atributos a seguir no arquivo `server.xml`, que informa ao eXtreme Scale para criar e iniciar um servidor de catálogos:

```
<server description="eXtreme Scale Catalog Server with default settings">

    <!-- Enable features -->
    <featureManager>
        <feature>eXtremeScale.server-1.1</feature>
    </featureManager>

    <xsServer isCatalog="true" listenerPort="${com.ibm.ws.xs.server.listenerPort}" />
```

```
    <logging traceSpecification="*=info" maxFileSize="200" maxFiles="10" />

</server>
```

Observe que o elemento listenerPort é referenciado no `server.xml`; no entanto, configure esse valor no arquivo `bootstrap.properties`. Pode ser útil separar elementos tais como números de porta fora do arquivo `server.xml` para que diversos processos que são executados com uma configuração idêntica possam compartilhar o arquivo `server.xml`, mas ainda tenham configurações exclusivas.

2. Configure o atributo listenerPort no arquivo `bootstrap.properties`.

   No exemplo anterior, o rastreio é especificado na configuração do perfil do Liberty e o atributo listenerPort especifica uma variável. Essa variável é configurada no arquivo `bootstrap.properties` no diretório de configuração do servidor, *`wlp_install_root`*`/usr/server/serverName`. Consulte o exemplo a seguir do arquivo `bootstrap.properties`:

   ```
   # Materiais Licenciados - Propriedade da IBM
   #
   # "Restricted Materials of IBM"
   #
   # Copyright IBM Corp. 2011 All Rights Reserved.
   #
   # US Government Users Restricted Rights - Use, duplication or
   # disclosure restricted by GSA ADP Schedule Contract with
   # IBM Corp.
   #
   # ------------------------------------------------------------------
   #
   # port for the OSGi console
   # osgi.console=5678

   com.ibm.ws.xs.server.listenerPort=2809
   ```

   Neste exemplo, a porta osgi.console está comentada, o que significa que o perfil do Liberty recebe na porta especificada para que os clientes telnet se conectem a um console OSGi. Este comportamento é útil para diagnosticar erros relacionados ao OSGi.

3. Configure o arquivo `server.xml` usando a mesma configuração que você pode usar para uma configuração do servidor independente. No arquivo `server.xml`, especifique o caminho do arquivo para o arquivo de propriedades em um atributo serverProps dentro do elemento com.ibm.ws.xs.server.config. Consulte o exemplo a seguir a partir do arquivo `server.xml`:

   ```
   <server>
   ...
   <com.ibm.ws.xs.server.config ... serverProps="/path/to/myServerProps.properties" ... />
   </server>
   ```

   Restrição: O modelo de configuração Liberty tem restrições na maneira como as propriedades são especificadas. Portanto, se precisar das propriedades a seguir, você deve especificá-las no arquivo de propriedades de servidor:

   *`foreignDomain`***`.endpoints`**
   Especifica os nomes de domínios de serviço de catálogo aos quais você deseja vincular na topologia de replicação multimaster.

   *`xioChannel`***`.xioContainerTCPNonSecure.Port`**
   Especifica o número de porta do listener descoberta do eXtremeIO no servidor. Se esse valor não for configurado, uma porta temporária será usada. Essa propriedade é usada somente quando a propriedade

transportType é configurada como `TCP/IP`.
`xioChannel.xioContainerTCPSecure.Port`.

Algumas propriedades que eram configuráveis anteriormente em um ambiente independente devem ser configuradas com a configuração de perfil do Liberty em vez dos mecanismos de configuração do eXtreme Scale.

- As configurações de criação de log e rastreio devem ser especificadas com o elemento de criação de log no arquivo `server.xml`, em vez de serem especificadas no arquivo de propriedades de servidor eXtreme Scale ou no elemento com.ibm.ws.xs.server.config. Para obter mais informações, consulte Perfil do Liberty: Rastreio e Criação de Log no Centro de Informações do WebSphere Application Server.
- O diretório ativo, como criação de log e rastreio, é uma configuração do lado do servidor e, portanto, deve ser especificado em todo o servidor.

Se as configurações anteriores estiverem incorretamente especificadas, o eXtreme Scale registrará em log uma mensagem de aviso, que indica que as configurações são ignoradas.

4. (Opcional) Para configurar a segurança com seus servidores, use o arquivo `server.xml` para especificar o caminho para o arquivo de propriedades do servidor, que contém todas as configurações de segurança. Quando o WebSphere eXtreme Scale é implementado em um ambiente do WebSphere Application Server, é possível simplificar o fluxo de autenticação e a configuração de segurança da camada de transporte do WebSphere Application Server. Para obter mais informações, consulte Integração de Segurança com o WebSphere Application Server.

Seus servidores eXtreme Scale estão prontos para execução no perfil do Liberty.

Conceitos relacionados:

"Perfil do Liberty" na página 39
O Perfil do Liberty é um ambiente de tempo de execução do servidor de aplicativos dinâmico de alta possibilidade de composição e de rápida inicialização.

Referências relacionadas:

Propriedades do Servidor de Perfis do Liberty
Utilize as opções do arquivo de propriedades do servidor para configurar os servidoresWebSphere eXtreme Scale que são executados no Perfil do Liberty.

Lição 5.2: Configurando um Servidor de Aplicativos da Web do Perfil do Liberty para Utilizar o eXtreme Scale para a Replicação de Sessão

É possível configurar um servidor de aplicativos da web para que, quando o servidor da web receber uma solicitação de HTTP para replicação de sessão, a solicitação seja encaminhada para o perfil do Liberty.

O perfil do Liberty não inclui replicação de sessão. No entanto, se você usar o WebSphere eXtreme Scale com o perfil do Liberty, poderá replicar sessões. Portanto, se um servidor falhar, os usuários do aplicativo não perderão dados da sessão.

Ao incluir o recurso webapp na definição do servidor e configurar o gerenciador de sessões, é possível usar a replicação de sessão em seus aplicativos eXtreme Scale executados no perfil do Liberty.

1. Ative o recurso da sessão HTTP no perfil do Liberty.
2. Configure um ID de clone exclusivo no arquivo server.xml do Liberty.

3. Gere e mescle arquivos de configuração do plug-in para implementação no plug-in do servidor de aplicativos.

Seus aplicativos eXtreme Scale que são executados no perfil do Liberty são ativados para replicação de sessão.

Tutorial: Integrar a Segurança do WebSphere eXtreme Scale com o WebSphere Application Server

Este tutorial demonstra como proteger uma implementação do servidor WebSphere eXtreme Scale em um ambiente do WebSphere Application Server.

Objetivos do aprendizado

Os objetivos do aprendizado para este tutorial são:

- Configurar o WebSphere eXtreme Scale para usar os plug-ins de autenticação do WebSphere Application Server
- Configurar a segurança de transporte do WebSphere eXtreme Scale para usar a configuração do WebSphere Application Server CSIv2
- Usar a autorização do Java Authentication and Authorization Service (JAAS) no WebSphere Application Server
- Usar um módulo de login customizado para a autorização JAAS baseada em grupo
- Usar o utilitário WebSphere eXtreme Scale **xscmd** no ambiente do WebSphere Application Server

Tempo Necessário

Este tutorial leva cerca de 4 horas do início ao fim.

Introdução: Integre a Segurança do WebSphere eXtreme Scale com o WebSphere Application Server usando os Plug-ins do WebSphere Application Server Authentication

Neste tutorial, integre a segurança do WebSphere eXtreme Scale com o WebSphere Application Server. Primeiro, configure a autenticação com um aplicativo da web simples que usa as credenciais do usuário autenticado a partir do encadeamento atual para se conectar ao ObjectGrid. Em seguida, investigue a criptografia dos dados que são transferidos entre o cliente e o servidor com a segurança da camada de transporte. Para conceder aos usuários diversos níveis de permissões, o Java Authentication and Authorization Service (JAAS) pode ser configurado. Depois de concluir a configuração, será possível usar o utilitário **xscmd** para monitorar suas grades de dados e mapas.

Este tutorial assume que todas os os clientes, servidores de contêineres e servidores de catálogos do WebSphere eXtreme Scale são implementados no ambiente do WebSphere Application Server.

Objetivos do aprendizado

Os objetivos do aprendizado para este tutorial são:

- Configurar o WebSphere eXtreme Scale para usar os plug-ins de autenticação do WebSphere Application Server

- Configurar a segurança de transporte do WebSphere eXtreme Scale para usar a configuração do WebSphere Application Server CSIv2
- Usar a autorização do Java Authentication and Authorization Service (JAAS) no WebSphere Application Server
- Usar um módulo de login customizado para a autorização JAAS baseada em grupo
- Usar o utilitário WebSphere eXtreme Scale **xscmd** no ambiente do WebSphere Application Server

Tempo Necessário

Este tutorial leva cerca de 4 horas do início ao fim.

Nível de qualificação

Intermediário.

Público

Desenvolvedores e administradores interessados na integração de segurança entre o WebSphere eXtreme Scale e o WebSphere Application Server.

Requisitos do Sistema e Topologia

- WebSphere Application Server Versão 7.0.0.11 ou posterior
- Atualize o tempo de execução Java para aplicar a seguinte correção: IZ79819: IBMJDK FALHA AO LER A INSTRUÇÃO PRINCIPAL COM ESPAÇO EM BRANCO A PARTIR DO ARQUIVO DE SEGURANÇA

Este tutorial usa quatro servidores de aplicativos WebSphere Application Server e um gerenciador de implementação para demonstrar a amostra.

Pré-requisitos

Um entendimento básico dos seguintes itens é útil antes de iniciar este tutorial:

- Modelo de programação do WebSphere eXtreme Scale
- Conceitos básicos a segurança do WebSphere eXtreme Scale
- Conceitos básicos a segurança do WebSphere Application Server

Para obter informações complementares sobre o WebSphere eXtreme Scale e sobre a integração de segurança do WebSphere Application Server, consulte “Integração de Segurança com o WebSphere Application Server” na página 794.

Conceitos relacionados:

“Visão Geral de Segurança” na página 304
WebSphere eXtreme Scale pode proteger o acesso a dados, incluindo permissão para integração com provedores de segurança externos.

Informações relacionadas:

WebSphere Application Server: Protegendo Aplicativos e Seu Ambiente

Módulo 1: Preparar o WebSphere Application Server

Antes de iniciar o tutorial para integração com o WebSphere eXtreme Scale, você deve criar uma configuração de segurança básica no WebSphere Application Server.

Objetivos do aprendizado

Com as lições neste módulo, você aprende como:

- Configurar a segurança do WebSphere Application Server para usar um repositório federado baseado em arquivo interno como um registro de conta do usuário.
- Criar grupos de usuários e usuários.
- Criar clusters para os servidores de aplicativos e do WebSphere eXtreme Scale.

Tempo Necessário

Este módulo leva cerca de 60 minutos.

Lição 1.1: Entendendo a Topologia e Obtendo os Arquivos do Tutorial

Para preparar seu ambiente para o tutorial, você deve configurar a segurança do WebSphere Application Server. Configure a segurança de administração e do aplicativo usando os repositórios federados baseados em arquivo interno como um registro de conta do usuário.

Essa lição o orienta pela topologia de amostra e pelos aplicativos que são usados no tutorial. Para começar a executar o tutorial, você deve fazer download dos aplicativos e colocar os arquivos de configuração nos locais corretos para seu ambiente. É possível fazer download do aplicativo de amostra a partir do Wiki do WebSphere eXtreme Scale.

Topologia de Amostra do WebSphere Application Server: Este tutorial guia você na criação de quatro servidores de aplicativos do WebSphere Application Server para demonstrar como usar os aplicativos de amostra com a segurança ativada. Esses servidores de aplicativos são agrupados em dois clusters, cada um com dois servidores:

- **Cluster appCluster**: Hospeda o aplicativo corporativo da amostra EmployeeManagement. Esse cluster possui dois servidores de aplicativos: s1 e s2.
- **Cluster xsCluster**: Hospeda os servidores de contêiner do eXtreme Scale. Esse cluster possui dois servidores de aplicativos: xs1 e xs2.

Nessa topologia de implementação, os servidores de aplicativos s1 e s2 são os servidores de cliente que acessam dados que estão sendo armazenados na grade de dados. Os servidores xs1 e xs2 são os servidores de contêiner que hospedam a grade de dados.

O servidor de catálogos é implementado no processo do gerenciador de implementação por padrão. Este tutorial usa o comportamento padrão. Hospedar o servidor de catálogos no gerenciador de implementação não é uma prática recomendada em um ambiente de produção. Em um ambiente de produção, você deve criar um domínio de serviço de catálogo para definir onde os servidores de catálogos iniciam. Consulte Criando Domínios do Serviço de Catálogo no WebSphere Application Server para obter mais informações.

Configuração alternativa: É possível hospedar todos os servidores de aplicativos em um único cluster, como no cluster appCluster. Com essa configuração, todos os servidores no cluster são ambos servidores de clientes e servidores de contêiner. Este tutorial usa dois clusters para distinguir entre os servidores de aplicativos que

hospedam os servidores de clientes e de contêiner.

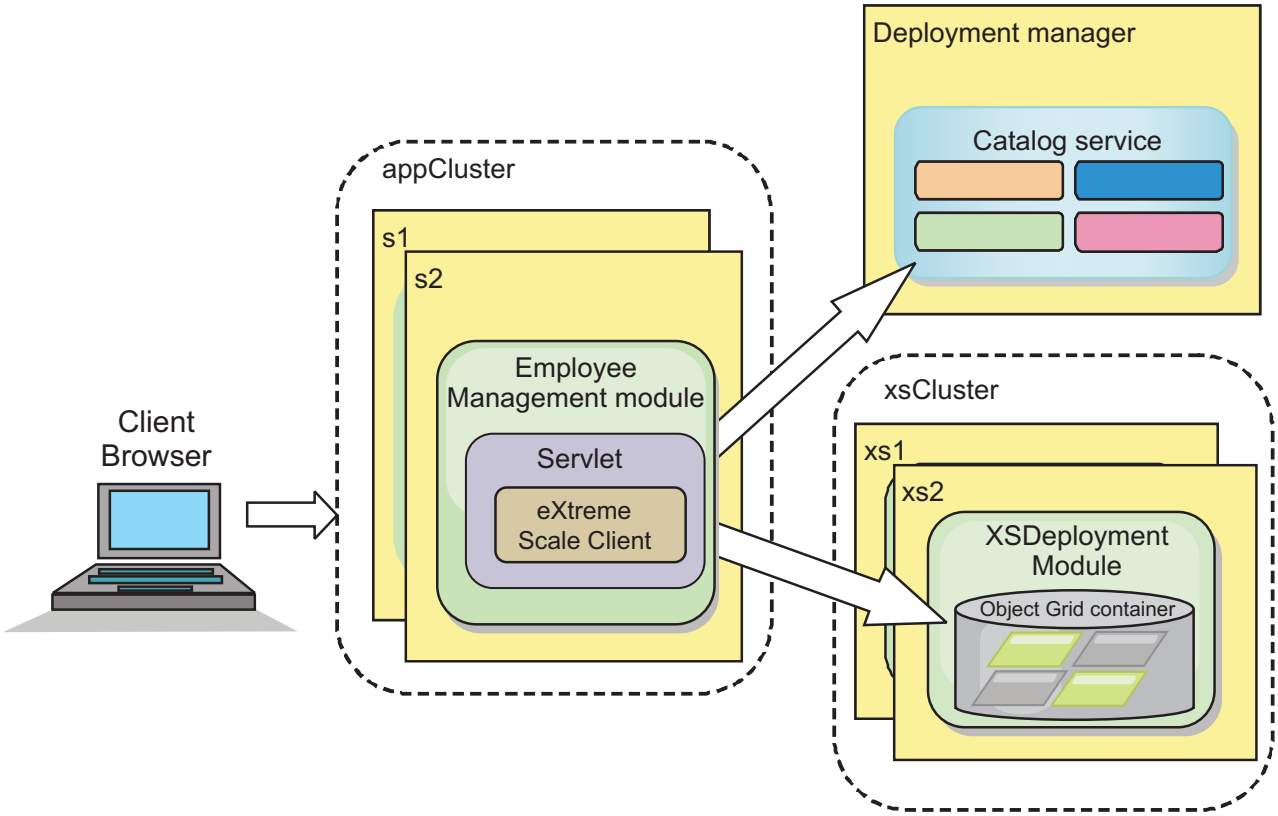


Figura 3. Topologia do Tutorial

Aplicativos: Neste tutorial, você está usando dois aplicativos e um arquivo de biblioteca compartilhado:

- **`EmployeeManagement.ear`**: O aplicativo `EmployeeManagement.ear` é um aplicativo corporativo simplificadodo Java 2 Platform, Enterprise Edition (J2EE). Ele contém um módulo da web para gerenciar os perfis dos funcionários. O módulo da web contém o arquivo `management.jsp` para exibir, inserir, atualizar e excluir perfis de funcionários que são armazenados nos servidores de contêiner.
- **`XSDeployment.ear`**: Este aplicativo contém um módulo de aplicativo corporativo sem nenhum artefato do aplicativo. Os objetos de cache são compactados no arquivo `EmployeeData.jar`. O arquivo `EmployeeData.jar` é implementado como uma biblioteca compartilhada para o arquivo `XSDeployment.ear`, de modo que o arquivo `XSDeployment.ear` possa acessar as classes. O propósito deste aplicativo é compactar os arquivos de configuração do eXtreme Scale . Quando este aplicativo corporativo é iniciado, os arquivos de configuração do eXtreme Scale são automaticamente detectados pelo tempo de execução do eXtreme Scale, portanto, os servidores de contêiner são criados. Esses arquivos de configuração incluem os arquivos `objectGrid.xml` e `objectGridDeployment.xml`.
- **`EmployeeData.jar`**: Este arquivo jar contém uma classe: a classe com.ibm.websphere.sample.xs.data.EmployeeData. Esta classe representa dados do funcionário que são armazenados na grade. Este arquivo Java Archive (JAR) é implementado com os arquivos `EmployeeManagement.ear` e `XSDeployment.ear` como uma biblioteca compartilhada.

Obter os Arquivos do Tutorial:

1. Faça download dos arquivos WASSecurity.zip e security.zip. É possível fazer download do aplicativo de amostra a partir do Wiki do WebSphere eXtreme Scale.
2. Extraia o arquivo WASSecurity.zip em um diretório para visualizar o binário e os artefatos de origem, por exemplo, o diretório /wxs_samples/. Esse diretório é referido como *samples_home* para o restante do tutorial. Para obter uma descrição do conteúdo do arquivo WASSecurity.zip e de como carregar a origem na área de trabalho do Eclipse, consulte o arquivo README.txt no pacote.
3. Extraia o arquivo security.zip no diretório *samples_home*. O arquivo security.zip contém os seguintes arquivos de configuração de segurança que são usados neste tutorial:
   - catServer2.props
   - server2.props
   - client2.props
   - securityWAS2.xml
   - xsAuth2.props

Sobre os Arquivos de Configuração:

Os arquivos objectGrid.xml e objectGridDeployment.xml criam as grades de dados e mapas que armazenam os dados do aplicativo.

Esses arquivos de configuração devem ser nomeados como objectGrid.xml e objectGridDeployment.xml. Quando o servidor de aplicativos é iniciado, o eXtreme Scale detecta estes arquivos no diretório META-INF dos módulos EJB e da web. Se estes arquivos forem localizados, supõe-se que a Java virtual machine (JVM) atua como um servidor de contêiner para as grades de dados definidas nos arquivos de configuração.

Arquivo objectGrid.xml

O arquivo objectGrid.xml define um ObjectGrid denominado Grid. A grade de dados Grid tem um mapa, o mapa Map1, que armazena o perfil do funcionário para o aplicativo.

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">

 <objectGrids>
        <objectGrid name="Grid" txTimeout="15">
            <backingMap name="Map1" />
        </objectGrid>
    </objectGrids>

</objectGridConfig>
```

Arquivo objectGridDeployment.xml

O arquivo objectGridDeployment.xml especifica como implementar a grade de dados Grid. Quando a grade é implementada, ela tem cinco partições e uma réplica síncrona.

```
<?xml version="1.0" encoding="UTF-8"?>

<deploymentPolicy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/deploymentPolicy ../deploymentPolicy.xsd"
 xmlns="http://ibm.com/ws/objectgrid/deploymentPolicy">
```

```
    <objectgridDeployment objectgridName="Grid">
        <mapSet name="mapSet" numberOfPartitions="5" minSyncReplicas="0"
maxSyncReplicas="1" >"1" >
            <map ref="Map1"/>
        </mapSet>
    </objectgridDeployment>

</deploymentPolicy>
```

Ponto de verificação de lições:

Nesta lição, você aprendeu sobre a topologia do tutorial e incluiu os arquivos de configuração e os aplicativos de amostra no seu ambiente.

Se desejar saber mais sobre como iniciar automaticamente os servidores de contêiner, consulte Configurando os Aplicativos do WebSphere Application Server para Iniciar Automaticamente os Servidores de Contêiner.

Lição 1.2: Configurar o Ambiente do WebSphere Application Server

Para preparar seu ambiente para o tutorial, você deve configurar a segurança do WebSphere Application Server. Ative a segurança de administração e do aplicativo usando repositórios federados baseados em arquivo internos como um registro de conta do usuário. Em seguida, é possível criar clusters de servidores para hospedar o aplicativo cliente e os servidores de contêiner.

As seguintes etapas foram gravadas usando o WebSphere Application Server Versão 7.0. No entanto, também podem ser aplicados os conceitos que se aplicam às versões anteriores do WebSphere Application Server.

Configurar a Segurança do WebSphere Application Server:

1. Configure a segurança do WebSphere Application Server.
   a. No console administrativo do WebSphere Application Server, clique em **Segurança** > **Segurança Global**.
   b. Selecione **Repositórios Federados** como a **Definição da Região Disponível**. Clique em **Configurar como atual**.
   c. Clique em **Configurar...** para acessar o painel Repositórios Federados.
   d. Digite o **Nome do usuário administrativo principal**, por exemplo, `admin`. Clique em **Aplicar.**
   e. Quando solicitado, digite a senha do usuário administrativo e clique em **OK**. Salve as alterações.
   f. Na página **Segurança Global**, verifique se a configuração de **Repositórios Federados** está definida para o registro de conta do usuário atual.
   g. Selecione os seguintes itens: **Ativar Segurança Administrativa**, **Ativar Segurança do Aplicativoe Usar segurança Java 2 para restringir o acesso do aplicativo aos recursos locais** . Clique em **Aplicar** e salve suas alterações.
   h. Reinicie o gerenciador de implementação e quaisquer servidores de aplicativo em execução.

   A Segurança Administrativa do WebSphere Application Server é ativada usando os repositórios federados baseados em arquivo internos como o registro de conta do usuário.
2. Crie dois grupos: adminGroup e operatorGroup.
   a. Clique em **Usuários e Grupos** > **Gerenciar grupos** > **Criar...**

b. Digite adminGroup como o nome do grupo. Insira Grupo de Administração como a descrição. Clique em **Criar**.
c. Clique em **Criar semelhante**. Digite operatorGroup como o nome do grupo. Insira Grupo de Operador como a descrição. Clique em **Criar**.
d. Clique em **Fechar**.

3. Crie usuários admin1 e operator1.
   a. Clique em **Usuários e Grupos** > **Gerenciar Usuários** > **Criar...**
   b. Crie um usuário chamado admin1 com o nome Joe e o sobrenome Doe com a senha do admin1. Clique em **Criar**.
   c. Crie um segundo usuário. Clique em **Criar semelhante** para criar um usuário chamado operator1 com o nome Jane e sobrenome Doe com a senha do operator1. Clique em **Criar**. Clique em **Fechar**.
4. Inclua usuários nos grupos de usuários. Inclua o usuário admin1 no adminGroup e o usuário operador1 no operatorGroup.
   a. Clique em **Usuários e Grupos** > **Gerenciar Usuários**
   b. Procure por usuários para incluir nos grupos. Clique em **Procurar.** e configure a procura de valor como um asterisco (*) para exibir todos os usuários.
   c. No resultado da procura, clique no usuário admin1 e clique na guia **Grupos**. Clique em **Incluir** para incluir o grupo.
   d. Procure pelos grupos para localizar os grupos disponíveis. Clique em adminGroup e depois em **Incluir**.
   e. Repita essas etapas para incluir o usuário operador1 no grupo de usuários operatorGroup.
5. Salve suas mudanças, efetue logout do console administrativo e reinicie o gerenciador de implementação e o agente do nó para ativar as configurações de segurança.

Você ativou a segurança e criou usuários e grupos de usuários que possuem acesso administrativo e de operador à sua configuração do WebSphere Application Server .

Criar Clusters de Servidores:

Crie dois clusters de servidores em sua configuração do WebSphere Application Server: O cluster appCluster para hospedar o aplicativo de amostra do tutorial e o cluster xsCluster para hospedar a grade de dados.

1. No console administrativo do WebSphere Application Server, abra o painel de clusters. Clique em **Servidores** > **Clusters** > **Clusters de Servidores de Aplicativos do WebSphere** > **Novo**.
2. Digite appCluster como o nome do cluster, deixe a opção **Preferir local** selecionada e clique em **Avançar**.
3. Crie servidores no cluster. Crie um servidor denominado s1, mantendo as opções padrão. Inclua um membro de cluster adicional denominado s2.
4. Conclua as etapas restantes no assistente para criar o cluster. Salve as mudanças.
5. Repita essas etapas para criar o cluster xsCluster. Este cluster possui dois servidores denominados xs1 e xs2.

Ponto de verificação de lições:

Você ativou a segurança global para a célula do WebSphere Application Server, criou usuários e grupos de usuários e criou clusters para hospedar o aplicativo e a grade e dados.

Módulo 2: Configurar o WebSphere eXtreme Scale para Usar os Plug-ins de Autenticação do WebSphere Application Server

Após criar a configuração do WebSphere Application Server, será possível integrar a autenticação do WebSphere eXtreme Scale com o WebSphere Application Server.

Quando um cliente do WebSphere eXtreme Scale se conecta a um servidor de contêiner que requer autenticação, o cliente deve fornecer um gerador de credencial representado pela interface com.ibm.websphere.objectgrid.security.plugins.CredentialGenerator . Um gerador de credenciais é um factory para criar uma credencial do cliente. Uma credencial de cliente pode ser: um par nome de usuário e senha, um ticket do Kerberos, um certificado de cliente ou dados de identificação de cliente em qualquer formato concordado entre o cliente e o servidor. Consulte o Documentação da API de Credencial para obter mais detalhes. Nessa amostra, o cliente do WebSphere eXtreme Scale é o aplicativo da web EmployeeManagment que é implementado no cluster appCluster. A credencial do cliente é um token de segurança do WebSphere que representa a identidade do usuário da web.

Objetivos do aprendizado

Com as lições neste módulo, você aprende como:

- Configurar a segurança do servidor de cliente.
- Configurar a segurança do servidor de catálogos.
- Configurar a segurança do servidor de contêiner.
- Instale e execute o aplicativo de amostra.

Tempo Necessário

Este módulo leva cerca de 60 minutos.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Informações relacionadas:

"Lição 2.1: Configurar a Segurança do Servidor do Cliente"
O arquivo de propriedades do cliente indica a classe de implementação CredentialGenerator a ser usada.

Documentação da API de Credencial

"Lição 2.2: Configurar a Segurança do Servidor de Catálogos" na página 56
Um servidor de catálogos contém dois níveis de informações de segurança: As propriedades de segurança que são comuns a todos os servidores do WebSphere eXtreme Scale, incluindo o serviço de catálogo e os servidores de contêiner, e as propriedades de segurança que são específicas ao servidor de catálogos.

Lição 2.1: Configurar a Segurança do Servidor do Cliente

O arquivo de propriedades do cliente indica a classe de implementação CredentialGenerator a ser usada.

Configure o arquivo de propriedades do cliente com a propriedade da JVM **-Dobjectgrid.client.props**. O nome do arquivo especificado para esta propriedade é um caminho de arquivo absoluto, como *samples_home*/tmp/security/client2.props. Consulte Arquivo de Propriedades do Cliente para obter mais informações sobre o arquivo de propriedades do cliente.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Informações relacionadas:

"Módulo 2: Configurar o WebSphere eXtreme Scale para Usar os Plug-ins de Autenticação do WebSphere Application Server" na página 54
Após criar a configuração do WebSphere Application Server, será possível integrar a autenticação do WebSphere eXtreme Scale com o WebSphere Application Server.

Documentação da API de Credencial

Conteúdo do Arquivo de Propriedades do Cliente:
Este exemplo usa os tokens de segurança do WebSphere Application Server como a credencial do cliente. O arquivo client2.props está no diretório *samples_home*/security. O arquivo client2.props inclui as seguintes configurações.

securityEnabled
Quando configurado para true, indica que o cliente deve enviar informações de segurança disponíveis para o servidor.

credentialAuthentication
Quando configurado para Suportado, indica que o cliente suporta a autenticação de credencial.

credentialGeneratorClass

Indica a classe com.ibm.websphere.objectgrid.ssecurity.plugins.builtins.WSTokenCredentialGenerator para que o cliente recupere os tokens de segurança a partir do encadeamento. Consulte o "Integração de Segurança com o WebSphere Application Server" na página 794 para obter mais informações sobre como os tokens de segurança são recuperados.

Configurando o Arquivo de Propriedades do Cliente Usando as Propriedades da Java virtual machine (JVM):

No console administrativo, conclua as seguintes etapas para ambos servidores `s1` e `s2` no cluster `appCluster`. Se uma topologia diferente estiver sendo usada, conclua as seguintes etapas para todos os servidores de aplicativos nos quais o aplicativo `EmployeeManagement` é implementado.

1. **Servidores** > **Servidores de aplicativo WebSphere** > *server_name* > **Java and Process Management** > **Definição de processo** > **Java Virtual Machine**.
2. Crie a seguinte propriedade JVM genérica para configurar o local do arquivo de propriedades do cliente:

   `-Dobjectgrid.client.props=`*`samples_home`*`/security/client2.props`
3. Clique em **OK** e salve as mudanças.

Ponto de verificação de lições:

Você editou o arquivo de propriedades do cliente e configurou os servidores no cluster `appCluster` para usar o arquivo de propriedades do cliente. Este arquivo de propriedades indica a classe de implementação CredentialGenerator a ser usada.

Lição 2.2: Configurar a Segurança do Servidor de Catálogos

Um servidor de catálogos contém dois níveis de informações de segurança: As propriedades de segurança que são comuns a todos os servidores do WebSphere eXtreme Scale, incluindo o serviço de catálogo e os servidores de contêiner, e as propriedades de segurança que são específicas ao servidor de catálogos.

As propriedades de segurança que são comuns aos servidores de catálogos e aos servidores de contêiner são configuradas no arquivo descritor XML de segurança. Um exemplo das propriedades comuns é a configuração do autenticador, que representa o registro do usuário e o mecanismo de autenticação. Consulte o Arquivo XML Descritor de Segurança para obter mais informações sobre as propriedades de segurança.

Para configurar o arquivo descritor XML de segurança, crie uma propriedade -Dobjectgrid.cluster.security.xml.url no argumento Java virtual machine (JVM). O nome do arquivo especificado para esta propriedade deve estar em um formato de URL, como `file:///`*`samples_home`*`/security/securityWAS2.xml`.

Referências relacionadas:

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Informações relacionadas:

"Módulo 2: Configurar o WebSphere eXtreme Scale para Usar os Plug-ins de Autenticação do WebSphere Application Server" na página 54
Após criar a configuração do WebSphere Application Server, será possível integrar a autenticação do WebSphere eXtreme Scale com o WebSphere Application Server.

Arquivo securityWAS2.xml:

Neste tutorial, o arquivo `securityWAS2.xml` está no diretório *samples_home*/`security`. O conteúdo do arquivo `securityWAS2.xml` com os comentários removidos é o seguinte:

```
<securityConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config/security
../objectGridSecurity.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config/security">

 <security securityEnabled="true">
  <authenticator
 className="com.ibm.websphere.objectgrid.security.plugins.builtins.WSTokenAuthenticator">
  </authenticator>
 </security>
</securityConfig>
```

As seguintes propriedades são definidas no arquivo `securityWAS2.xml`:

securityEnabled
: A propriedade securityEnabled é configurada para `true`, indicando que a segurança global do WebSphere eXtreme Scale do servidor de catálogos foi ativada.

autenticador
: O autenticador é configurado como a classe com.ibm.websphere.objectgrid.security.plugins.builtins.WSTokenAuthenticator. Com essa implementação integrada do plug-in Autenticador, o servidor WebSphere eXtreme Scale pode converter os tokens de segurança em um objeto Subject. Consulte o "Integração de Segurança com o WebSphere Application Server" na página 794 para obter mais informações sobre como os tokens de segurança são convertidos.

Arquivo catServer2.props:

O arquivo de propriedades do servidor armazena as propriedades específicas do servidor, dentre elas as propriedades de segurança específicas do servidor. Consulte o Arquivo de Propriedades do Servidor para obter informações adicionais. O arquivo de propriedades do servidor pode ser configurado com a propriedade `-Dobjectgrid.server.props` no argumento da JVM. O valor do nome do arquivo para essa propriedade é especificado como um caminho absoluto, como *samples_home*`/security/catServer2.props`. Para este tutorial, um arquivo `catServer2.props` está incluído no diretório *samples_home*`/security`. O conteúdo do arquivo `catServer2.props` com os comentários removidos é o seguinte:

securityEnabled
A propriedade securityEnabled é configurada para `true` para indicar que este servidor de catálogos é um servidor seguro.

credentialAuthentication
A propriedade credentialAuthentication é configurada para `Necessária`, portanto, qualquer cliente que esteja conectado ao servidor precisa fornecer uma credencial.

secureTokenManagerType
O secureTokenManagerType está configurado para `none` para indicar que o segredo da autenticação não é criptografado quando junta os servidores existentes.

authenticationSecret
A propriedade authenticationSecret está configurada para `ObjectGridDefaultSecret`. Esta sequência secreta é usada para juntar o cluster de servidores eXtreme Scale. Quando um servidor junta a grade de dados, ele é desafiado a apresentar a sequência secreta. Se a sequência secreta do servidor de junção corresponder à sequência no servidor de catálogos, o servidor de junção será aceito. Se a cadeia não corresponder, o pedido de junção é rejeitado.

transportType
A propriedade transportType é configurada inicialmente para `TCP/IP`. Posteriormente no tutorial, a segurança de transporte é ativada.

Configurando o arquivo de propriedades de servidor com propriedades JVM:

Configure o arquivo de propriedades do servidor no servidor do gerenciador de implementação. Se uma topologia diferente da topologia deste tutorial estiver sendo usada, configure o arquivo de propriedades do servidor para todos os servidores de aplicativos que estiverem sendo usados para hospedar servidores de contêiner.

1. Abra a configuração da Java virtual machine para o servidor. No console administrativo, clique em **Administração do Sistema** > **Gerenciador de Implementação** > **Gerenciamento Java e Processos** > **Definição de Processo** > **Java Virtual Machine**.
2. Inclua os seguintes argumentos JVM genéricos:

```
-Dobjectgrid.cluster.security.xml.url=file:///samples_home/security/securityWAS2.xml
-Dobjectgrid.server.props=samples_home/security/catServer2.props
```

3. Clique em **OK** e salve as mudanças.

Ponto de verificação de lições:

Você configurou a segurança do servidor de catálogos ao associar os arquivos `securityWAS2.xml` e `catServer2.props` com o gerenciador de implementação, que hospeda o processo do servidor de catálogos na configuração do WebSphere Application Server.

Lição 2.3: Configurar a Segurança do Servidor do Contêiner

Quando um servidor de contêiner se conecta ao serviço de catálogo, o servidor de contêiner obtém todas as configurações de segurança que estiverem definidas no arquivo XML ObjectGrid Security, como a configuração do autenticador, o valor do tempo limite de sessão de login e outras informações de configuração. Um servidor de contêiner também possui suas próprias propriedades de segurança específicas do servidor no arquivo de propriedade do servidor.

Configure o arquivo de propriedades do servidor com a propriedade `-Dobjectgrid.server.props` da Java virtual machine (JVM). O nome do arquivo especificado para esta propriedade é um caminho de arquivo absoluto, como *samples_home*`/security/server2.props`.

Neste tutorial, os servidores de contêiner são hospedados nos servidores `xs1` e `xs2` no cluster `xsCluster`.

Arquivo server2.props:

O arquivo `server2.props` está no diretório *samples_home*`/security` sob o diretório `WASSecurity`. As propriedades definidas no arquivo `server2.props` são:

securityEnabled
A propriedade securityEnabled é configurada para `true` para indicar que este servidor de contêiner é um servidor seguro.

credentialAuthentication
A propriedade credentialAuthentication é configurada para `Necessária`, portanto, qualquer cliente que esteja conectado ao servidor precisa fornecer uma credencial.

secureTokenManagerType
O secureTokenManagerType está configurado para `none` para indicar que o segredo da autenticação não é criptografado quando junta os servidores existentes.

authenticationSecret
A propriedade authenticationSecret está configurada para `ObjectGridDefaultSecret`. Esta sequência secreta é usada para juntar o cluster de servidores eXtreme Scale. Quando um servidor junta a grade de dados, ele é desafiado a apresentar a sequência secreta. Se a sequência secreta do servidor de junção corresponder à sequência no servidor de catálogos, o servidor de junção será aceito. Se a cadeia não corresponder, o pedido de junção é rejeitado.

Configurando o arquivo de propriedades de servidor com propriedades JVM:

Configure o arquivo de propriedades do servidor nos servidores xs1 e xs2. Se a topologia não estiver sendo usada para este tutorial, configure o arquivo de propriedades do servidor para todos os servidores de aplicativos que estiverem sendo usados para hospedar servidores de contêiner.

1. Abra a página da Java virtual machine para o servidor. **Servidores** > **Servidores de Aplicativos** > *server_name* > **Gerenciamento Java e Processos** > **Definição de Processo** > **Java Virtual Machine**.
2. Inclua os argumentos da JVM genéricos:
   `-Dobjectgrid.server.props=`*samples_home*`/security/server2.props`
3. Clique em **OK** e salve as mudanças.

Ponto de verificação de lições:

Agora, a autenticação do servidor WebSphere eXtreme Scale está protegida. Ao configurar esta segurança, todos os aplicativos que tentam se conectar com os servidores WebSphere eXtreme Scale são necessárias para fornecer uma credencial. Neste tutorial, o WSTokenAuthenticator é o autenticador. Como resultado, o cliente deverá fornecer um token de segurança do WebSphere Application Server.

Lição 2.4: Instalar e Executar a Amostra

Depois que a autenticação for configurada, o aplicativo de amostra poderá ser instalado e executado.

Criando uma Biblioteca Compartilhada para o Arquivo `EmployeeData.jar`:

1. No console administrativo do WebSphere Application Server, abra a página **Bibliotecas Compartilhadas**. Clique em **Ambiente** > **Bibliotecas Compartilhadas**.
2. Escolha o escopo **célula**.
3. Crie a biblioteca compartilhada. Clique em **Novo**. Insira `EmployeeManagementLIB` como o **Nome**. Insira o caminho para o arquivo `EmployeeData.jar` no caminho de classe, por exemplo, *samples_home*`/WASSecurity/EmployeeData.jar`.
4. Clique em **Aplicar**.

Instalando a Amostra:

1. Instale o arquivo `EmployeeManagement.ear`.
   a. Para iniciar a instalação, clique em **Aplicativos** > **Novo Aplicativo** > **Novo Aplicativo Corporativo**. Escolha o caminho detalhado para instalar o aplicativo.
   b. Na etapa **Mapear módulos para servidores**, especifique o cluster `appCluster` para instalar o módulo EmployeeManagementWeb.
   c. Na etapa **Mapear bibliotecas compartilhadas**, selecione o módulo `EmployeeManagementWeb`.
   d. Clique em **Referenciar bibliotecas compartilhadas**. Selecionar a biblioteca `EmployeeManagementLIB`.
   e. Mapeie a função `webUser` para **Tudo Autenticado na Região do Aplicativo**.
   f. Clique em **OK**.

   Os clientes são executados nos servidores `s1` e `s2` neste cluster.
2. Instale o arquivo de amostra `XSDeployment.ear`.
   a. Para iniciar a instalação, clique em **Aplicativos** > **Novo Aplicativo** > **Novo Aplicativo Corporativo**. Escolha o caminho detalhado para instalar o aplicativo.
   b. Na etapa **Mapear módulos para servidores**, especifique o cluster `xsCluster` para instalar o módulo da web `XSDeploymentWeb`.
   c. Na etapa **Mapear bibliotecas compartilhadas**, selecione o módulo `XSDeploymentWeb`.
   d. Clique em **Referenciar bibliotecas compartilhadas**. Selecionar a biblioteca `EmployeeManagementLIB`.
   e. Clique em **OK**.

   Os servidores `xs1` e `xs2` neste cluster hospedam os servidores de contêiner.
3. Reinicie o gerenciador de implementação. Quando o gerenciador de implementação é iniciado, o servidor de catálogos também inicia. Se observar o arquivo `SystemOut.log` do gerenciador de implementação, será possível ver a seguinte mensagem indicando que o arquivo de propriedades do servidor eXtreme Scale foi carregado.

   ```
   CWOBJ0913I: Os arquivos de propriedade de servidor foram carregados:
   /wxs_samples/security/catServer2.props.
   ```
4. Reinicie o cluster xsCluster. Quando o xsCluster é iniciado, o aplicativo `XSDeployment` é iniciado e um servidor de contêiner é iniciado nos servidores xs1 e xs2 respectivamente. Se você olhar o arquivo `SystemOut.log` dos

servidores xs1 e xs2, a seguinte mensagem que indica que o arquivo de propriedades do servidor foi carregado é exibida:

```
CWOBJ0913I: Os arquivos de propriedade de servidor foram carregados:
/wxs_samples/security/server2.props.
```

5. Reinicie o cluster appClusters. Quando o cluster appClusters é iniciado, o aplicativo EmployeeManagement também é iniciado. Se observar o arquivo `SystemOut.log` dos servidores s1 e s2, será possível ver a seguinte mensagem indicando que o arquivo de propriedades do cliente foi carregado.

   ```
   CWOBJ0924I: O arquivo de propriedades do cliente {0} foi carregado.
   ```

   As mensagens de aviso sobre as propriedades authenticationRetryCount, transportType, e clientCertificateAuthentication podem ser ignoradas. Os valores padrão devem ser usados porque os valores não foram especificados no arquivo de propriedades.Se estiver usando o WebSphere eXtreme Scale Versão 7.0, uma mensagem CWOBJ9000I somente em inglês será exibida para indicar que o arquivo de propriedades do cliente foi carregado. Se a mensagem esperada não for exibida, verifique se a propriedade -Dobjectgrid.server.props ou -Dobjectgrid.client.props foi configurada no argumento da JVM. Se as propriedades estiverem realmente configuradas, certifique-se de que o traço (-) seja um caractere UTF.

Executando o Aplicativo de Amostra:

1. Execute o arquivo `management.jsp`. Em um navegador da web, acesse `http://<your_servername>:<port>/EmployeeManagementWeb/management.jsp`. Por exemplo, é possível usar a seguinte URL: `http://localhost:9080/EmployeeManagementWeb/management.jsp`.
2. Forneça autenticação para o aplicativo. Insira as credenciais do usuário que foram mapeadas para a função webUser. Por padrão, essa função do usuário é mapeada para todos os usuários autenticados. Digite `admin1` como seu ID de usuário e `admin1` como a senha. Uma página para exibir, incluir, atualizar e excluir funcionários é exibida.
3. Exibir Funcionários Clique em **Exibir um Funcionário**. Insira `emp1@acme.com` como o endereço de email e clique em **Enviar**. Uma mensagem é exibida informando que o usuário não pode ser localizado.
4. Incluir um funcionário. Clique em **Incluir um Funcionário**. Insira `emp1@acme.com` como o endereço de email, insira `Joe` como o nome e insira `Doe` como o sobrenome. Clique em **Enviar**. Uma mensagem é exibida informando que um funcionário com o endereço `emp1@acme.com` foi incluído.
5. Exibir o novo funcionário. Clique em **Exibir um Funcionário**. Insira `emp1@acme.com` como o endereço de email com campos vazios para o nome e sobrenome e clique em **Enviar**. Uma mensagem é exibida informando que o funcionário foi localizado e que os nomes corretos são exibidos nos campos nome e sobrenome.
6. Excluir o funcionário. Clique em **Excluir um funcionário**. Insira `emp1@acme.com` e clique em **Enviar**. Uma mensagem é exibida informando que o funcionário foi excluído.

Ponto de verificação de lições:

Você instalou e executou o aplicativo de amostra. Como este tutorial usa a integração do WebSphere Application Server, não será possível ver o cenário quando um cliente falhar ao se autenticar no servidor eXtreme Scale. Se o usuário se autenticar no WebSphere Application Server com êxito, o eXtreme Scale também é autenticado com êxito.

Módulo 3: Configurar a Segurança de Transporte

Configure a segurança de transporte para proteger a transferência de dados entre os clientes e servidores na configuração.

No módulo anterior no tutorial, você ativou a autenticação do WebSphere eXtreme Scale. Com a autenticação, qualquer aplicativo que tentar se conectar com o servidor WebSphere eXtreme Scale precisará fornecer uma credencial. Portanto, nenhum cliente não autenticado pode se conectar com o servidor WebSphere eXtreme Scale. Os clientes devem ser um aplicativo autenticado que esteja em execução em uma célula do WebSphere Application Server.

Com a configuração até esse módulo, a transferência de dados entre os clientes no cluster appCluster e os servidores no cluster xsCluster não é criptografada. Essa configuração poderá ser aceitável apenas se seus clusters do WebSphere Application Server estiverem instalados em servidores por trás de um firewall. Entretanto, em alguns cenários, um tráfego não criptografado não é aceito por algumas razões, embora a topologia esteja protegida por um firewall. Por exemplo, uma política de controle pode aplicar o tráfego criptografado. O WebSphere eXtreme Scale suporta a Segurança da Camada de Transporte/Secure Sockets Layer (TLS/SSL) para uma comunicação segura entre os terminais do ObjectGrid, que incluem servidores de cliente, servidores de contêineres e servidores de catálogos.

Nesta implementação de amostra, os clientes e servidores de contêiner do eXtreme Scale estão todos executando no ambiente do WebSphere Application Server. As propriedades do cliente ou do servidor não são necessárias para definir as configurações SSL porque a segurança de transporte do eXtreme Scale é gerenciada pelas configurações de transporte do Common Secure Interoperability Protocol Versão 2 (CSIV2) do WebSphere Application Server. Os servidores do WebSphere eXtreme Scale usam a mesma instância do Object Request Broker (ORB) como os servidores de aplicativos nos quais eles são executados. Especifique todas as configurações de SSL para servidores de cliente e de contêiner na configuração do WebSphere Application Server usando estas configurações de transporte de CSIv2. O servidor de catálogos possui seus próprios caminhos de transporte proprietários que não usam Internet Inter-ORB Protocol (IIOP) ou Remote Method Invocation (RMI). Devido a estes caminhos de transporte proprietários, o servidor de catálogos não pode ser gerenciado pelas configurações de transporte WebSphere Application Server CSIV2. Portanto, você deve configurar as propriedades SSL no arquivo de propriedades do servidor para o servidor de catálogos.

Objetivos do aprendizado

Depois de concluir as lições neste módulo, você saberá como:

- Configurar o transporte de entrada e de saída CSIv2
- Incluir propriedades SSL no arquivo de propriedades do servidor de catálogos
- Verificar o arquivo de propriedades do ORB.
- Executar a amostra.

Tempo Necessário

Este módulo leva cerca de 60 minutos.

Pré-requisitos

Esta etapa do tutorial é construída sobre os módulos anteriores. Conclua os módulos anteriores neste tutorial antes de configurar a segurança do transporte.

Lição 3.1: Configurar o Transporte de Entrada e de Saída CSIv2

Para configurar o protocolo Segurança da Camada de Transporte/Secure Sockets Layer (TLS/SSL) para o transporte do servidor, configure o transporte de entrada e o transporte de saída do Common Secure Interoperability Protocol Versão 2 (CSIv2) para `SSL Necessário` para todos os servidores do WebSphere Application Server que hospedam clientes, servidores de catálogo e servidores de contêineres.

Na topologia de exemplo do tutorial, você deve configurar essas propriedades para os servidores de aplicativos s1, s2, xs1 e xs2. As etapas a seguir configuram os transportes de entrada e saída para todos os servidores na configuração.

Configure os transportes de entrada e saída no console administrativo. Certifique-se de que a segurança administrativa esteja ativada.

- **WebSphere Application Server Versão 7.0**: Clique em **Segurança** > **Segurança Global** > **Segurança RMI/IIOP** > **Comunicações de entrada CSIv2**. Altere o tipo de transporte na Camada de Transporte CSIv2 como **SSL Necessário**. Repita esta etapa para configurar as comunicações de saída CSIv2.

As configurações de segurança do terminal gerenciadas centralmente podem ser usadas ou os repositórios SSL podem ser configurados. Consulte Configurações do Transporte de Entrada Common Secure Interoperability Versão 2 para obter mais informações.

Lição 3.2: Incluir Propriedades SSL no Arquivo de Propriedades do Servidor de Catálogos

O servidor de catálogos tem seus próprios caminhos de transporte proprietários que não podem ser gerenciados pelas configurações de transporte do WebSphere Application Server Common Secure Interoperability Protocol Version 2 (CSIV2). Portanto, você deve configurar as propriedades do Secure Sockets Layer (SSL) no arquivo de propriedades do servidor para o servidor de catálogos.

Para configurar a segurança do servidor de catálogos, etapas adicionais são necessárias porque o servidor de catálogos tem seus próprios caminhos de transporte proprietários. Esses caminhos de transporte não podem ser gerenciados pelas configurações de transporte do Application Server CSIV2.

1. Edite as propriedades SSL no arquivo `catServer2.props`. Para configurar a segurança do servidor de catálogos, remova o comentário das seguintes propriedades SSL no arquivo de propriedades do servidor de catálogos. Para este tutorial, as propriedades do servidor de catálogos estão no arquivo `catServer2.props` . Atualize as propriedades keyStore e trustStore para referenciar o local apropriado em seu ambiente.

```
#alias=default
#contextProvider=IBMJSSE2
#protocol=SSL
#keyStoreType=PKCS12
#keyStore=/<WAS_HOME>/IBM/WebSphere/AppServer/profiles/<DMGR_NAME>/config/
cells/<CELL_NAME>/nodes/<NODE_NAME>/key.p12
#keyStorePassword=WebAS
#trustStoreType=PKCS12
#trustStore=/<WAS_HOME>/IBM/WebSphere/AppServer/profiles/<DMGR_NAME>/config/
cells/<CELL_NAME>/nodes/<NODE_NAME>/trust.p12
#trustStorePassword=WebAS
#clientAuthentication=false
```

O arquivo `catServer2.props` usa o keystore e o armazenamento confiável no nível do nó WebSphere Application Server padrão. Se estiver implementando um ambiente de implementação mais complexo, você deverá escolher o keystore e o armazenamento confiável corretos. Em alguns casos, você deve criar um keystore e um armazenamento confiável e importar as chaves dos keystores de outros servidores. Observe que a sequência `WebAS` é a senha padrão do keystore e do armazenamento confiável do WebSphere Application Server. Consulte Configuração de Certificado Autoassinado Padrão para obter mais detalhes.

2. No arquivo `catServer2.props`, atualize o valor da propriedade transportType. Para as etapas anteriores do tutorial, o valor era definido para `TCP/IP`. Altere o valor para `SSL Necessário`.
3. Reinicie o gerenciador de implementação para ativar as mudanças das configurações de segurança do servidor de catálogos.

Ponto de verificação de lições:

Você configurou as propriedades SSL para o servidor de catálogos.

Lição 3.3: Executar a Amostra

Reinicie todos os servidores e execute o aplicativo de amostra novamente. Você deve poder executar as etapas sem nenhum problema.

Consulte “Lição 2.4: Instalar e Executar a Amostra” na página 60 para obter mais informações sobre como executar e instalar o aplicativo de amostra.

Ponto de verificação de lições:

Você executou o aplicativo de amostra com a segurança de transporte ativada.

Módulo 4: Usar a Autorização do Java Authentication and Authorization Service (JAAS) no WebSphere Application Server

Agora que você configurou a autenticação de clientes, é possível configurar ainda mais a autenticação para conceder aos usuários diferentes permissões. Por exemplo, um usuário operador pode apenas visualizar dados, enquanto que um usuário administrador pode executar todas as operações.

Após autenticar um cliente, como no módulo anterior neste tutorial, é possível fornecer privilégios de segurança por meio dos mecanismos de autorização do eXtreme Scale. O módulo anterior deste tutorial demonstrou como ativar a autenticação para uma grade de dados usando a integração com o WebSphere Application Server. Como resultado, nenhum cliente não autenticado pode se conectar aos servidores eXtreme Scale ou submeter solicitações para seu sistema. Entretanto, todo cliente autenticado tem a mesma permissão ou privilégios para o servidor, como de leitura, gravação ou exclusão de dados armazenados nos mapas do ObjectGrid. Os clientes também podem emitir qualquer tipo de consulta.

Esta parte do tutorial demonstra como usar a autorização do eXtreme Scale para fornecer diferentes privilégios para usuários autenticados. O WebSphere eXtreme Scale usa um mecanismo de autorização baseado em permissão. É possível designar categorias de permissão diferentes que são representadas por diferentes classes de permissão. Esse módulo apresenta a classe MapPermission. Para obter uma lista de todas as permissões possíveis, consulte “Programação de Autorização de Cliente” na página 827.

No WebSphere eXtreme Scale, a classe `com.ibm.websphere.objectgrid.security.MapPermission` representa permissões para os recursos do eXtreme Scale, especificamente os métodos das interfaces ObjectMap ou JavaMap. O WebSphere eXtreme Scale define as seguintes cadeias de permissões para acesso aos métodos de ObjectMap e JavaMap:

- **read**: Concede permissão para ler os dados do mapa.
- **write**: Concede permissão para atualizar os dados no mapa.
- **insert**: Concede permissão para inserir os dados no mapa.
- **remove**: Concede permissão para remover os dados do mapa.
- **invalidate**: Concede permissão para invalidar os dados a partir do mapa.
- **all**: Concede todas as permissões para ler, gravar, inserir, remover e invalidar.

A autorização ocorre quando um cliente do eXtreme Scale usa uma API de acesso a dados, como o ObjectMap, o JavaMap ou as APIs EntityManager. O tempo de execução verifica as permissões do mapa correspondente quando o método é chamado. Se as permissões necessárias não forem concedidas ao cliente, isso resultará em uma exceção AccessControlException. Este tutorial demonstra como usar a autorização do Java Authentication and Authorization Service (JAAS) para conceder acesso de mapa de autorização para diferentes usuários.

Objetivos do aprendizado

Depois de concluir as lições neste módulo, você saberá como:

- Ativar a autorização para WebSphere eXtreme Scale.
- Ativar a autorização baseada no usuário
- Configurar a autorização baseada em grupo.

Tempo Necessário

Este módulo leva cerca de 60 minutos.

Pré-requisitos

Você deve concluir os módulos anteriores neste tutorial antes de configurar autenticação.

Conceitos relacionados:

"Programação de Autorização de Cliente" na página 827
O WebSphere eXtreme Scale suporta a autorização Java Authentication and Authorization Service (JAAS) que está pronta para uso e também suporta a autorização customizada usando a interface ObjectGridAuthorization.

Lição 4.1: Ativar a Autorização do WebSphere eXtreme Scale

Para ativar a autorização no WebSphere eXtreme Scale, você deve ativar a segurança em um ObjectGrid específico.

Para ativar a autorização no ObjectGrid, você deve configurar o atributo **`securityEnabled`** para true desse ObjectGrid específico no arquivo XML. Para este tutorial, é possível usar o arquivo `XSDeployment_sec.ear` no diretório *samples_home*`/WASSecurity`, que já possui a segurança configurada no arquivo `objectGrid.xml`, ou é possível editar o arquivo `objectGrid.xml` existente para ativar a segurança. Esta lição demonstra como editar o arquivo para ativar a segurança.

1. Extraia os arquivos no arquivo `XSDeployment.ear` e, em seguida, descompacte o arquivo `XSDeploymentWeb.war`.

2. Abra o arquivo objectGrid.xml e configure o atributo securityEnabled para true no nível do ObjectGrid. A seguir há um exemplo desse atributo:

```
<?xml version="1.0" encoding="UTF-8"?>

<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">

    <objectGrids>
        <objectGrid name="Grid" securityEnabled="true">
            <backingMap name="Map1" />
        </objectGrid>
    </objectGrids>

</objectGridConfig>
```

   Se diversos ObjectGrids estiverem definidos, esse atributo deverá ser configurado em cada grade de dados.
3. Recompacte os arquivos XSDeploymentWeb.war e XSDeployment.ear para incluir suas mudanças. Nomeie o arquivo XSDeployment_sec.ear de modo que o pacote original não seja sobrescrito.
4. Desinstale o aplicativo XSDeployment existente e instale o arquivo XSDeployment_sec.ear. Consulte “Lição 2.4: Instalar e Executar a Amostra” na página 60 para obter mais informações sobre a implementação de aplicativos.

Ponto de verificação de lições:

Você ativou a segurança no ObjectGrid, que também ativa a autorização na grade de dados.

Lição 4.2: Ativar Autorização Baseada no Usuário

No módulo de autenticação deste tutorial, dois usuários foram criados: operator1 e admin1. É possível designar permissões diferentes para esses usuários com a autorização Java Authentication and Authorization Service (JAAS).

Definindo a Política de Autorização do Java Authentication and Authorization Service (JAAS) Usando os Principals do Usuário:

É possível designar permissões para os usuários criados anteriormente. Designe permissões somente leitura ao usuário operator1 para todos os mapas. Designe ao usuário admin1 todas as permissões. Use o arquivo de política de autorização JAAS para conceder permissões para os principals.

Edite o arquivo de autorização do JAAS. O arquivo xsAuth2.policy está no diretório *samples_home*/security:

```
grant codebase http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction
Principal com.ibm.ws.security.common.auth.WSPrincipalImpl "defaultWIMFileBasedRealm/operator1" {
    permission com.ibm.websphere.objectgrid.security.MapPermission "Grid.Map1", "read";
};

grant codebase http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction
Principal com.ibm.ws.security.common.auth.WSPrincipalImpl "defaultWIMFileBasedRealm/admin1" {
    permission com.ibm.websphere.objectgrid.security.MapPermission "Grid.Map1", "all";
};
```

Neste arquivo, o código base http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction é uma URL reservada especialmente para o ObjectGrid. Todas as permissões do ObjectGrid concedidas aos principals devem usar esse código base especial. As seguintes permissões são designadas nesse arquivo:

- A primeira instrução de concessão concede permissão `read` para o principal `operator1`. O usuário `operador1` possui permissão somente leitura para o mapa Map1 da instância Grid do ObjectGrid.
- A segunda instrução de concessão concede a permissão de mapa 'all' para o principal do admin1. O usuário `admin1` possui permissão all para o mapa Map1 na instância Grid do ObjectGrid.
- O nome do principal é `defaultWIMFileBasedRealm/operator1`, mas não `Operator1`. O WebSphere Application Server inclui automaticamente o nome da região no nome do principal quando repositórios federados são usados como o registro de conta do usuário. Ajuste esse valor, se necessário.

Configurando o Arquivo de Política de Autorização JAAS Usando as Propriedades da JVM:
Use as seguintes etapas para configurar as propriedades JVM para os servidores xs1 e xs2, que estão no cluster xsCluster. Se estiver usando uma topologia diferente da topologia de amostra usada neste tutorial, configure o arquivo em todos os servidores de contêiner.

1. No console administrativo, clique em **Servidores** > **Servidores de Aplicativos** > ***server_name*** > **Gerenciamento Java e Processos** > **Definição de Processo** > **Java virtual machine**
2. Inclua os seguintes argumentos JVM genéricos:
   `-Djava.security.policy=`*`samples_home`*`/security/xsAuth2.policy`
3. Clique em **OK** e salve as mudanças.

Executando os Aplicativos de Amostra para Testar a Autorização:
É possível usar o mesmo aplicativo de amostra para testar as configurações de autorização. O usuário administrador possui todas as permissões no mapa Map1, inclusive permissões para exibir e incluir funcionários. O usuário operador pode apenas visualizar os funcionários porque esse usuário receber permissão somente leitura.

1. Reinicie todos os servidores de aplicativos que estão executando servidores de contêiner.
2. Abra o aplicativo `EmployeeManagementWeb`. Em um navegador da web, abra `http://<host>:<port>/EmployeeManagermentWeb/management.jsp`.
3. Efetue login no aplicativo como administrador. Use o nome de usuário `admin1` e a senha `admin1`.
4. Tente exibir um funcionário. Clique em **Exibir um Funcionário** e procure pelo endereço de e-mail `authemp1@acme.com`. Uma mensagem exibe que o usuário não pode ser localizado.
5. Incluir um funcionário. Clique em **Incluir um Funcionário**. Inclua o email `authemp1@acme.com`, o nome `Joe` e o sobrenome `Doe` e, em seguida, clique em **Enviar**. Uma mensagem exibe que o funcionário foi incluído.
6. Efetue login como o usuário operador. Abra uma segunda janela do navegador da web e depois abra a seguinte URL: `http://<host>:<port>/EmployeeManagermentWeb/management.jsp`. Use o nome de usuário `operator1` e a senha `operator1`.
7. Tente exibir um funcionário. Clique em **Exibir um Funcionário** e procure pelo endereço de e-mail `authemp1@acme.com`. O funcionário é exibido.
8. Incluir um funcionário. Clique em **Incluir um Funcionário**. Inclua o email `authemp2@acme.com`, o nome `Joe` e o sobrenome `Doe` e, em seguida, clique em **Enviar**. A mensagem a seguir é exibida:
   `Ocorre uma exceção ao Incluir o funcionário. Consulte abaixo para obter mensagens de exceção detalhadas.`

A seguinte exceção está na cadeia de exceções:

```
java.security.AccessControlException: Acesso negado
(com.ibm.websphere.objectgrid.security.MapPermission Grid.Map1 insert)
```

Esta mensagem é exibida porque o usuário `operator1` não tem permissão para inserir dados no mapa Map1.

Se você estiver executando com uma versão do WebSphere Application Server anterior à Versão 7.0.0.11, um erro java.lang.StackOverflowError será exibido no servidor de contêiner. Este erro é causado por um problema com o IBM Developer Kit. O problema é corrigido no IBM Developer Kit fornecido com o WebSphere Application Server Versão 7.0.0.11 e posterior.

Ponto de verificação de lições:

Nesta lição, você configurou a autorização ao designar permissões para usuários específicos.

Lição 4.3: Configurar Autorização Baseada em Grupo

Na lição anterior, você designou autorização baseada em usuário individual com os principais do usuário na política de autorização do Java Authentication and Authorization Service. No entanto, quando você tiver centenas ou milhares de usuários, use a autorização baseado em grupo, que autoriza o acesso baseado em grupos em vez de em usuários individuais.

Infelizmente, o objeto Subject que é autenticado no WebSphere Application Server contém apenas um principal de usuário. Este objeto não contém um principal de grupo. É possível incluir um módulo de login customizado para preencher o principal do grupo no objeto Subject.

Para este tutorial, o módulo de login customizado é denominado com.ibm.websphere.samples.objectgrid.security.lm.WASAddGroupLoginModule. O módulo está no arquivo `groupLM.jar`. Coloque o arquivo JAR no diretório `WAS-INSTALL/lib/ext`.

O WASAddGroupLoginModule recupera a credencial do grupo público a partir do sujeito WebSphere Application Server e cria um principal de Grupo, com.ibm.websphere.samples.objectgrid.security.WSGroupPrincipal, para representar o grupo. Esse principal de grupo pode então ser usado para autorização do grupo. Os grupos são definidos no arquivo `xsAuthGroup2.policy` :

```
grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
principal com.ibm.websphere.sample.xs.security.WSGroupPrincipal
  "defaultWIMFileBasedRealm/cn=operatorGroup,o=defaultWIMFileBasedRealm" {
    permission com.ibm.websphere.objectgrid.security.MapPermission "Grid.Map1", "read";
};

grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
principal com.ibm.websphere.sample.xs.security.WSGroupPrincipal
 "defaultWIMFileBasedRealm/cn=adminGroup,o=defaultWIMFileBasedRealm" {
    permission com.ibm.websphere.objectgrid.security.MapPermission "Grid.Map1", "all";
};
```

O nome do grupo é o `WSGroupPrincipal`, que representa o grupo.

Incluindo o Módulo de Login Customizado:
O módulo de login customizado deve ser incluído em cada uma das seguintes entradas do módulo de login do sistema: Se estiver usando Lightweight Third Party Authentication (LTPA), inclua a entrada nos módulos de login RMI_INBOUND. O LTPA é o mecanismo de autenticação padrão para o

WebSphere Application Server Versão 7.0. Para uma configuração do WebSphere Application Server Network Deployment, é necessário definir apenas as entradas de configuração do mecanismo de autenticação de LTPA.

Use as seguintes etapas para configurar o módulo de login com.ibm.websphere.samples.objectgrid.security.lm.WASAddGroupLoginModule fornecido:

1. No console administrativo, clique em **Segurança** > **Segurança Global** > **Java Authentication and Authorization Service** > **Logins do Sistema** > *login_module_name* > **Módulos de Login do JAAS** > **Novo**.
2. Insira o nome da classe como `com.ibm.websphere.sample.xs.security.lm.WASAddGroupLoginModule`.
3. Opcional: Inclua uma propriedade `debug` e configure o valor como `true`.
4. Clique em **Aplicar** para incluir o novo módulo na lista de módulos de login.

Configurando o Arquivo de Propriedades JAAS Authorization Usando as Propriedades da JVM:

No console administrativo, execute as seguintes etapas para os servidores xs1 e xs2 no xsCluster. Se uma topologia de implementação diferente for usada, execute as etapas a seguir para os servidores de aplicativos que hospedam os servidores de contêiner.

1. No console administrativo, clique em **Servidores** > **Servidores de Aplicativos** > *server_name* > **Gerenciamento Java e Processos** > **Definição de Processo** > **Java virtual machine**
2. Insira os argumentos Genéricos de JVM a seguir ou substitua a entrada `-Djava.security.policy` pelo texto a seguir:

   `-Djava.security.policy=`*`samples_home`*`/security/xsAuthGroup2.policy`
3. Clique em **OK** e salve as mudanças.

Testando a Autorização do Grupo com o Aplicativo de Amsotra:

É possível testar se e autorização de grupo foi configurada pelo módulo de login com o aplicativo de amostra.

1. Reinicie os servidores de contêiner. Para este tutorial, os servidores de contêiner são os servidores de xs1 e xs2.
2. Efetue login no aplicativo de amostra. Em um navegador da web, abra `http://<host>:<port>/EmployeeManagementWeb/management.jsp` e efetue login com o nome de usuário `admin1` e senha `admin1`.
3. Exibir um funcionário. Clique em **Exibir um Funcionário** e procure pelo endereço de email `authemp2@acme.com`. Uma mensagem exibe que o usuário não pode ser localizado.
4. Incluir um funcionário. Clique em **Incluir um Funcionário**. Inclua o email `authemp2@acme.com`, o nome `Joe` e o sobrenome `Doe` e, em seguida, clique em **Enviar**. Uma mensagem exibe que o funcionário foi incluído.
5. Efetue login como o usuário operador. Abra uma segunda janela do navegador da web e depois a seguinte URL: `http://<host>:<port>/EmployeeManagermentWeb/management.jsp`. Use o nome de usuário `operator1` e a senha `operator1`.
6. Tente exibir um funcionário. Clique em **Exibir um Funcionário** e procure pelo endereço de email `authemp2@acme.com`. O funcionário é exibido.

7. Incluir um funcionário. Clique em **Incluir um Funcionário**. Inclua o email `authemp3@acme.com`, o nome `Joe` e o sobrenome `Doe` e, em seguida, clique em **Enviar**. A mensagem a seguir é exibida:

   ```
   Ocorre uma exceção ao Incluir o funcionário. Consulte abaixo para obter mensagens de exceção detalhadas.
   ```

   A seguinte exceção está na cadeia de exceções:

   ```
   java.security.AccessControlException: Acesso negado
   (com.ibm.websphere.objectgrid.security.MapPermission Grid.Map1 insert)
   ```

   Esta mensagem é exibida porque o usuário operator não tem permissão para inserir dados no mapa Map1.

Ponto de verificação de lições:

Você configurou grupos para simplificar a designação de permissão para os usuários de seu aplicativo.

Módulo 5: Use a Ferramenta `xscmd` para Monitorar as Grades de Dados e Mapas

É possível usar a ferramenta **xscmd** para mostrar as grades de dados e os tamanhos de mapa primários da grade de dados `Grid` . A ferramenta **xscmd** usa o MBean para consultar todos os artefatos grade de dados, tais como shards primários, shards de réplica, servidores de contêiner, tamanhos de mapa, e assim por diante.

Neste tutorial, os servidores de contêiner e de catálogos estão em execução nos servidores de aplicativos WebSphere Application Server. O tempo de execução do WebSphere eXtreme Scale registra os beans gerenciados (MBean) com o servidor MBean que é criado pelo tempo de execução do WebSphere Application Server. A segurança usada pela ferramenta **xscmd** é fornecida pela segurança MBean do WebSphere Application Server. Portanto, uma configuração de segurança específica do WebSphere eXtreme Scale não é necessária.

1. Usando uma ferramenta de linha de comandos, abra o diretório *DMGR_PROFILE*`/bin` .
2. Executar a ferramenta **xscmd**.

   Use o comando **-c showPlacement -sf P** para listar o posicionamento dos shards primários. Linux UNIX

   ```
   xscmd.sh -g Grid -ms mapSet -c showPlacement -sf P
   ```

   Windows

   ```
   xscmd.bat -g Grid -ms mapSet -c showPlacement -sf P
   ```

   Antes de poder visualizar a saída, será solicitado efetuar login com seu ID e senha do WebSphere Application Server.

Tarefas relacionadas:

Monitorando com o Utilitário **xscmd**
O utilitário **xscmd** substitui o utilitário **xsadmin** de amostra como uma ferramenta de monitoramento e administração totalmente suportada. Com o utilitário **xscmd**, é possível exibir informações textuais sobre sua topologia do WebSphere eXtreme Scale.

Administrando com o Utilitário **xscmd**
Com o utilitário **xscmd**, é possível concluir tarefas administrativas no ambiente, tal como: estabelecer links de replicação multi-master, substituir o quorum e parar os grupos de servidores com o comando teardown.

Ponto de verificação de lições

Você usou a ferramenta **xscmd** no WebSphere Application Server.

Tutorial: Integrar a Segurança do WebSphere eXtreme Scale em um Ambiente Misto com um Autenticador Externo

Este tutorial demonstra como proteger os servidores do WebSphere eXtreme Scale que são parcialmente implementados em um ambiente do WebSphere Application Server.

Na implementação deste tutorial, os servidores de contêiner são implementados no WebSphere Application Server. O servidor de catálogos é implementado como um servidor independente e é iniciado em um ambiente do Java Standard Edition (Java SE).

Como o servidor de catálogos não é implementado no WebSphere Application Server, não é possível usar os plug-ins do WebSphere Application Server Authentication. Para obter mais informações sobre o processo de configuração dos plug-ins do WebSphere Application Server Authentication, consulte “Tutorial: Integrar a Segurança do WebSphere eXtreme Scale com o WebSphere Application Server” na página 47. Neste tutorial, um autenticador diferente é necessário para a autenticação do servidor de catálogos. Configure um autenticador do keystore para autenticar os clientes.

Objetivos do aprendizado

Os objetivos do aprendizado para este tutorial são:

- Configurar o WebSphere eXtreme Scale para usar o plug-in KeyStoreLoginAuthenticator.
- Configurar a segurança de transporte do WebSphere eXtreme Scale para usar a configuração do WebSphere Application Server CSIv2 e o arquivo de propriedades do WebSphere eXtreme Scale.
- Usar a autorização do Java Authentication and Authorization Service (JAAS) no WebSphere Application Server
- Usar o utilitário **xscmd** para monitorar as grades de dados e mapas criados no tutorial.

Tempo Necessário

Este tutorial leva cerca de 4 horas do início ao fim.

Introdução: Segurança em um Ambiente Misto

Neste tutorial, integre a segurança do WebSphere eXtreme Scale em um ambiente misto. Os servidores de contêiner são executados no WebSphere Application Server e o serviço de catálogos é executado no modo independente. Como o servidor de catálogos está no modo independente, você deve configurar um autenticador externo.

Importante: Se ambos servidor de contêiner e o servidor de catálogos estiverem em execução no WebSphere Application Server, será possível usar os plug-insdo WebSphere Application Server Authentication ou um autenticador externo. Para obter mais informações sobre como usar os plug-ins do WebSphere Application Server Authentication, consulte "Tutorial: Integrar a Segurança do WebSphere eXtreme Scale com o WebSphere Application Server" na página 47.

Objetivos do aprendizado

Os objetivos do aprendizado para este tutorial são:

- Configurar o WebSphere eXtreme Scale para usar o plug-in KeyStoreLoginAuthenticator.
- Configurar a segurança de transporte do WebSphere eXtreme Scale para usar a configuração do WebSphere Application Server CSIv2 e o arquivo de propriedades do WebSphere eXtreme Scale.
- Usar a autorização do Java Authentication and Authorization Service (JAAS) no WebSphere Application Server
- Usar o utilitário **xscmd** para monitorar as grades de dados e mapas criados no tutorial.

Tempo Necessário

Este tutorial leva cerca de 4 horas do início ao fim.

Nível de qualificação

Intermediário.

Público

Desenvolvedores e administradores que estão interessados na integração de segurança entre o WebSphere eXtreme Scale e o WebSphere Application Server e que configuram autenticadores externos.

Requisitos do Sistema

- WebSphere Application Server Versão 7.0.0.11 ou posterior com as correções a seguir aplicadas:correção temporária PM20613 e correção temporária PM15818.
- O servidor de catálogos deve estar em execução em uma instalação independente e não em uma instalação integrada ao WebSphere Application Server.
- Atualize o tempo de execução Java para aplicar a seguinte correção: IZ79819: IBMJDK FALHA AO LER A INSTRUÇÃO PRINCIPAL COM ESPAÇO EM BRANCO A PARTIR DO ARQUIVO DE SEGURANÇA
- O nó independente que executa o serviço de catálogo deve usar o IBM Software Development Kit Versão 1.6 J9. Esse SDK é incluído na instalação do WebSphere Application Server. O nó do servidor de catálogos deve ser uma instalação

independente porque não é possível executar o comando **startOgServer** dentro de uma instalação do WebSphere eXtreme Scale no WebSphere Application Server.

Este tutorial usa quatro servidores de aplicativos WebSphere Application Server e um gerenciador de implementação para demonstrar a amostra.

Pré-requisitos

Um entendimento básico dos seguintes itens é útil antes de iniciar este tutorial:

- Modelo de programação do WebSphere eXtreme Scale
- Conceitos básicos a segurança do WebSphere eXtreme Scale
- Conceitos básicos a segurança do WebSphere Application Server

Para obter informações complementares sobre o WebSphere eXtreme Scale e sobre a integração de segurança do WebSphere Application Server, consulte "Integração de Segurança com o WebSphere Application Server" na página 794.

Módulo 1: Preparar o Ambiente do WebSphere Application Server e Independente Combinado

Antes de iniciar o tutorial, você deve criar uma topologia básica que inclui servidores de contêiner que são executados no WebSphere Application Server. Neste tutorial, os servidores de catálogos são executados no modo independente.

Objetivos do aprendizado

Com as lições neste módulo, você aprende como:

- Entender a topologia combinada e os arquivos que são necessários para o tutorial
- Configurar o WebSphere Application Server para executar os servidores de contêiner.

Tempo Necessário

Este módulo leva cerca de 60 minutos.

Lição 1.1: Entendendo a Topologia e Obtendo os Arquivos do Tutorial

Para preparar seu ambiente para o tutorial, você deve configurar os servidores de catálogos e de contêiner para a topologia.

Essa lição o orienta pela topologia de amostra e pelos aplicativos que são usados no tutorial. Para começar a executar o tutorial, você deve fazer download dos aplicativos e colocar os arquivos de configuração nos locais corretos para seu ambiente. É possível fazer download do aplicativo de amostra a partir do wikiWebSphere eXtreme Scale.

Topologia: Neste tutorial, os seguintes clusters são criados na célula WebSphere Application Server:

- **Cluster appCluster**: Hospeda o aplicativo corporativo da amostra EmployeeManagement. Esse cluster possui dois servidores de aplicativos: s1 e s2.
- **Cluster xsCluster**: Hospeda os servidores de contêiner do eXtreme Scale. Esse cluster possui dois servidores de aplicativos: xs1 e xs2.

Nessa topologia de implementação, os servidores de aplicativos s1 e s2 são os servidores de cliente que acessam dados que estão sendo armazenados na grade de dados. Os servidores xs1 e xs2 são os servidores de contêiner que hospedam a grade de dados.

Configuração alternativa: É possível hospedar todos os servidores de aplicativos em um único cluster, como no cluster appCluster. Com essa configuração, todos os servidores no cluster são ambos servidores de clientes e servidores de contêiner. Este tutorial usa dois clusters para distinguir entre os servidores de aplicativos que hospedam os servidores de clientes e de contêiner.

Neste tutorial, um domínio de serviço de catálogo é configurado, que consiste de um servidor remoto que não está na célula do WebSphere Application Server. Esta configuração não é a padrão, o que resulta nos servidores de catálogos serem executados no gerenciador de implementação e outros processos na célula do WebSphere Application Server . Consulte o Criando Domínios do Serviço de Catálogo no WebSphere Application Server para obter mais informações sobre como criar um domínio de serviço de catálogo composto por servidores remotos.

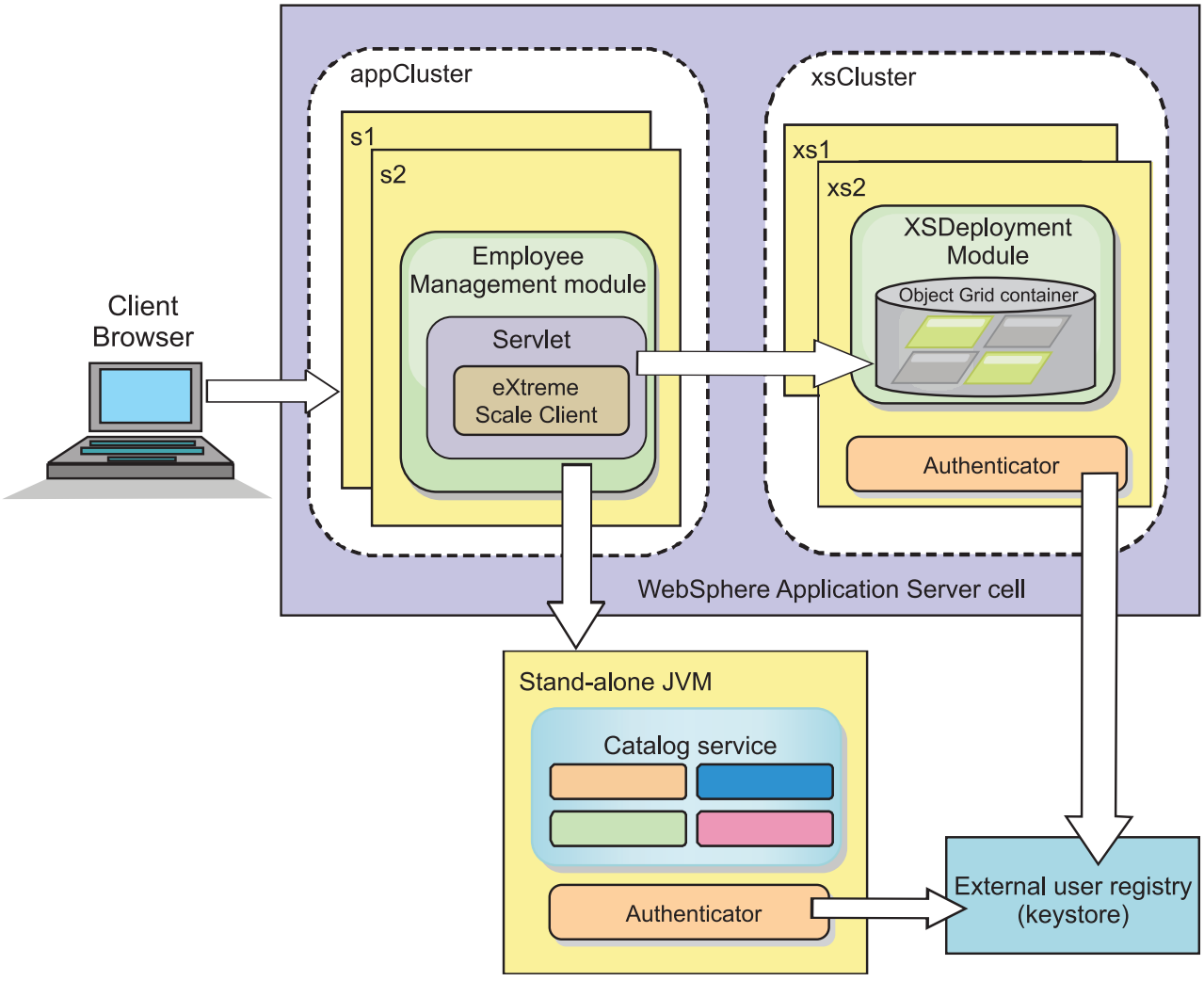


Figura 4. Topologia do Tutorial

Aplicativos: Neste tutorial, você está usando dois aplicativos e um arquivo de biblioteca compartilhado:

- **EmployeeManagement.ear**: O aplicativo EmployeeManagement.ear é um aplicativo corporativo simplificadodo Java 2 Platform, Enterprise Edition (J2EE). Ele contém um módulo da web para gerenciar os perfis dos funcionários. O módulo da web contém o arquivo management.jsp para exibir, inserir, atualizar e excluir perfis de funcionários que são armazenados nos servidores de contêiner.
- **XSDeployment.ear**: Este aplicativo contém um módulo de aplicativo corporativo sem nenhum artefato do aplicativo. Os objetos de cache são compactados no arquivo EmployeeData.jar. O arquivo EmployeeData.jar é implementado como uma biblioteca compartilhada para o arquivo XSDeployment.ear, de modo que o arquivo XSDeployment.ear possa acessar as classes. O propósito deste aplicativo é compactar o eXtreme Scale no arquivo de configuração e no arquivo de propriedades. Quando este aplicativo corporativo é iniciado, os arquivos de configuração do eXtreme Scale são automaticamente detectados pelo tempo de execução do eXtreme Scale, portanto, os servidores de contêiner são criados. Esses arquivos de configuração incluem os arquivos objectGrid.xml e objectGridDeployment.xml.
- **EmployeeData.jar**: Este arquivo jar contém uma classe: a classe com.ibm.websphere.sample.xs.data.EmployeeData. Esta classe representa dados do funcionário que são armazenados na grade. Este arquivo Java Archive (JAR) é implementado com os arquivos EmployeeManagement.ear e XSDeployment.ear como uma biblioteca compartilhada.

Obter os Arquivos do Tutorial:

1. Faça download dos arquivos WASSecurity.zip e security_extauth.zip a partir do wiki do WebSphere eXtreme Scale.
2. Extraia o arquivo WASSecurity.zip em um diretório para visualizar os artefatos binários e de origem, por exemplo, em um diretório wxs_samples/. Esse diretório é referido como *samples_home* para o restante do tutorial. Consulte o arquivo README.txt no pacote para obter uma descrição do conteúdo e como carregar a origem na área de trabalho do Eclipse. Os seguintes arquivos de configuração do ObjectGrid estão no diretório META-INF:
   - objectGrid.xml
   - objectGridDeployment.xml
3. Crie um diretório para armazenar os arquivos de propriedade que são usados para proteger este ambiente. Por exemplo, você pode criar o diretório /opt/wxs/security.
4. Extraia o arquivo security_extauth.zip para o *samples_home*. O arquivo security_extauth.zip contém os seguintes arquivos de configuração de segurança que são usados neste tutorial. Os arquivos de configuração são:
   - catServer3.props
   - server3.props
   - client3.props
   - security3.xml
   - xsAuth3.props
   - xsjaas3.config
   - sampleKS3.jks

Sobre os Arquivos de Configuração:

Os arquivos objectGrid.xml e objectGridDeployment.xml criam as grades de dados e mapas que armazenam os dados do aplicativo.

Esses arquivos de configuração devem ser nomeados como objectGrid.xml e objectGridDeployment.xml. Quando o servidor de aplicativos é iniciado, o eXtreme Scale detecta estes arquivos no diretório META-INF dos módulos EJB e da web. Se estes arquivos forem localizados, supõe-se que a Java virtual machine (JVM) atua como um servidor de contêiner para as grades de dados definidas nos arquivos de configuração.

Arquivo objectGrid.xml

O arquivo objectGrid.xml define um ObjectGrid denominado Grid. A grade de dados Grid tem um mapa, o mapa Map1, que armazena o perfil do funcionário para o aplicativo.

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">

 <objectGrids>
        <objectGrid name="Grid" txTimeout="15">
            <backingMap name="Map1" />
        </objectGrid>
    </objectGrids>

</objectGridConfig>
```

Arquivo objectGridDeployment.xml

O arquivo objectGridDeployment.xml especifica como implementar a grade de dados Grid. Quando a grade é implementada, ela tem cinco partições e uma réplica síncrona.

```
<?xml version="1.0" encoding="UTF-8"?>

<deploymentPolicy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/deploymentPolicy ../deploymentPolicy.xsd"
 xmlns="http://ibm.com/ws/objectgrid/deploymentPolicy">

    <objectgridDeployment objectgridName="Grid">
        <mapSet name="mapSet" numberOfPartitions="5" minSyncReplicas="0"
maxSyncReplicas="1" >"1" >
            <map ref="Map1"/>
        </mapSet>
    </objectgridDeployment>

</deploymentPolicy>
```

Ponto de verificação de lições:

Nesta lição, você aprendeu sobre a topologia do tutorial e incluiu os arquivos de configuração e os aplicativos de amostra no seu ambiente.

Lição 1.2: Configurar o Ambiente do WebSphere Application Server

Para preparar seu ambiente para o tutorial, você deve configurar a segurança do WebSphere Application Server. Ative a segurança de administração e do aplicativo usando repositórios federados baseados em arquivo internos como um registro de conta do usuário. Em seguida, é possível criar clusters de servidores para hospedar o aplicativo cliente e os servidores de contêiner. Também é necessário criar e iniciar os servidores de catálogos.

As seguintes etapas foram gravadas usando o WebSphere Application Server Versão 7.0. No entanto, também podem ser aplicados os conceitos que se aplicam às versões anteriores do WebSphere Application Server.

Configurar a Segurança do WebSphere Application Server:
Crie e aumente perfis para o gerenciador de implementação e os nós com o WebSphere eXtreme Scale. Consulte Instalando o WebSphere eXtreme Scale ou o WebSphere eXtreme Scale Client com WebSphere Application Server para obter mais informações.

Configure a segurança do WebSphere Application Server.

1. No console administrativo do WebSphere Application Server, clique em **Segurança** > **Segurança Global**.
2. Selecione **Repositórios Federados** como a **Definição da Região Disponível**. Clique em **Configurar como atual**.
3. Clique em **Configurar...** para acessar o painel Repositórios Federados.
4. Digite o **Nome do usuário administrativo principal**, por exemplo, `admin`. Clique em **Aplicar.**
5. Quando solicitado, digite a senha do usuário administrativo e clique em **OK**. Salve as alterações.
6. Na página **Segurança Global**, verifique se a configuração de **Repositórios Federados** está definida para o registro de conta do usuário atual.
7. Selecione os seguintes itens: **Ativar Segurança Administrativa**, **Ativar Segurança do Aplicativo**e **Usar segurança Java 2 para restringir o acesso do aplicativo aos recursos locais** . Clique em **Aplicar** e salve suas alterações.
8. Reinicie o gerenciador de implementação e quaisquer servidores de aplicativo em execução.

A Segurança Administrativa do WebSphere Application Server é ativada usando os repositórios federados baseados em arquivo internos como o registro de conta do usuário.

Criar Clusters de Servidores:

Crie dois clusters de servidores em sua configuração do WebSphere Application Server: O cluster `appCluster` para hospedar o aplicativo de amostra do tutorial e o cluster `xsCluster` para hospedar a grade de dados.

1. No console administrativo do WebSphere Application Server, abra o painel de clusters. Clique em **Servidores** > **Clusters** > **Clusters de Servidores de Aplicativos do WebSphere** > **Novo**.
2. Digite `appCluster` como o nome do cluster, deixe a opção **Preferir local** selecionada e clique em **Avançar**.
3. Crie servidores no cluster. Crie um servidor denominado `s1`, mantendo as opções padrão. Inclua um membro de cluster adicional denominado `s2`.
4. Conclua as etapas restantes no assistente para criar o cluster. Salve as mudanças.
5. Repita essas etapas para criar o cluster `xsCluster`. Este cluster possui dois servidores denominados `xs1` e `xs2`.

Criar um Domínio de Serviço de Catálogo:

Depois de configurar o cluster de servidores e a segurança, você deve definir onde os servidores de catálogos serão iniciados.

Defina um domínio de serviço de catálogo no WebSphere eXtreme Scale

1. No console administrativo do WebSphere Application Server, clique em **Administração do sistema** > **WebSphere eXtreme Scale** > **Domínios do serviço de catálogo**.
2. Crie o domínio do serviço de catálogo. Clique em **Novo**. Crie o domínio de serviço de catálogo com o nome `catalogService1` e ative o domínio de serviço de catálogo como o padrão.
3. Inclua servidores remotos no domínio de serviço de catálogo. Selecione **Servidor Remoto**. Forneça o nome do host no qual o servidor de catálogos está em execução. Utilize o valor da porta do listener de `16809` para este exemplo.
4. Clique em **OK** e salve as mudanças.

Ponto de verificação de lições:

Você ativou a segurança no WebSphere Application Server e criou a topologia do servidor para o WebSphere eXtreme Scale.

Módulo 2: Configurar a Autenticação do WebSphere eXtreme Scale em um Ambiente Misto

Ao configurar autenticação, é possível determinar de maneira confiável a identidade do solicitante. O WebSphere eXtreme Scale suporta autenticação cliente-para-servidor e servidor-para-servidor.

Fluxo de Autenticação

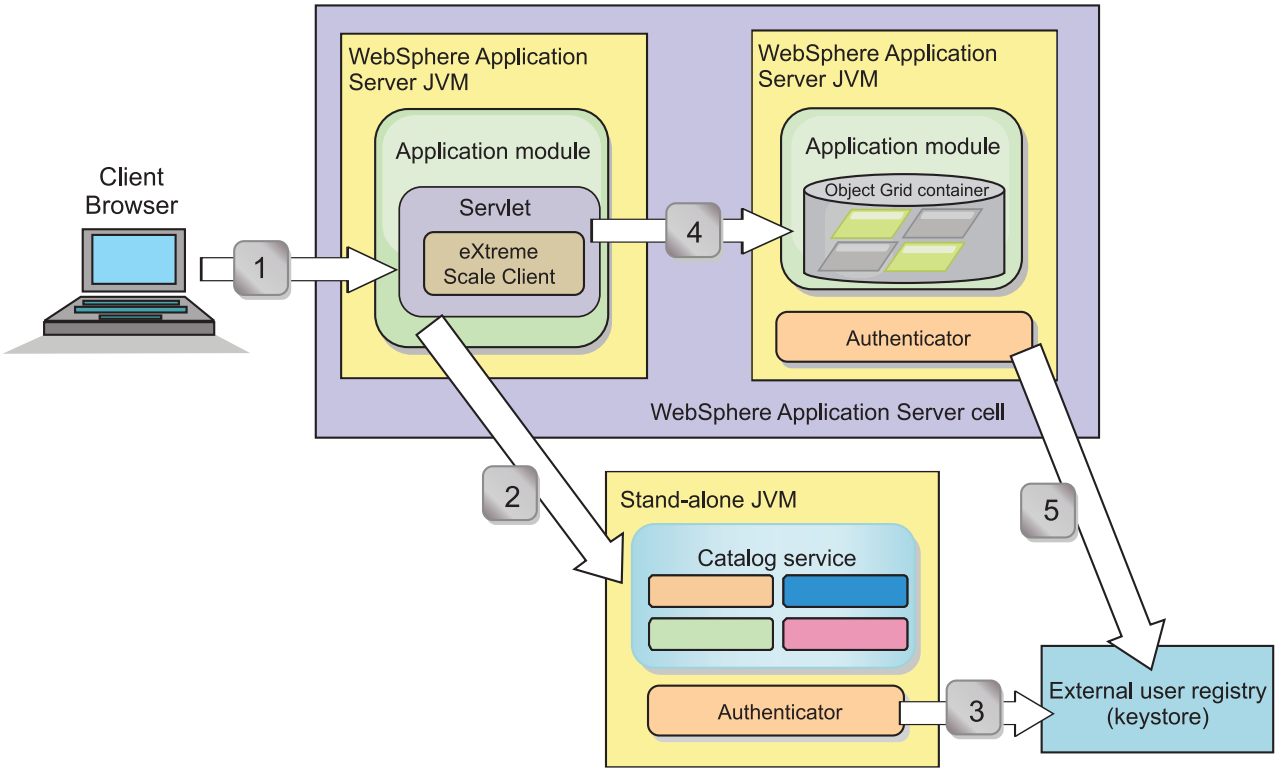


Figura 5. Fluxo de Autenticação

O diagrama anterior mostra dois servidores de aplicativos. O primeiro servidor de aplicativos hospeda o aplicativo da web, que também é um cliente do WebSphere

eXtreme Scale . O segundo servidor de aplicativos hospeda um servidor de contêiner. O servidor de catálogos está em execução em uma Java virtual machine (JVM) independente em vez de WebSphere Application Server.

As setas marcadas com números do diagrama indicam o fluxo da autenticação:

1. Um usuário de aplicativo corporativo acessa o navegador da web e efetua login no primeiro servidor de aplicativos com um nome de usuário e senha. O primeiro servidor de aplicativos envia o nome de usuário e senha do cliente para a infraestrutura de segurança para se autenticar no registro do usuário. Esse registro do usuário é um keystore. Como resultado, as informações de segurança são armazenadas no encadeamento do WebSphere Application Server.
2. O arquivo JavaServer Pages (JSP) age como um cliente do WebSphere eXtreme Scale para recuperar as informações de segurança a partir do arquivo de propriedades do cliente. O aplicativo JSP que está agindo como o cliente do WebSphere eXtreme Scale envia a credencial de segurança do cliente do WebSphere eXtreme Scale junto com a solicitação para o servidor de catálogos. Enviar a credencial de segurança com a solicitação é considerado um modelo *runAs*. Em um modelo runAs, o cliente do navegador da web é executado como um cliente do WebSphere eXtreme Scale para acessar os dados armazenados no servidor de contêiner. O cliente usa uma credencial de cliente da Java virtual machine (JSP) para se conectar aos servidores WebSphere eXtreme Scale. Usar o modelo runAs é o mesmo que conectar-se a um banco de dados com um ID do usuário e senha no nível da origem de dados.
3. O servidor de catálogos recebe a credencial do cliente do WebSphere eXtreme Scale, que inclui os tokens de segurança do WebSphere Application Server. Em seguida, o servidor de catálogos chama o plug-in do autenticador para autenticar a credencial do cliente. O autenticador se conecta ao registro do usuário externo e envia a credencial do cliente para o registro do usuário para autenticação.
4. O cliente envia o ID do usuário e a senha para o servidor de contêiner que é hospedado no servidor de aplicativos.
5. O serviço de contêiner, hospedado no servidor de aplicativos, recebe a credencial do cliente do WebSphere eXtreme Scale, que é o par de ID do usuário e senha. Em seguida, o servidor de contêiner chama o plug-in do autenticador para autenticar a credencial do cliente. O autenticador se conecta ao registro do usuário de keystore e envia a credencial do cliente para o registro do usuário para autenticação

Objetivos do aprendizado

Com as lições neste módulo, você aprende como:

- Configure a segurança do cliente do WebSphere eXtreme Scale.
- Configure a segurança do servidor de catálogos do WebSphere eXtreme Scale.
- Configure a segurança do servidor de contêiner do WebSphere eXtreme Scale.
- Instale e execute o aplicativo de amostra.

Tempo Necessário

Este módulo leva cerca de 60 minutos.

Lição 2.1: Configurar a Segurança do Cliente do WebSphere eXtreme Scale

Configure as propriedades do cliente com um arquivo de propriedades. O arquivo de propriedades do cliente indica a classe de implementação CredentialGenerator a ser usada.

Conteúdo do Arquivo de Propriedades do Cliente:

O tutorial usa tokens de segurança do WebSphere Application Server para obter a credencial do cliente. O diretório *samples_home*/`security_extauth` contém o arquivo `client3.props`.

O arquivo `client3.props` inclui as seguintes configurações:

securityEnabled
Ativa a segurança do cliente do WebSphere eXtreme Scale. O valor é configurado para `true` para indicar que o cliente deve enviar informações de segurança disponíveis para o servidor.

credentialAuthentication
Especifica o suporte de autenticação da credencial do cliente. O valor é configurado para `Suportado` para indicar que o cliente suporta autenticação de credencial.

credentialGeneratorClass
Especifica o nome da classe que implementa a interface com.ibm.websphere.objectgrid.security.plugins.CredentialGenerator. O valor é configurado para a classe com.ibm.websphere.objectgrid.security.plugins.builtins. UserPasswordCredentialGenerator para que o cliente recupere as informações de segurança a partir da classe UserPasswordCredentialGenerator.

credentialGeneratorProps
Especifica o nome do usuário e a senha: `manager manager1`. O nome do usuário é `manager` e a senha é `manager1`. Também é possível usar o comando **`FilePasswordEncoder.bat|sh`** para codificar essa propriedade usando um algoritmo exclusivo ou (xor).

Configurando o Arquivo de Propriedades do Cliente Usando as Propriedades da Java virtual machine (JVM):
No console administrativo, conclua as seguintes etapas para ambos servidores `s1` e `s2` no cluster `appCluster`. Se uma topologia diferente estiver sendo usada, conclua as seguintes etapas para todos os servidores de aplicativos nos quais o aplicativo `EmployeeManagement` é implementado.

1. **Servidores** > **Servidores de aplicativo WebSphere** > *server_name* > **Java and Process Management** > **Definição de processo** > **Java Virtual Machine**.
2. Crie a seguinte propriedade JVM genérica para configurar o local do arquivo de propriedades do cliente:

   ```
   -Dobjectgrid.client.props=samples_home/security_extauth/client3.props
   ```

3. Clique em **OK** e salve as mudanças.

Ponto de verificação de lições:

Você editou o arquivo de propriedades do cliente e configurou os servidores no cluster `appCluster` para usar o arquivo de propriedades do cliente. Este arquivo de propriedades indica a classe de implementação CredentialGenerator a ser usada.

Lição 2.2: Configurar a Segurança do Servidor de Catálogos

Um servidor de catálogos contém dois níveis de informações de segurança: O primeiro nível contém as propriedades de segurança que são comuns a todos os servidores do WebSphere eXtreme Scale, incluindo o serviço de catálogo e os servidores de contêiner. O segundo nível contém as propriedades de segurança que são específicas para o servidor de catálogos.

As propriedades de segurança que são comuns aos servidores de catálogos e aos servidores de contêiner são configuradas no arquivo descritor XML de segurança. Um exemplo das propriedades comuns é a configuração do autenticador, que representa o registro do usuário e o mecanismo de autenticação. Consulte o Arquivo XML Descritor de Segurança para obter mais informações sobre as propriedades de segurança.

Para configurar o arquivo descritor XML de segurança em um ambiente Java SE, use uma opção **-clusterSecurityFile** quando executar o comando **startOgServer** ou **startXsServer**. Especifique um valor em um formato de arquivo, como *samples_home*/security_extauth/security3.xml.

security3.xml file:

Neste tutorial, o arquivo securityWAS2.xml está no diretório *samples_home*/security_extauth. O conteúdo do arquivo security3.xml com os comentários removidos é o seguinte:

```
<securityConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config/security
../objectGridSecurity.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config/security">

 <security securityEnabled="true">
  <authenticator
 className="com.ibm.websphere.objectgrid.security.plugins.
builtins.KeyStoreLoginAuthenticator">
  </authenticator>
 </security>
</securityConfig>
```

As seguintes propriedades são definidas no arquivo security3.xml:

securityEnabled
: A propriedade securityEnabled é configurada para true, indicando que a segurança global do WebSphere eXtreme Scale do servidor de catálogos foi ativada.

autenticador
: O autenticador é configurado como a classe com.ibm.websphere.objectgrid.security.plugins.builtins.KeyStoreLoginAuthenticator. Com essa implementação integrada do plug-in Autenticador, o ID do usuário e senha são passados para verificar se ele está configurado no arquivo keystore. A classe KeyStoreLoginAuthenticator usa um alias de módulo de login KeyStoreLogin, portanto, uma configuração de login do Java Authentication and Authorization Service (JAAS) é necessária.

Arquivo catServer3.props:

O arquivo de propriedades do servidor armazena as propriedades específicas do servidor, dentre elas as propriedades de segurança específicas do servidor. Consulte o Arquivo de Propriedades do Servidor para obter informações adicionais. É possível usar a opção **-serverProps** para especificar a propriedade do servidor de catálogos ao executar o comando **startOgServer** ou **startXsServer**.

Para este tutorial, um arquivo `catServer3.props` é incluído no diretório. O conteúdo do arquivo `catServer3.props` com os comentários removidos é o seguinte:

```
securityEnabled=true
credentialAuthentication=Required
transportType=TCP/IP
secureTokenManagerType=none
authenticationSecret=ObjectGridDefaultSecret
```

securityEnabled
A propriedade securityEnabled é configurada para `true` para indicar que este servidor de catálogos é um servidor seguro.

credentialAuthentication
A propriedade credentialAuthentication é configurada para `Necessária`, portanto, qualquer cliente que esteja conectado ao servidor precisa fornecer uma credencial. No arquivo de propriedades do cliente, o valor credentialAuthentication é configurado para `Suportado`, portanto, o servidor recebe as credenciais que são enviados pelo cliente.

secureTokenManagerType
O secureTokenManagerType está configurado para `none` para indicar que o segredo da autenticação não é criptografado quando junta os servidores existentes.

authenticationSecret
A propriedade authenticationSecret está configurada para `ObjectGridDefaultSecret`. Esta sequência secreta é usada para juntar o cluster de servidores eXtreme Scale. Quando um servidor junta a grade de dados, ele é desafiado a apresentar a sequência secreta. Se a sequência secreta do servidor de junção corresponder à sequência no servidor de catálogos, o servidor de junção será aceito. Se a cadeia não corresponder, o pedido de junção é rejeitado.

transportType
A propriedade transportType é configurada inicialmente para `TCP/IP`. Posteriormente no tutorial, a segurança de transporte é ativada.

Arquivo `xsjaas3.config`:

Como a implementação KeyStoreLoginAuthenticator usa um módulo de login, você deve configurar o modelo de login com um arquivo de configuração de login de autenticação JAAS. O conteúdo do arquivo `xsjaas3.config` é:

```
KeyStoreLogin{
com.ibm.websphere.objectgrid.security.plugins.builtins.KeyStoreLoginModule required
     keyStoreFile="samples_home/security_extauth/sampleKS3.jks" debug = true;
};
```

Se um local para o *samples_home* diferente de `/wxs_samples/`for usado, será necessário atualizar o local do keyStoreFile. Esta configuração de login indica que o módulo
com.ibm.websphere.objectgrid.security.plugins.builtins.KeyStoreLoginModule é usado como o módulo de login. O arquivo keystore é configurado para o arquivo `sampleKS3.jks`.

O arquivo keystore `sampleKS3.jks` de amostra armazena dois IDs do usuário e senhas: manager/manager1 e cashier/cashier1.

Os seguintes comandos **`keytool`** podem ser usados para criar esse keystore:

- `keytool -genkey -v -keystore ./sampleKS3.jks -storepass sampleKS1 -alias manager -keypass manager1 -dname CN=manager,O=acme,OU=OGSample -validity 10000`
- `keytool -genkey -v -keystore ./sampleKS3.jks -storepass sampleKS1 -alias operator -keypass operator1 -dname CN=operator,O=acme,OU=OGSample -validity 10000`

Iniciar o Servidor de Catálogos com a Segurança Ativada:

Para iniciar o servidor de catálogos, emita o comando **startOgServer** ou **startXsServer** com os parâmetros **-clusterFile** e **-serverProps** para transmitir nas propriedades de segurança.

Use uma instalação independente do WebSphere eXtreme Scale para executar o servidor de catálogos. Ao usar a imagem de instalação independente, o IBM SDK deve ser usado. É possível usar o SDK que está incluído com o WebSphere Application Server ao definir a variável *JAVA_HOME* para apontar para o IBM SDK. Por exemplo, `set JAVA_HOME=was_root/IBM/WebSphere/AppServer/java/`

1. Acesse o diretório `bin`.

   ```
   cd wxs_home/bin
   ```

2. Execute o comando **startOgServer** ou **startXsServer**.

   Linux UNIX

   ```
   ./startOgServer.sh cs1 -listenerPort 16809 -JMXServicePort 16099 -catalogServiceEndPoints
   cs1:[HOST_NAME]:16601:16602 -clusterSecurityFile samples_home/security_extauth/security3.xml
   -serverProps samples_home/security_extauth/catServer3.props -jvmArgs
   -Djava.security.auth.login.config="samples_home/security_extauth/xsjaas3.config"
   ```

   Windows

   ```
   startOgServer.bat cs1 -listenerPort 16809 -JMXServicePort 16099 -catalogServiceEndPoints
   cs1:[HOST_NAME]:16601:16602 -clusterSecurityFile samples_home/security_extauth/security3.xml
   -serverProps samples_home/security_extauth/catServer3.props -jvmArgs
   -Djava.security.auth.login.config="samples_home/security_extauth/xsjaas3.config"
   ```

   Linux UNIX 8.6+

   ```
   ./startXsServer.sh cs1 -listenerPort 16809 -JMXServicePort 16099 -catalogServiceEndPoints
   cs1:[HOST_NAME]:16601:16602 -clusterSecurityFile samples_home/security_extauth/security3.xml
   -serverProps samples_home/security_extauth/catServer3.props -jvmArgs
   -Djava.security.auth.login.config="samples_home/security_extauth/xsjaas3.config"
   ```

   Windows 8.6+

   ```
   startXsServer.bat cs1 -listenerPort 16809 -JMXServicePort 16099 -catalogServiceEndPoints
   cs1:[HOST_NAME]:16601:16602 -clusterSecurityFile samples_home/security_extauth/security3.xml
   -serverProps samples_home/security_extauth/catServer3.props -jvmArgs
   -Djava.security.auth.login.config="samples_home/security_extauth/xsjaas3.config"
   ```

Depois de executar o comando **startOgServer** ou **startXsServer**, um servidor seguro é iniciado com a porta do listener 16809, a porta do cliente 16601, a porta de pier 16602 e a porta JMX 16099. Se existir um conflito de portas, altere o número da porta para um número de porta não usado.

Parar um Servidor de Catálogos com a Segurança Ativada:

É possível usar o comando **stopOgServer** ou **stopXsServer** para parar o servidor de catálogos.

1. Acesse o diretório `bin`.

   ```
   cd wxs_home/bin
   ```

2. Execute o comando **stopOgServer** ou **stopXsServer**. Linux UNIX

```
stopOgServer.sh cs1 -catalogServiceEndPoints localhost:16809 -clientSecurityFile
samples_home/security_extauth/client3.props
```

Windows

```
stopOgServer.bat cs1 -catalogServiceEndPoints localhost:16809 -clientSecurityFile
samples_home/security_extauth/client3.props
```

Linux UNIX 8.6+

```
stopXsServer.sh cs1 -catalogServiceEndPoints localhost:16809 -clientSecurityFile
samples_home/security_extauth/client3.props
```

Windows 8.6+

```
stopXsServer.bat cs1 -catalogServiceEndPoints localhost:16809 -clientSecurityFile
samples_home/security_extauth/client3.props
```

Ponto de verificação de lições:

Você configurou a segurança do servidor de catálogos ao associar os arquivos `security3.xml`, `catServer3.props` e `xsjaas3.config` ao serviço de catálogo.

Lição 2.3: Configurar a Segurança do Servidor do Contêiner

Quando um servidor de contêiner se conecta ao serviço de catálogos, o servidor de contêiner obtém todas as configurações de segurança que estiverem definidas no arquivo XML ObjectGrid Security. O arquivo XML ObjectGrid Security define a configuração do autenticador, o valor de tempo limite da sessão de login e outras informações de configuração. Um servidor de contêiner também possui suas próprias propriedades de segurança específicas do servidor no arquivo de propriedade do servidor.

Configure o arquivo de propriedades do servidor com a propriedade -Dobjectgrid.server.props da Java virtual machine (JVM). O nome do arquivo especificado para esta propriedade é um caminho de arquivo absoluto, como *samples_home*`/security_extauth/server3.props`.

Neste tutorial, os servidores de contêiner são hospedados nos servidores `xs1` e `xs2` no cluster `xsCluster`.

Arquivo `server3.props`:

O arquivo `server3.props` está no diretório *samples_home*`/security_extauth/`. O conteúdo do arquivo `server3.props` é o seguinte:

```
securityEnabled=true
credentialAuthentication=Required
secureTokenManagerType=none
authenticationSecret=ObjectGridDefaultSecret
```

securityEnabled
A propriedade securityEnabled é configurada para `true` para indicar que este servidor de contêiner é um servidor seguro.

credentialAuthentication
A propriedade credentialAuthentication é configurada para `Necessária`, portanto, qualquer cliente que esteja conectado ao servidor precisa fornecer uma credencial. No arquivo de propriedades do cliente, a propriedade credentialAuthentication é configurada para `Suportado`, portanto, o servidor recebe a credencial que é enviada pelo cliente.

secureTokenManagerType

O secureTokenManagerType está configurado para `none` para indicar que o segredo da autenticação não é criptografado quando junta os servidores existentes.

authenticationSecret

A propriedade authenticationSecret está configurada para `ObjectGridDefaultSecret`. Esta sequência secreta é usada para juntar o cluster de servidores eXtreme Scale. Quando um servidor junta a grade de dados, ele é desafiado a apresentar a sequência secreta. Se a sequência secreta do servidor de junção corresponder à sequência no servidor de catálogos, o servidor de junção será aceito. Se a cadeia não corresponder, o pedido de junção é rejeitado.

Configurando o arquivo de propriedades de servidor com propriedades JVM:

Configure o arquivo de propriedades do servidor nos servidores xs1 e xs2. Se a topologia não estiver sendo usada para este tutorial, configure o arquivo de propriedades do servidor para todos os servidores de aplicativos que estiverem sendo usados para hospedar servidores de contêiner.

1. Abra a página da Java virtual machine para o servidor. **Servidores** > **Servidores de aplicativo WebSphere** > *server_name* > **Java and Process Management** > **Definição de processo** > **Java Virtual Machine**.
2. Inclua os argumentos JVM genéricos:

   `-Dobjectgrid.server.props=`*`samples_home`*`/security_extauth/server3.props`
3. Clique em **OK** e salve as mudanças.

Incluindo o Módulo de Login Customizado:

O servidor de contêiner usa a mesma implementação KeyStoreAuthenticator que o servidor de catálogos. A implementação KeyStoreAuthenticator usa um alias de módulo de login **`KeyStoreLogin`**, portanto, você deve incluir um módulo de login customizado nas entradas do modelo de login do aplicativo.

1. No console administrativo do WebSphere Application Server, clique em **Segurança** > **Segurança Global** > **Java Authentication and Authorization Service**.
2. Clique em **Logins do Aplicativo**.
3. Clique em **Novo** e inclua um alias `KeyStoreLogin`. Clique em **Aplicar**.
4. Em **Módulos de login JAAS**, clique em **Novo**.
5. Insira `com.ibm.websphere.objectgrid.security.plugins.builtins.KeyStoreLoginModule` como o nome de classe do módulo e escolha **SUFFICIENT** como a estratégia de autenticação. Clique em **Aplicar**.
6. Inclua uma propriedade customizada `keyStoreFile` com o valor *`samples_home`*`/security_extauth/sampleKS.jks`.
7. Opcional: Inclua a propriedade customizada `debug` com o valor `true`.
8. Salve a configuração.

Ponto de verificação de lições:

Agora, a autenticação do servidor WebSphere eXtreme Scale está protegida. Ao configurar esta segurança, todos os aplicativos que tentam se conectar com os servidores WebSphere eXtreme Scale são necessárias para fornecer uma credencial.

Nesse tutorial, o KeyStoreLoginAuthenticator é o autenticador. Como resultado, o cliente é necessário para fornecer um nome de usuário e senha.

Lição 2.4: Instalar e Executar a Amostra

Depois que a autenticação for configurada, o aplicativo de amostra poderá ser instalado e executado.

Criando uma Biblioteca Compartilhada para o Arquivo `EmployeeData.jar`:

1. No console administrativo do WebSphere Application Server, abra a página **Bibliotecas Compartilhadas**. Clique em **Ambiente** > **Bibliotecas Compartilhadas**.
2. Escolha o escopo **célula**.
3. Crie a biblioteca compartilhada. Clique em **Novo**. Insira `EmployeeManagementLIB` como o **Nome**. Insira o caminho para o arquivo `EmployeeData.jar` no caminho de classe, por exemplo, *samples_home*`/WASSecurity/EmployeeData.jar`.
4. Clique em **Aplicar**.

Instalando a Amostra:

1. Instale o arquivo `EmployeeManagement_extauth.ear` no diretório *samples_home*`/security_extauth`.

   Importante: O arquivo `EmployeeManagement_extauth.ear` é diferente do arquivo *samples_home*`/WASSecurity/EmployeeManagement.ear`. O modo com que a sessão do ObjectGrid é recuperada foi atualizado para utilizar a credencial que é armazenada em cache no arquivo de propriedades do cliente no aplicativo `EmployeeManagement_extauth.ear`. Consulte os comentários na classe com.ibm.websphere.sample.xs.DataAccessor no projeto *samples_home*`/WASSecurity/EmployeeManagementWeb` para ver o código que foi atualizado para esta mudança.

   a. Para iniciar a instalação, clique em **Aplicativos** > **Novo Aplicativo** > **Novo Aplicativo Corporativo**. Escolha o caminho detalhado para instalar o aplicativo.
   b. Na etapa **Mapear módulos para servidores**, especifique o cluster `appCluster` para instalar o módulo EmployeeManagementWeb.
   c. Na etapa **Mapear bibliotecas compartilhadas**, selecione o módulo `EmployeeManagementWeb`.
   d. Clique em **Referenciar bibliotecas compartilhadas**. Selecionar a biblioteca `EmployeeManagementLIB`.
   e. Mapeie a função `webUser` para **Tudo Autenticado na Região do Aplicativo**.
   f. Clique em **OK**.

   Os clientes são executados nos servidores `s1` e `s2` neste cluster.
2. Instale o arquivo de amostra `XSDeployment.ear` no diretório *samples_home*`/WASSecurity`.
   a. Para iniciar a instalação, clique em **Aplicativos** > **Novo Aplicativo** > **Novo Aplicativo Corporativo**. Escolha o caminho detalhado para instalar o aplicativo.
   b. Na etapa **Mapear módulos para servidores**, especifique o cluster `xsCluster` para instalar o módulo da web `XSDeploymentWeb`.
   c. Na etapa **Mapear bibliotecas compartilhadas**, selecione o módulo `XSDeploymentWeb`.
   d. Clique em **Referenciar bibliotecas compartilhadas**. Selecionar a biblioteca `EmployeeManagementLIB`.

e. Clique em **OK**.

Os servidores xs1 e xs2 neste cluster hospedam os servidores de contêiner.

3. Verifique se o servidor de catálogos foi iniciado. Para obter mais informações sobre como iniciar um servidor de catálogos para este tutorial, consulte "Iniciar o Servidor de Catálogos com a Segurança Ativada" na página 83.
4. Reinicie o cluster xsCluster. Quando o xsCluster é iniciado, o aplicativo XSDeployment é iniciado e um servidor de contêiner é iniciado nos servidores xs1 e xs2 respectivamente. Se você olhar o arquivo SystemOut.log dos servidores xs1 e xs2, a seguinte mensagem que indica que o arquivo de propriedades do servidor foi carregado é exibida:

   ```
   CWOBJ0913I: Os arquivos de propriedade de servidor foram carregados:
   samples_home/security_extauth/server3.props.
   ```

5. Reinicie o cluster appClusters. Quando o cluster appClusters é iniciado, o aplicativo EmployeeManagement também é iniciado. Se observar o arquivo SystemOut.log dos servidores s1 e s2, será possível ver a seguinte mensagem indicando que o arquivo de propriedades do cliente foi carregado.

   ```
   CWOBJ0924I: O arquivo de propriedades do cliente {0} foi carregado.
   ```

   Se estiver usando o WebSphere eXtreme Scale Versão 7.0, uma mensagem CWOBJ9000I somente em inglês será exibida para indicar que o arquivo de propriedades do cliente foi carregado. Se a mensagem esperada não for exibida, verifique se a propriedade -Dobjectgrid.server.props ou -Dobjectgrid.client.props foi configurada no argumento da JVM. Se as propriedades estiverem realmente configuradas, certifique-se de que o traço (-) seja um caractere UTF.

Executando o Aplicativo de Amostra:

1. Execute o arquivo management.jsp. Em um navegador da web, acesse http://*<your_servername>*:*<port>*/EmployeeManagementWeb/management.jsp. Por exemplo, é possível usar a seguinte URL: http://localhost:9080/EmployeeManagementWeb/management.jsp.
2. Forneça autenticação para o aplicativo. Insira as credenciais do usuário que foram mapeadas para a função webUser. Por padrão, essa função do usuário é mapeada para todos os usuários autenticados. Digite qualquer nome do usuário e senha válidos, como o nome a senha do usuário administrativo. Uma página para exibir, incluir, atualizar e excluir funcionários é exibida.
3. Exibir Funcionários Clique em **Exibir um Funcionário**. Insira emp1@acme.com como o endereço de email e clique em **Enviar**. Uma mensagem é exibida informando que o usuário não pode ser localizado.
4. Incluir um funcionário. Clique em **Incluir um Funcionário**. Insira emp1@acme.com como o endereço de email, insira Joe como o nome fornecido e Doe como o sobrenome. Clique em **Enviar**. Uma mensagem é exibida informando que um funcionário com o endereço emp1@acme.com foi incluído.
5. Exibir o novo funcionário. Clique em **Exibir um Funcionário**. Insira emp1@acme.com como o endereço de email com campos vazios para o nome e sobrenomes e clique em **Submeter**. Uma mensagem é exibida informando que o funcionário foi localizado e que os nomes corretos são exibidos nos campos nome e sobrenome.
6. Excluir o funcionário. Clique em **Excluir um funcionário**. Insira emp1@acme.com e clique em **Enviar**. Uma mensagem é exibida informando que o funcionário foi excluído.

Como o tipo de transporte do servidor de catálogos é configurado para `TCP/IP`, verifique se a configuração do transporte de saída s1 e s2 do servidor não está definida para `SSL Necessário`. Caso contrário, uma exceção ocorrerá. Se você observar o arquivo de saída do sistema do servidor de catálogos, `logs/cs1/SystemOut.log`, a seguinte saída de depuração indicará a autenticação do armazenamento de chaves:

```
SystemOut     0 [KeyStoreLoginModule] initialize: Successfully loaded key store
SystemOut     0 [KeyStoreLoginModule] login: entry
SystemOut     0 [KeyStoreLoginModule] login: user entered user name: manager
SystemOut     0   Print out the certificates:
...
```

Ponto de verificação de lições:

Você instalou e executou o aplicativo de amostra.

Módulo 3: Configurar a Segurança de Transporte

Configure a segurança de transporte para proteger a transferência de dados entre os clientes e servidores na configuração.

No módulo anterior no tutorial, você ativou a autenticação do WebSphere eXtreme Scale. Com a autenticação, qualquer aplicativo que tentar se conectar com o servidor WebSphere eXtreme Scale precisará fornecer uma credencial. Portanto, nenhum cliente não autenticado pode se conectar com o servidor WebSphere eXtreme Scale. Os clientes devem ser um aplicativo autenticado que esteja em execução em uma célula do WebSphere Application Server.

Com a configuração até esse módulo, a transferência de dados entre os clientes no cluster appCluster e os servidores no cluster xsCluster não é criptografada. Essa configuração poderá ser aceitável apenas se seus clusters do WebSphere Application Server estiverem instalados em servidores por trás de um firewall. Entretanto, em alguns cenários, um tráfego não criptografado não é aceito por algumas razões, embora a topologia esteja protegida por um firewall. Por exemplo, uma política de controle pode aplicar o tráfego criptografado. O WebSphere eXtreme Scale suporta a Segurança da Camada de Transporte/Secure Sockets Layer (TLS/SSL) para uma comunicação segura entre os terminais do ObjectGrid, que incluem servidores de cliente, servidores de contêineres e servidores de catálogos.

Nesta implementação de amostra, os clientes e servidores de contêiner do eXtreme Scale estão todos executando no ambiente do WebSphere Application Server. As propriedades do cliente ou do servidor não são necessárias para definir as configurações SSL porque a segurança de transporte do eXtreme Scale é gerenciada pelas configurações de transporte do Common Secure Interoperability Protocol Versão 2 (CSIV2) do WebSphere Application Server. Os servidores do WebSphere eXtreme Scale usam a mesma instância do Object Request Broker (ORB) como os servidores de aplicativos nos quais eles são executados. Especifique todas as configurações de SSL para servidores de cliente e de contêiner na configuração do WebSphere Application Server usando estas configurações de transporte de CSIv2. Você deve configurar as propriedades SSL no arquivo de propriedades do servidor para o servidor de catálogos.

Objetivos do aprendizado

Depois de concluir as lições neste módulo, você saberá como:

- Configurar o transporte de entrada e de saída CSIv2
- Incluir propriedades SSL no arquivo de propriedades do servidor de catálogos

- Verificar o arquivo de propriedades do ORB.
- Executar a amostra.

Tempo Necessário

Este módulo leva cerca de 60 minutos.

Pré-requisitos

Esta etapa do tutorial é construída sobre os módulos anteriores. Conclua os módulos anteriores neste tutorial antes de configurar a segurança do transporte.

Lição 3.1: Configurar o Transporte de Entrada e de Saída CSIv2

Para configurar o protocolo Segurança da Camada de Transporte/Secure Sockets Layer (TLS/SSL) para o transporte do servidor, configure o transporte de entrada e o transporte de saída do Common Secure Interoperability Protocol Versão 2 (CSIv2) para `SSL Necessário` para todos os servidores do WebSphere Application Server que hospedam clientes, servidores de catálogo e servidores de contêineres.

Na topologia de exemplo do tutorial, você deve configurar essas propriedades para os servidores de aplicativos s1, s2, xs1 e xs2. As etapas a seguir configuram os transportes de entrada e saída para todos os servidores na configuração.

Configure os transportes de entrada e saída no console administrativo. Certifique-se de que a segurança administrativa esteja ativada.

- **WebSphere Application Server Versão 7.0**: Clique em **Segurança** > **Segurança Global** > **Segurança RMI/IIOP** > **Comunicações de entrada CSIv2**. Altere o tipo de transporte na Camada de Transporte CSIv2 como **SSL Necessário**. Repita esta etapa para configurar as comunicações de saída CSIv2.

As configurações de segurança do terminal gerenciadas centralmente podem ser usadas ou os repositórios SSL podem ser configurados. Consulte Configurações do Transporte de Entrada Common Secure Interoperability Versão 2 para obter mais informações.

Lição 3.2: Incluir Propriedades SSL no Arquivo de Propriedades do Servidor de Catálogos

O servidor de catálogos está executando fora do WebSphere Application Server, portanto, você deve configurar as propriedades SSL no arquivo de propriedades do servidor.

A outra razão para configurar as propriedades SSL no arquivo de propriedades do servidor é porque o servidor de catálogos tem seus próprios caminhos de transporte proprietários que não podem ser gerenciados pelas configurações de transporte do WebSphere Application Server Common Secure Interoperability Protocol Versão 2 (CSIV2). Portanto, você deve configurar as propriedades do Secure Sockets Layer (SSL) no arquivo de propriedades do servidor para o servidor de catálogos.

Propriedades SSL no Arquivo `catServer3.props`:

```
alias=default
contextProvider=IBMJSSE2
protocol=SSL
keyStoreType=PKCS12
keyStore=/was_root/IBM/WebSphere/AppServer/profiles/
<deployment_manager_name>/config/cells/<cell_name>/nodes/
<node_name>/key.p12
keyStorePassword=WebAS
```

```
trustStoreType=PKCS12
trustStore=/was_root/IBM/WebSphere/AppServer/profiles/
<deployment_manager_name>/config/cells/<cell_name>/nodes/
<node_name>/trust.p12
trustStorePassword=WebAS
clientAuthentication=false
```

O arquivo `catServer3.props` usa o keystore e o armazenamento confiável de nível do nó do WebSphere Application Server padrão. Se estiver implementando um ambiente de implementação mais complexo, você deverá escolher o keystore e o armazenamento confiável corretos. Em alguns casos, você deve criar um keystore e um armazenamento confiável e importar as chaves dos keystores de outros servidores. Observe que a sequência `WebAS` é a senha padrão do keystore e do armazenamento confiável do WebSphere Application Server. Consulte Configuração de Certificado Autoassinado Padrão para obter mais detalhes.

Essas entradas já estão incluídas no arquivo *samples_home*`/security_extauth/catServer3.props` como comentários. É possível remover o comentário das entradas e fazer as atualizações apropriadas de sua instalação nas variáveis *was_root*, *<deployment_manager_name>*, *<cell_name>* e *<node_name>*.

Depois de configurar as propriedades SSL, altere o valor da propriedade transportType de `TCP/IP` para `SSL Necessário`.

Propriedades SSL no arquivo `client3.props`:

As propriedades SSL também devem ser configuradas no arquivo `client3.props` porque este arquivo é usado quando você para o servidor de catálogos que está sendo executado fora do WebSphere Application Server.

Essas propriedades não têm efeito sobre os servidores do cliente que estão em execução no WebSphere Application Server porque eles usam as configurações de transporte WebSphere Application Server Common Security Interoperability Protocol Versão 2 (CSIV2). Entretanto, quando você para o servidor de catálogos, um arquivo de propriedades do cliente deve ser fornecido no comando **`stopOgServer`** . Configure as seguintes propriedades no arquivo <SAMPLES_HOME>/security_extauth/client3.props) para corresponderem aos valores especificados acima no arquivo catServer3.props:

```
#contextProvider=IBMJSSE2
#protocol=SSL
#keyStoreType=PKCS12
#keyStore=/was_root/IBM/WebSphere/AppServer/profiles/
<deployment_manager_name>/config/cells/<cell_name>/nodes/
<node_name>/key.p12
#keyStorePassword=WebAS
#trustStoreType=PKCS12
#trustStore=/was_root/IBM/WebSphere/AppServer/profiles/
<deployment_manager_name>/config/cells/<cell_name>/nodes/
<node_name>/trust.p12
#trustStorePassword=WebAS
```

Assim como no arquivo `catServer3.props`, é possível usar os comentários que já estão fornecido no arquivo *samples_home*`/security_extauth/client3.props` com as atualizações apropriadas para as variáveis *was_root*, *<deployment_manager_name>*, *<cell_name>* e *<node_name>* para corresponderem ao seu ambiente.

Ponto de verificação de lições:

Você configurou as propriedades SSL para o servidor de catálogos.

Lição 3.3: Executar a Amostra

Reinicie todos os servidores e execute o aplicativo de amostra novamente. Você deve poder executar as etapas sem nenhum problema.

Consulte “Lição 2.4: Instalar e Executar a Amostra” na página 86 para obter mais informações sobre como executar e instalar o aplicativo de amostra.

Módulo 4: Usar a Autorização do Java Authentication and Authorization Service (JAAS) no WebSphere Application Server

Agora que você configurou a autenticação de clientes, é possível configurar ainda mais a autorização para conceder aos usuários diferentes permissões. Por exemplo, um usuário "operador" pode apenas visualizar dados, enquanto que um usuário "gerente" pode executar todas as operações.

Após autenticar um cliente, como no módulo anterior neste tutorial, é possível fornecer privilégios de segurança por meio dos mecanismos de autorização do eXtreme Scale. O módulo anterior deste tutorial demonstrou como ativar a autenticação para uma grade de dados usando a integração com o WebSphere Application Server. Como resultado, nenhum cliente não autenticado pode se conectar aos servidores eXtreme Scale ou submeter solicitações para seu sistema. Entretanto, todo cliente autenticado tem a mesma permissão ou privilégios para o servidor, como de leitura, gravação ou exclusão de dados armazenados nos mapas do ObjectGrid. Os clientes também podem emitir qualquer tipo de consulta.

Esta parte do tutorial demonstra como usar a autorização do eXtreme Scale para fornecer diferentes privilégios para usuários autenticados. O WebSphere eXtreme Scale usa um mecanismo de autorização baseado em permissão. É possível designar categorias de permissão diferentes que são representadas por diferentes classes de permissão. Esse módulo apresenta a classe MapPermission. Para obter uma lista de todas as permissões possíveis, consulte “Programação de Autorização de Cliente” na página 827.

No WebSphere eXtreme Scale, a classe `com.ibm.websphere.objectgrid.security.MapPermission` representa permissões para os recursos do eXtreme Scale, especificamente os métodos das interfaces ObjectMap ou JavaMap. O WebSphere eXtreme Scale define as seguintes cadeias de permissões para acesso aos métodos de ObjectMap e JavaMap:

- **read**: Concede permissão para ler os dados do mapa.
- **write**: Concede permissão para atualizar os dados no mapa.
- **insert**: Concede permissão para inserir os dados no mapa.
- **remove**: Concede permissão para remover os dados do mapa.
- **invalidate**: Concede permissão para invalidar os dados a partir do mapa.
- **all**: Concede todas as permissões para ler, gravar, inserir, remover e invalidar.

A autorização ocorre quando um cliente do eXtreme Scale usa uma API de acesso a dados, como o ObjectMap, o JavaMap ou as APIs EntityManager. O tempo de execução verifica as permissões do mapa correspondente quando o método é chamado. Se as permissões necessárias não forem concedidas ao cliente, isso resultará em uma exceção AccessControlException. Este tutorial demonstra como usar a autorização do Java Authentication and Authorization Service (JAAS) para conceder acesso de mapa de autorização para diferentes usuários.

Objetivos do aprendizado

Depois de concluir as lições neste módulo, você saberá como:

- Ativar a autorização para WebSphere eXtreme Scale.
- Ativar a autorização baseada no usuário

Tempo Necessário

Este módulo leva cerca de 60 minutos.

Lição 4.1: Ativar a Autorização do WebSphere eXtreme Scale

Para ativar a autorização no WebSphere eXtreme Scale, você deve ativar a segurança em um ObjectGrid específico.

Para ativar a autorização no ObjectGrid, você deve configurar o atributo **securityEnabled** para true desse ObjectGrid específico no arquivo XML. Para este tutorial, é possível usar o arquivo `XSDeployment_sec.ear` a partir do diretório *samples_home*`/WASSecurity`, que já possui a segurança configurada no arquivo `objectGrid.xml`, ou é possível editar o arquivo `objectGrid.xml` existente para ativar a segurança. Esta lição demonstra como editar o arquivo para ativar a segurança.

1. Opcional: Extraia os arquivos no arquivo `XSDeployment.ear` e, em seguida, descompacte o arquivo `XSDeploymentWeb.war`.
2. Opcional: Abra o arquivo `objectGrid.xml` e configure o atributo **securityEnabled** para `true` no nível do ObjectGrid. A seguir há um exemplo desse atributo:

```
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">

    <objectGrids>
        <objectGrid name="Grid" txTimeout="15" securityEnabled="true">
               <backingMap name="Map1" />
        </objectGrid>
    </objectGrids>

</objectGridConfig>
```

   Se diversos ObjectGrids estiverem definidos, esse atributo deverá ser configurado em cada grade.
3. Opcional: Recompacte os arquivos `XSDeploymentWeb.war` e `XSDeployment.ear` para incluir suas mudanças.
4. Necessário: Desinstale o arquivo `XSDeployment.ear` e, em seguida, instale o arquivo `XSDeployment.ear`. É possível usar o arquivo modificado nas etapas anteriores ou instalar o arquivo `XSDeployment_sec.ear` que é fornecido no diretório *samples_home*`/WASSecurity`. Consulte o “Lição 2.4: Instalar e Executar a Amostra” na página 86 para obter informações adicionais sobre a instalação do aplicativo.
5. Reinicie todos os servidores de aplicativos para ativar a autorização do WebSphere eXtreme Scale.

Ponto de verificação de lições:

Você ativou a segurança no ObjectGrid, que também ativa a autorização na grade de dados.

Lição 4.2: Ativar Autorização Baseada no Usuário

No módulo de autenticação deste tutorial, dois usuários foram criados: `operator` e `manager`. É possível designar permissões diferentes para esses usuários com a autorização Java Authentication and Authorization Service (JAAS).

Definindo a Política de Autorização do Java Authentication and Authorization Service (JAAS) Usando os Principals do Usuário:

É possível designar permissões para os usuários criados anteriormente. Designe permissões somente leitura ao usuário `operator` para todos os mapas. Designe ao usuário `manager` todas as permissões. Use o arquivo de política de autorização JAAS para conceder permissões para os principals.

Edite o arquivo de autorização do JAAS. O arquivo `xAuth3.policy` está no diretório *samples_home*`/security_extauth`.

```
grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
    principal javax.security.auth.x500.X500Principal
    "CN=operator,O=acme,OU=OGSample" {
    permission com.ibm.websphere.objectgrid.security.MapPermission "Grid.Map1", "read";
};

grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
    principal javax.security.auth.x500.X500Principal
    "CN=manager,O=acme,OU=OGSample" {
    permission com.ibm.websphere.objectgrid.security.MapPermission "Grid.Map1", "all";
};
```

Neste arquivo, o código base `http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction` é uma URL reservada especialmente para o ObjectGrid. Todas as permissões do ObjectGrid concedidas aos principals devem usar esse código base especial. As seguintes permissões são designadas nesse arquivo:

- A primeira instrução de concessão concede permissão `read` para o principal `"CN=operator,O=acme,OU=OGSample"`. O usuário `"CN=operator,O=acme,OU=OGSample"` possui permissão somente leitura para o mapa Map1 da instância Grid do ObjectGrid.
- A segunda instrução de concessão concede a permissão de mapa 'all' para o principal do `"CN=manager,O=acme,OU=OGSample"`. O usuário `"CN=manager,O=acme,OU=OGSample"` possui permissão all para o mapa Map1 na instância Grid do ObjectGrid.

Configurando o Arquivo de Política de Autorização JAAS Usando as Propriedades da JVM:

Use as seguintes etapas para configurar as propriedades JVM para os servidores xs1 e xs2, que estão no cluster xsCluster. Se estiver usando uma topologia diferente da topologia de amostra usada neste tutorial, configure o arquivo em todos os servidores de contêiner.

1. No console administrativo, clique em **Servidores** > **Servidores de Aplicativos** > *server_name* > **Gerenciamento Java e Processos** > **Definição de Processo** > **Java virtual machine**
2. Inclua os seguintes argumentos JVM genéricos:

   `-Djava.security.policy=`*samples_home*`/security_extauth/xsAuth3.policy`
3. Clique em **OK** e salve as mudanças.

Executando os Aplicativos de Amostra para Testar a Autorização:

É possível usar o mesmo aplicativo de amostra para testar as configurações de autorização. O usuário gerenciador possui todas as permissões no mapa Map1,

inclusive permissões para exibir e incluir funcionários. O usuário operador pode apenas visualizar os funcionários porque esse usuário receber permissão somente leitura.

1. Reinicie todos os servidores de aplicativos que estão executando servidores de contêiner. Para este tutorial, reinicie os servidores `xs1` e `xs2`.
2. Abra o aplicativo `EmployeeManagementWeb`. Em um navegador da web, abra `http://<host>:<port>/EmployeeManagermentWeb/management.jsp`.
3. Efetue login no aplicativo usando qualquer nome de usuário e senha válidos.
4. Tente exibir um funcionário. Clique em **Exibir um Funcionário** e procure pelo endereço de e-mail `authemp1@acme.com`. Uma mensagem exibe que o usuário não pode ser localizado.
5. Incluir um funcionário. Clique em **Incluir um Funcionário**. Inclua o email `authemp1@acme.com`, o nome fornecido `Joe` e o sobrenome `Doe`. Clique em **Enviar**. Uma mensagem exibe que o funcionário foi incluído.
6. Edite o arquivo *samples_home*`/security_extauth/client3.props`. Altere o valor de propriedade credentialGeneratorProps a partir do `gerenciador manager1` para `operador operator1`. Depois de editar o arquivo, o servlet usará o nome do usuário "operador" e a senha "operator1" para se autenticar nos servidoresWebSphere eXtreme Scale.
7. Reinicie o cluster appCluster para selecionar as mudanças no arquivo *samples_home*`/security_extauth/client3.props`.
8. Tente exibir um funcionário. Clique em **Exibir um Funcionário** e procure pelo endereço de e-mail `authemp1@acme.com`. O funcionário é exibido.
9. Incluir um funcionário. Clique em **Incluir um Funcionário**. Inclua o email `authemp2@acme.com`, o nome fornecido `Joe` e o sobrenome `Doe`. Clique em **Enviar**. A mensagem a seguir é exibida:

   ```
   Ocorre uma exceção ao Incluir o funcionário. Consulte abaixo para obter mensagens de exceção detalhadas.
   ```

   O texto da exceção detalhado é o seguinte:

   ```
   java.security.AccessControlException: Acesso negado
   (com.ibm.websphere.objectgrid.security.MapPermission Grid.Map1 insert)
   ```

   Esta mensagem é exibida porque o usuário `operator` não tem permissão para inserir dados no mapa Map1.

Se você estiver executando com uma versão do WebSphere Application Server anterior à Versão 7.0.0.11, um erro java.lang.StackOverflowError será exibido no servidor de contêiner. Este erro é causado por um problema com o IBM Developer Kit. O problema é corrigido no IBM Developer Kit fornecido com o WebSphere Application Server Versão 7.0.0.11 e posterior.

Ponto de verificação de lições:

Nesta lição, você configurou a autorização ao designar permissões para usuários específicos.

Módulo 5: Use o Utilitário `xscmd` para Monitorar as Grades de Dados e Mapas

O utilitário **`xscmd`** pode ser usado para mostrar as grades de dados e tamanhos de mapa principais da grade de dados `Grade`. A ferramenta **`xscmd`** usa o MBean para consultar todos os artefatos grade de dados, tais como os shards primários, os shards de réplica, servidores de contêiner, tamanhos de mapa, e outros dados.

Para este tutorial, o servidor de catálogos está em execução como um servidor Java SE independente. Os servidores de contêiner estão em execução nos servidores de aplicativos do WebSphere Application Server.

Para o servidor de catálogos, um servidor MBean é criado na Java virtual machine (JVM) padrão. Quando a ferramenta **xscmd** é usada no servidor de catálogos, a segurança do WebSphere eXtreme Scale é usada.

Para os servidores de contêiner, o tempo de execução do WebSphere eXtreme Scale registra o beans gerenciados (MBean) com o servidor MBean que é criado pelo tempo de execução do WebSphere Application Server. A segurança usada pela ferramenta **xscmd** é fornecida pela segurança MBean do WebSphere Application Server.

1. Usando uma ferramenta de linha de comandos, abra o diretório *DMGR_PROFILE*/bin .
2. Executar a ferramenta **xscmd**. Use os parâmetros **-c showPlacement -st P** como nos exemplos a seguir:

   Linux UNIX

   ```
   xscmd.sh -c showPlacement -cep localhost:16099 -g Grid -ms mapSet -sf P
   -user manager -pwd manager1
   ```

   Windows

   ```
   xscmd.bat -c showPlacement -cep localhost:16099 -g Grid -m mapSet -sf P
   -user manager -pwd manager1
   ```

   Atenção:

   Se você utilizar o comando a seguir para acessar a grade de dados, também poderá estar autorizado a desempenhar ações administrativas, como listAllJMXAddresses:

   ```
   ./xscmd.sh -user <user> -password <password> <other_parameters>
   ```

   Se esta operação funciona para este usuário, qualquer operação **xscmd** também pode ser executada pelo mesmo usuário. Para obter informações adicionais, consulte “Resolução de Problemas de Segurança” na página 893
   O nome do usuário e a senha são passados para o servidor de catálogos para autenticação.
3. Visualize os resultados do comando.

   ```
   *** Showing all primaries for grid - Grid & mapset - mapSet
   Partition Container Host Server
   0 myCell02\myNode04\xs2_C-1 myhost.mycompany.com myCell02\myNode04\xs2
   1 myCell02\myNode04\xs2_C-1 myhost.mycompany.com myCell02\myNode04\xs2
   2 myCell02\myNode04\xs2_C-1 myhost.mycompany.com myCell02\myNode04\xs2
   3 myCell02\myNode04\xs2_C-1 myhost.mycompany.com myCell02\myNode04\xs2
   4 myCell02\myNode04\xs2_C-1 myhost.mycompany.com myCell02\myNode04\xs2
   ```
4. Executar a ferramenta **xscmd**. Use o parâmetro **-c showMapSizes** como nos exemplos a seguir:

   Linux UNIX

   ```
   xscmd.sh -c showMapSizes -cep localhost:16099 -g Grid -ms mapSet  -user manager -pwd manager1
   ```

   Windows

   ```
   xscmd.bat -c showMapSizes -cep localhost:16099 -g Grid -ms mapSet -user manager -pwd manager1
   ```

   O nome do usuário e a senha são passados para o servidor de catálogos para autenticação. Depois de executar o comando, será solicitado fornecer o ID de

usuário e senha do WebSphere Application Server para autenticação no WebSphere Application Server. Você deve fornecer estas informações de login porque a opção **-c showMapSizes** obtém o tamanho de mapa de cada servidor de contêiner, o qual requer a segurança do WebSphere Application Server.

5. Opcional: É possível alterar o arquivo `PROFILE/properties/sas.client.props` para executar o comando sem o ID do usuário e a senha necessários. Altere a propriedade com.ibm.CORBA.loginSource a partir do `prompt` para `propriedades` e, em seguida, forneça o ID de usuário e a senha. Um exemplo das propriedades no arquivo `PROFILE/properties/sas.client.props` é o seguinte:

   ```
   com.ibm.CORBA.loginSource=properties
   # RMI/IIOP user identity
   com.ibm.CORBA.loginUserid=Admin
   com.ibm.CORBA.loginPassword=xxxxxx
   ```

6. Opcional: Se estiver usando o comando **xscmd** em uma instalação independente do WebSphere eXtreme Scale, você deverá incluir as opções a seguir:
   - Se estiver usando a segurança do WebSphere eXtreme Scale:

     ```
     -user
     -pwd
     ```

   - Se estiver usando a segurança do WebSphere eXtreme Scale com geração de credencial customizada:

     ```
     -user
     -pwd
     -cgc
     -cgp
     ```

   - Se SSL estiver ativado:

     ```
     -tt
     -cxpv
     -prot
     -ks
     -ksp
     -kst
     -ts
     -tsp
     -tst
     ```

   Se a segurança do WebSphere eXtreme Scale e o SSL estiverem ativados, ambos os conjuntos de parâmetros serão necessários.

Tarefas relacionadas:

Monitorando com o Utilitário **xscmd**
O utilitário **xscmd** substitui o utilitário **xsadmin** de amostra como uma ferramenta de monitoramento e administração totalmente suportada. Com o utilitário **xscmd**, é possível exibir informações textuais sobre sua topologia do WebSphere eXtreme Scale.

Administrando com o Utilitário **xscmd**
Com o utilitário **xscmd**, é possível concluir tarefas administrativas no ambiente, tal como: estabelecer links de replicação multi-master, substituir o quorum e parar os grupos de servidores com o comando teardown.

Ponto de verificação de lições

Você usou a ferramenta **xscmd** para monitorar as grades de dados e os mapas em sua configuração.

Tutorial: Executando Pacotes Configuráveis do eXtreme Scale na Estrutura do OSGi

A amostra OSGi é construída sobre as amostras do serializador do Google Protocol Buffers. Quando esse conjunto de lições for concluído, os plug-ins de amostra do serializador terão sido executados na estrutura OSGi.

Objetivos do aprendizado

Esta amostra demonstra os pacotes configuráveis OSGi. O plug-in serializador é incidental e não é necessário. A amostra de OSGi está disponível na galeria de amostras do WebSphere eXtreme Scale. Você deve fazer o download da amostra e extraí-la no diretório *wxs_home*/samples. O diretório raiz para a amostra OSGi é wxs_home/samples/OSGiProto.

Os exemplos de comando neste tutorial assumem que você está executando no sistema operacional UNIX. Você deve ajustar o exemplo de comando para ser executado em um sistema operacional Windows.

Após concluir as lições neste tutorial, você entenderá os conceitos de amostra do OSGi e saberá como concluir os objetivos a seguir:

- Instalar o pacote configurável do servidor WebSphere eXtreme Scale no contêiner OSGi para iniciar o servidor eXtreme Scale.
- Configurar seu ambiente de desenvolvimento do eXtreme Scale para executar o cliente de amostra.
- Usar o comando xscmd para consultar a classificação do serviço do pacote configurável da amostra, fazer upgrade dele para uma nova classificação de serviço e verificar a nova classificação de serviço.

Tempo Necessário

Esse módulo demora aproximadamente 60 minutos para ser concluído.

Pré-requisitos

Além de fazer download e extrair as amostras do serializador, este tutorial também possui os pré-requisitos a seguir:

- Instalar e extrair o produto eXtreme Scale
- Configurar o Eclipse Equinox Environment

Introdução: Iniciando e Configurando o Servidor e o Contêiner do eXtreme Scale para Executar Plug-ins na Estrutura do OSGi

Neste tutorial, inicie um servidor eXtreme Scale na estrutura do OSGi, inicie um contêiner do eXtreme Scale e ligue os plug-ins de amostra com o ambiente de tempo de execução do eXtreme Scale.

Objetivos do aprendizado

Depois de concluir as lições neste tutorial, você entenderá os conceitos de amostra do OSGi e saberá como concluir os seguintes objetivos:

- Instalar o pacote configurável do servidor WebSphere eXtreme Scale no contêiner OSGi para iniciar o servidor eXtreme Scale.

- Configurar seu ambiente de desenvolvimento do eXtreme Scale para executar o cliente de amostra.
- Usar o comando xscmd para consultar a classificação do serviço do pacote configurável da amostra, fazer upgrade dele para uma nova classificação de serviço e verificar a nova classificação de serviço.

Tempo Necessário

Esse tutorial demora aproximadamente 60 minutos para ser concluído. Se você explorar outros conceitos relacionados a este tutorial, poderá demorar mais tempo para ele ser concluído.

Nível de qualificação

Intermediário.

Público

Desenvolvedores e administradores que desejam construir, instalar e executar os pacotes configuráveis do eXtreme Scale na estrutura do OSGi.

Requisitos do Sistema

- Cliente da linha de comandos Luminis OSGi Configuration Admin, versão 0.2.5
- Apache Felix File Install, versão 3.0.2
- Quando usar o Eclipse Gemini como o provedor de contêiner blueprint, os seguintes itens são necessários:
  - Eclipse Gemini Blueprint, versão 1.0.0
  - Spring Framework, versão 3.0.5
  - SpringSource AOP Alliance API, versão 1.0.0
  - SpringSource Apache Commons Logging, versão 1.1.1
- Quando usar o Aries Apache como o provedor do Blueprint Container, você deve ter os seguintes requisitos:
  - Apache Aries, captura instantânea mais recente
  - Biblioteca ASM
  - Criação de Log PAX

Pré-requisitos

Para concluir este tutorial, você deve fazer o download da amostra e extraí-la no diretório `wxs_home/samples`. O diretório raiz para a amostra OSGi é `wxs_home/samples/OSGiProto`.

Resultados Esperados:

Ao concluir este tutorial, você terá instalado os pacotes configuráveis de amostra e executado um cliente do eXtreme Scale para inserir dados na grade. Também espera-se que esses pacotes configuráveis de amostra sejam consultados e atualizados usando os recursos dinâmicos fornecidos pelo contêiner OSGi.

Conceitos relacionados:

"Visão Geral da Estrutura do OSGi" na página 162
O OSGi define um sistema módulo dinâmico para Java. A plataforma de serviço OSGi possui uma arquitetura em camadas e é projetada para ser executada em vários perfis padrão Java. É possível iniciar servidores e clientes do WebSphere eXtreme Scale em um contêiner OSGi.

Tarefas relacionadas:

"Instalando a Estrutura do Eclipse Equinox OSGi com o Eclipse Gemini para Clientes e Servidores" na página 164
Se desejar implementar o WebSphere eXtreme Scale na estrutura do OSGi, você deverá configurar o Ambiente do Eclipse Equinox.

Referências relacionadas:

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Módulo 1: Preparando para Instalar e Configurar os Pacotes Configuráveis do Servidor eXtreme Scale

Conclua este módulo para explorar os pacotes configuráveis de amostra OSGi e examine os arquivos de configuração que você usa para configurar o servidor eXtreme Scale.

Objetivos do aprendizado

Depois de concluir as lições neste módulo, você entenderá os conceitos e saberá como concluir os objetivos a seguir:

- Localizar e explorar os pacotes configuráveis que estão incluídos na amostra OSGi.
- Examine os arquivos de configuração que são usados para configurar a grade e o servidor do eXtreme Scale.

Lição 1.1: Entendendo os Pacotes Configuráveis OSGi de Amostra

Conclua esta lição para localizar e explorar os pacotes configuráveis que são fornecidos na amostra do OSGi.

Pacotes Configuráveis OSGi de Amostra:
Diferente dos pacotes configuráveis que estão configurados no arquivo `config.ini`, que é mostrado no tópico sobre como configurar o ambiente do Eclipse Equinox, os seguintes pacotes configuráveis adicionais são usados na amostra OSGi:

`objectgrid.jar`
O pacote configurável do tempo de execução do servidor WebSphere eXtreme Scale. Este pacote configurável está localizado no diretório *`wxs_home`*`/lib directory`.

`com.google.protobuf_2.4.0a.jar`
O pacote configurável Google Protocol Buffers, versão 2.4.0a. Este pacote configurável está localizado no diretório *`wxs_sample_osgi_root`*`/lib`.

ProtoBufSamplePlugins-1.0.0.jar
Versão 1.0.0 do pacote configurável de plug-in do usuário com as implementações de plug-in ObjectGridEventListener e MapSerializerPlugin. Este pacote configurável está localizado no diretório *wxs_sample_osgi_root*/lib. Os serviços são configurados com a classificação de serviço 1.

Esta versão usa o XML Blueprint padrão para configurar os serviços de plug-in do eXtreme Scale. A classe de serviço é uma classe implementada pelo usuário na interface do WebSphere eXtreme Scale, com.ibm.websphere.objectgrid.plugins.osgi.PluginServiceFactory. A classe implementada pelo usuário cria um bean para cada solicitação e funciona de modo semelhante a um bean de protótipo com escopo definido.

ProtoBufSamplePlugins-2.0.0.jar
Versão 2.0.0 do pacote configurável de plug-in do usuário com as implementações de plug-in ObjectGridEventListener e MapSerializerPlugin de amostra. Este pacote configurável está localizado no diretório *wxs_sample_osgi_root*/lib. Os serviços são configurados com a classificação de serviço 2.

Esta versão usa o XML Blueprint padrão para configurar os serviços de plug-in do eXtreme Scale. A classe de serviço está usando uma classe integrada do WebSphere eXtreme Scale, com.ibm.websphere.objectgrid.plugins.osgi.PluginServiceFactoryImpl, que usa o serviço do BlueprintContainer. Usando a configuração XML blueprint padrão, os beans podem ser configurados como um escopo de protótipo ou escopo singleton. O bean não é configurado como escopo de shard.

ProtoBufSamplePlugins-Gemini-3.0.0.jar
Versão 3.0.0 do pacote configurável de plug-in do usuário com as implementações de plug-in ObjectGridEventListener e MapSerializerPlugin. Este pacote configurável está localizado no diretório *wxs_sample_osgi_root*/lib. Os serviços são configurados com o serviço de classificação 3.

Esta versão usa o XML blueprint específico do Eclipse Gemini para configurar os serviços de plug-in do eXtreme Scale. A classe de serviço está usando uma classe integrada do WebSphere eXtreme Scale, com.ibm.websphere.objectgrid.plugins.osgi.PluginServiceFactoryImpl, que usa o serviço do BlueprintContainer. A maneira de configurar um bean do escopo de shard é usar uma abordagem específica do Gemini. Esta versão configura o bean myShardListener como um bean de escopo de shard ao fornecer {http://www.ibm.com/schema/objectgrid}shard como o valor do escopo e configurar um atributo fictício para que o escopo customizado seja reconhecido pelo Gemini. Isso ocorre devido ao seguinte problema do Eclipse: https://bugs.eclipse.org/bugs/show_bug.cgi?id=348776

ProtoBufSamplePlugins-Aries-4.0.0.jar
Versão 4.0.0 do pacote configurável de plug-in do usuário com as implementações de plug-in ObjectGridEventListener e MapSerializerPlugin de amostra. Este pacote configurável está localizado no diretório *wxs_sample_osgi_root*/lib. Os serviços são configurados com a classificação de serviço 4.

Esta versão usa o XML blueprint padrão para configurar os serviços de plug-in do eXtreme Scale. A classe de serviço está usando uma classe integrada do WebSphere eXtreme Scale, com.ibm.websphere.objectgrid.plugins.osgi.PluginServiceFactoryImpl, que

usa o serviço do BlueprintContainer. Ao usar a configuração XML blueprint padrão, os beans podem ser configurados usando um escopo customizado. Esta versão configura o myShardListenerbean como bean de shard com escopo definido ao fornecer `{http://www.ibm.com/schema/objectgrid}shard` como o valor do escopo.

ProtoBufSamplePlugins-Activator-5.0.0.jar
Versão 5.0.0 do pacote configurável de plug-in do usuário com as implementações de plug-in ObjectGridEventListener e MapSerializerPlugin de amostra. Este pacote configurável está localizado no diretório *wxs_sample_osgi_root*`/lib`. Os serviços são configurados com o serviço de classificação 5.

Esta versão não é usada em todo o contêiner blueprint. Nesta versão, os serviços são registrados usando o registro de serviço OSGi. A classe de serviço é uma classe implementada pelo usuário para a interface do WebSphere eXtreme Scale, com.ibm.websphere.objectgrid.plugins.osgi.PluginServiceFactory. A classe implementada pelo usuário cria um bean para cada solicitação. Ela funciona de modo semelhante a um bean de protótipo com escopo definido.

Ponto de verificação de lições:

Ao explorar os pacotes configuráveis que são fornecidos com a amostra OSGi, é possível entender melhor como desenvolver suas próprias implementações que serão executadas no contêiner OSGi.

Você aprendeu:

- Sobre os pacotes configuráveis que estão incluídos com a amostra OSGi
- O local desses pacotes configuráveis
- A classificação de serviço com a qual cada pacote configurável foi configurado

Lição 1.2: Entender os Arquivos de Configuração do OSGi

A amostra OSGi inclui arquivos de configuração usados para iniciar e configurar a grade e o servidor do WebSphere eXtreme Scale.

Arquivos de Configuração OSGi:
Nesta lição, você explorará os arquivos de configuração a seguir que estão incluídos na amostra OSGI:

- `collocated.server.properties`
- `protoBufObjectGrid.xml`
- `protoBufDeployment.xml`
- `blueprint.xml`

collocated.server.properties

Uma configuração do servidor é necessária para iniciar um servidor. Quando o pacote configurável do servidor eXtreme Scale é iniciado, ele não inicia um servidor. Ele aguarda o PID de configuração, `com.ibm.websphere.xs.server`, ser criado com um arquivo de propriedades do servidor. Esse arquivo de propriedades do servidor especifica o nome do servidor, o número da porta e outras propriedades do servidor.

Na maioria dos casos, uma configuração é criada para configurar o arquivo de propriedades do servidor. Raramente, você pode querer apenas iniciar um servidor com cada propriedade configurada para um valor padrão. Nesse caso, é possível criar uma configuração denominada `com.ibm.websphere.xs.server` com o valor configurado para `padrão`.

Para obter mais detalhes sobre o arquivo de propriedades de servidor, consulte o tópico Arquivo de Propriedades do Servidor.

O arquivo de propriedades do servidor de amostra OSGi inicia um catálogo único. Esse arquivo de propriedades de amostra inicia um serviço de catálogo e um servidor de contêiner únicos no processo da estrutura do OSGi. Os clientes do eXtreme Scale se conectam à porta 2809 e os clientes do JMX se conectam à porta 1099. O conteúdo do arquivo de propriedades do servidor de amostra é:

```
serverName=collocatedServer
isCatalog=true
catalogClusterEndPoints=collocatedServer:localhost:6601:6602
traceSpec=ObjectGridOSGi=all=enabled
traceFile=logs/trace.log
listenerPort=2809
JMXServicePort=1099
```

protoBufObjectGrid.xml

O arquivo XML do descritor do ObjectGrid `protoBufObjectGrid.xml` de amostra contém o conteúdo a seguir, com comentários removidos.

```
<objectGridConfig
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
    xmlns="http://ibm.com/ws/objectgrid/config">

    <objectGrids>
        <objectGrid name="Grid" txTimeout="15">

            <bean id="ObjectGridEventListener"
                osgiService="myShardListener"/>

            <backingMap name="Map" readOnly="false"
                lockStrategy="PESSIMISTIC" lockTimeout="5"
                copyMode="COPY_TO_BYTES"
                pluginCollectionRef="serializer"/>

        </objectGrid>
    </objectGrids>

    <backingMapPluginCollections>
        <backingMapPluginCollection id="serializer">
            <bean id="MapSerializerPlugin"
                osgiService="myProtoBufSerializer"/>"/>
        </backingMapPluginCollection>
    </backingMapPluginCollections>
 </objectGridConfig>
```

Há dois plug-ins configurados neste arquivo XML do descritor do ObjectGrid:

ObjectGridEventListener
O plug-in de nível de shard. Para cada instância do ObjectGrid, há uma instância de ObjectGridEventListener. Ela é configurada para usar o myShardListener de serviço do OSGi. Isso significa que quando a grade é criada, o plug-in ObjectGridEventListener usa o serviço OSGi myShardListener com a classificação deserviço mais alta disponível.

MapSerializerPlugin
O plug-in de nível de mapa. Para o mapa de apoio denominado `Map`, há um plug-in MapSerializerPlugin configurado. Ele é configurado para usar

o serviço OSGimyProtoBufSerializer. Isso significa que quando o mapa é criado, o plug-in MapSerializerPlugin usa o serviço myProtoBufSerializer com a maior classificação de serviço obtida disponível.

protoBufDeployment.xml

O arquivo XML do descritor de implementação descreve a política de implementação para a grade denominada `Grid`, que usa cinco partições. Consulte o exemplo de código a seguir do arquivo XML:

```
<deploymentPolicy
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://ibm.com/ws/objectgrid/deploymentPolicy ../deploymentPolicy.xsd"
 xmlns="http://ibm.com/ws/objectgrid/deploymentPolicy">

  <objectgridDeployment objectgridName="Grid">
    <mapSet name="MapSet" numberOfPartitions="5">
      <map ref="Map"/>
    </mapSet>
  </objectgridDeployment>
</deploymentPolicy>
```

blueprint.xml

Como alternativa para o uso do arquivo `collocated.server.properties` em conjunto com o PID de configuração, `com.ibm.websphere.xs.server`, o XML do ObjectGrid e os arquivos XML de implementação podem ser incluídos em um pacote configurável OSGi, juntamente com um arquivo XML Blueprint, conforme mostrado no exemplo a seguir :

```
<blueprint
   xmlns="http://www.osgi.org/xmlns/blueprint/v1.0.0"
       xmlns:objectgrid="http://www.ibm.com/schema/objectgrid"
       default-activation="lazy">

    <objectgrid:server id="server" isCatalog="true"
                name="server"
                tracespec="ObjectGridOSGi=all=enabled"
                tracefile="C:/Temp/logs/trace.log"
                workingDirectory="C:/Temp/working"
                jmxport="1099">
         <objectgrid:catalog host="localhost" port="2809"/>
    </objectgrid:server>

    <objectgrid:container id="container"
  objectgridxml="/META-INF/objectgrid.xml"
       deploymentxml="/META-INF/deployment.xml"
  server="server"/>
</blueprint>
```

Ponto de verificação de lições:

Nesta lição, você aprendeu sobre os arquivos de configuração que são usados na amostra OSGi. Agora, quando iniciar e configurar a grade e o servidor eXtreme Scale, você entenderá quais arquivos estão sendo usados nestes processos e como esses arquivos interagem com seus plug-ins na estrutura do OSGi.

Módulo 2: Instalando e Iniciando Pacotes Configuráveis do eXtreme Scale na Estrutura do OSGi

Use as lições neste módulo para instalar o pacote configurável do servidor eXtreme Scale no contêiner OSGi e iniciar o servidor WebSphere eXtreme Scale.

Iniciar o servidor na estrutura do OSGi não significa que seus pacotes configuráveis OSGi estão prontos para execução. Você deve configurar as

propriedades do servidor e os contêineres para que os pacotes configuráveis OSGi que forem instalados sejam reconhecidos e executados corretamente.

Objetivos do aprendizado

Após concluir as lições neste módulo, você entenderá os conceitos e saberá como concluir as tarefas a seguir:

- Instalar os pacotes configuráveis do eXtreme Scale usando o console do Equinox OSGi.
- Configurar o servidor eXtreme Scale.
- Configure o contêiner do eXtreme Scale.
- Instale e inicie os pacotes configuráveis de amostra do eXtreme Scale.

Pré-requisitos

Para concluir este módulo, as tarefas a seguir são necessárias antes de iniciar:

- Instalar e extrair o produto eXtreme Scale
- Configurar o Eclipse Equinox Environment

Você também deve preparar para acessar os seguintes arquivos para concluir as lições neste módulo:

- Pacote Configurável `objectgrid.jar`. Instale esse pacote configurável do eXtreme Scale.
- Arquivo `collocated.server.properties`. Inclua as propriedades do servidor nesse arquivo de configuração.

Espera-se que os seguintes pacotes configuráveis sejam instalados e iniciados:

- Pacote configurável `protobuf-java-2.4.0a-bundle.jar`
- Pacote configurável `ProtoBufSamplePlugins-1.0.0.jar`

Lição 2.1: Iniciar o Console e Instalar o Pacote Configurável do Servidor eXtreme Scale

Nesta lição, use o console do Equinox OSGi para instalar o pacote configurável do servidor WebSphere eXtreme Scale.

1. Execute o seguinte comando para iniciar o console Equinox OSGi:

   ```
   cd equinox_root
   java -jar plugins\org.eclipse.osgi_3.6.1.R36x_v20100806.jar -console
   ```

2. Após iniciar o console OSGi, emita o comando `ss` no console e os pacotes configuráveis a seguir serão iniciados:

   Atenção: Se você concluiu a tarefa, Instalando os pacotes configuráveis do eXtreme Scale, o pacote configurável já terá sido ativado. Se o pacote configurável for iniciado, pare-o antes de concluir essa etapa.

   Saída do Eclipse Gemini:

   ```
   osgi> ss
   Framework is launched.
   id State Bundle
   0 ACTIVE org.eclipse.osgi_3.6.1.R36x_v20100806
   1 ACTIVE org.eclipse.osgi.services_3.2.100.v20100503
   2 ACTIVE org.eclipse.osgi.util_3.2.100.v20100503
   3 ACTIVE org.eclipse.equinox.cm_1.0.200.v20100520
   4 ACTIVE com.springsource.org.apache.commons.logging_1.1.1
   5 ACTIVE com.springsource.org.aopalliance_1.0.0
   6 ACTIVE org.springframework.aop_3.0.5.RELEASE
   7 ACTIVE org.springframework.asm_3.0.5.RELEASE
   8 ACTIVE org.springframework.beans_3.0.5.RELEASE
   ```

```
9 ACTIVE org.springframework.context_3.0.5.RELEASE
10 ACTIVE org.springframework.core_3.0.5.RELEASE
11 ACTIVE org.springframework.expression_3.0.5.RELEASE
12 ACTIVE org.apache.felix.fileinstall_3.0.2
13 ACTIVE net.luminis.cmc_0.2.5
14 ACTIVE org.eclipse.gemini.blueprint.core_1.0.0.RELEASE
15 ACTIVE org.eclipse.gemini.blueprint.extender_1.0.0.RELEASE
16 ACTIVE org.eclipse.gemini.blueprint.io_1.0.0.RELEASE
```

Saída do Apache Aries:

```
osgi> ss
Framework is launched.
id State Bundle
0 ACTIVE org.eclipse.osgi_3.6.1.R36x_v20100806
1 ACTIVE org.eclipse.osgi.services_3.2.100.v20100503
2 ACTIVE org.eclipse.osgi.util_3.2.100.v20100503
3 ACTIVE org.eclipse.equinox.cm_1.0.200.v20100520
4 ACTIVE org.ops4j.pax.logging.pax-logging-api_1.6.3
5 ACTIVE org.ops4j.pax.logging.pax-logging-service_1.6.3
6 ACTIVE org.objectweb.asm.all_3.3.0
7 ACTIVE org.apache.aries.blueprint_0.3.2.SNAPSHOT
8 ACTIVE org.apache.aries.util_0.4.0.SNAPSHOT
9 ACTIVE org.apache.aries.proxy_0.4.0.SNAPSHOT
10 ACTIVE org.apache.felix.fileinstall_3.0.2
11 ACTIVE net.luminis.cmc_0.2.5
```

3. Instale o pacote configurável `objectgrid.jar`. Para iniciar um servidor na Java virtual machine (JVM), é necessário instalar um pacote configurável do servidor eXtreme Scale. Este pacote configurável do servidor eXtreme Scale pode iniciar um servidor e criar contêineres. Use o comando a seguir para instalar o arquivo `objectgrid.jar`:

   ```
   osgi> install file:///wxs_home/lib/objectgrid.jar
   ```

   Consulte o seguinte exemplo:

   ```
   osgi> install file:///opt/wxs/ObjectGrid/lib/objectgrid.jar
   ```

   O Equinox exibe o ID do pacote configurável, por exemplo:

   ```
   Bundle id is 19
   ```

   Lembre-se: Seu ID do pacote configurável pode ser diferente. O caminho do arquivo deve ser uma URL absoluta para o caminho do pacote configurável. Caminhos relativos não são suportados.

Ponto de verificação de lições:

Nesta lição, você usou o console do Equinox OSGi para instalar o pacote configurável `objectgrid.jar`, o qual você usará para iniciar um servidor e criar um contêiner posteriormente neste tutorial.

Lição 2.2: Customizar e Configurar o Servidor eXtreme Scale

Use essa lição para customizar e incluir as propriedades do servidor para o servidor WebSphere eXtreme Scale.

1. Edite o arquivo `wxs_sample_osgi_root/projects/server /properties/collocated.server.properties`.
   a. Altere a propriedade do traceFile para `equinox_roo/logs/trace.log`.
2. Salve o arquivo.
3. Insira as linhas de código a seguir no console OSGI para criar a configuração do servidor a partir do arquivo. O exemplo a seguir é exibido em diversas linhas para propósitos de publicação.

```
osgi> cm create com.ibm.websphere.xs.server
osgi> cm put com.ibm.websphere.xs.server objectgrid.server.props
wxs_sample_osgi_root/projects/server./properties/collocated.server.properties
```

4. Para visualizar a configuração, execute o seguinte comando:

```
osgi> cm get com.ibm.websphere.xs.server
Configuration for service (pid) "com.ibm.websphere.xs.server"
(bundle location = null)
key value
----                    ----
objectgrid.server.props  wxs_sample_osgi_root/projects/server
/properties/collocated.server.properties
service.pid              com.ibm.websphere.xs.server
```

Ponto de verificação de lições:

Nessa lição, você editou o arquivo `wxs_sample_osgi_root/projects/server /properties/collocated.server.properties` para especificar as configurações do servidor, como o diretório ativo e o local para os arquivos de log de rastreio.

Lição 2.3: Configurar o Contêiner do eXtreme Scale

Conclua esta lição para configurar um contêiner, que inclui o arquivo descritor XML e o arquivo XML de implementação do ObjectGrid do WebSphere eXtreme Scale. Esses arquivos incluem a configuração para a grade e sua topologia.

Para criar um contêiner, primeiro crie um serviço de configuração usando o factory de serviço gerenciado pelo número de identificação do processo (PID), com.ibm.websphere.xs.container. A configuração do serviço é um factory de serviço gerenciado para que seja possível criar vários PIDs de serviço a partir do PID do factory. Em seguida, para iniciar o serviço do contêiner, configure os PIDs objectgridFile e deploymentPolicyFile para cada PID de serviço.

Conclua as seguintes etapas para customizar e incluir as propriedades do servidor para a estrutura do OSGi:

1. No console OSGI, insira o seguinte comando para criar o contêiner a partir do arquivo:

```
osgi> cm createf com.ibm.websphere.xs.container
PID: com.ibm.websphere.xs.container-1291179621421-0
```

2. Insira os comandos a seguir para ligar o PID recentemente criado aos arquivos XML do ObjectGrid.

   Lembre-se: O número de PID será diferente do número que está incluído neste exemplo.

```
osgi> cm put com.ibm.websphere.xs.container-1291179621421-0 objectgridFile wxs_sample_osgi_root/projects/server/META-INF/protoBufObjectgrid.xml

osgi> cm put com.ibm.websphere.xs.container-1291179621421-0 deploymentPolicyFile wxs_sample_osgi_root/projects/server/META-INF/protoBufDeployment.xml
```

3. Use o seguinte comando para exibir a configuração:

```
osgi> cm get com.ibm.websphere.xs.container-1291760127968-0
Configuration for service (pid) "com.ibm.websphere.xs.container-1291760127968-0"
(bundle location = null)

key value
------                  ------
deploymentPolicyFile   /opt/wxs/ObjectGrid/samples/OSGiProto/server/META-INF/protoBufDeployment.xml
objectgridFile         /opt/wxs/ObjectGrid/samples/OSGiProto/server/META-INF/protoBufObjectgrid.xml
service.factoryPid   com.ibm.websphere.xs.container
service.pid       com.ibm.websphere.xs.container-1291760127968-0
```

Ponto de verificação de lições:

Nesta lição, você criou um serviço de configuração, que foi usado para criar um contêiner do eXtreme Scale. Como os arquivos XML do ObjectGrid contêm a configuração para a grade e sua topologia, foi necessário vincular o contêiner criado para esses arquivos XML do ObjectGrid. Com essa configuração, o contêiner do eXtreme Scale pode reconhecer os pacotes configuráveis do OSGi que serão executados posteriormente neste tutorial.

Lição 2.4: Instalar o Google Protocol Buffers e os Pacotes Configuráveis do Plug-in de Amostra

Conclua este tutorial para instalar o pacote configurável `protobuf-java-2.4.0a-bundle.jar` e o pacote configurável de plug-in `ProtoBufSamplePlugins-1.0.0.jar` usando o console do Equinox OSGi.

Instale o Plug-in do Google Protocol Buffers:
Conclua as etapas a seguir para instalar o plug-in do Google Protocol Buffers.

No console OSGI, insira o comando a seguir para instalar o plug-in:

```
osgi> install file:///wxs_sample_osgi_root/lib/com.google.protobuf_2.4.0a.jar
```

A saída a seguir é exibida:

```
Bundle ID is 21
```

Visão Geral dos Pacotes Configuráveis do Plug-in de Amostra:
A amostra do OSGi inclui cinco pacotes configuráveis que incluem os plug-ins do eXtreme Scale, dentre eles um plug-in ObjectGridEventListener e MapSerializerPlugin customizado. O plug-in MapSerializerPlugin usa a amostra do Google Protocol Buffers e as mensagens fornecidas pela amostra do MapSerializerPlugin.

Os seguintes pacotes configuráveis estão localizados no diretório *wxs_sample_osgi_root*`/lib`: `ProtoBufSamplePlugins-1.0.0.jar` e o `ProtoBufSamplePlugins-2.0.0.jar`.

O arquivo `blueprint.xml` possui o seguinte conteúdo com comentários removidos:

```
<blueprint xmlns="http://www.osgi.org/xmlns/blueprint/v1.0.0">
 <bean id="myShardListener" class="com.ibm.websphere.samples.xs.proto.osgi.MyShardListenerFactory"/>
 <service ref="myShardListener" interface="com.ibm.websphere.objectgrid.plugins.osgi.PluginServiceFactory" ranking="1">
 </service>

 <bean id="myProtoBufSerializer" class="com.ibm.websphere.samples.xs.proto.osgi.ProtoMapSerializerFactory">
  <property name="keyType" value="com.ibm.websphere.samples.xs.serializer.app.proto.DataObjects1$OrderKey" />
  <property name="valueType" value="com.ibm.websphere.samples.xs.serializer.app.proto.DataObjects1$Order" />
 </bean>

 <service ref="myProtoBufSerializer" interface="com.ibm.websphere.objectgrid.plugins.osgi.PluginServiceFactory"
  ranking="1">
 </service>
</blueprint>
```

O arquivo XML Blueprint exporta dois serviços, myShardListener e myProtoBufSerializer. Esses dois serviços são referenciados no arquivo `protoBufObjectgrid.xml`.

Instalar o Pacote Configurável do Plug-in de Amostra:

Conclua as seguintes etapas para instalar o pacote configurável `ProtoBufSamplePlugins-1.0.0.jar`.

Execute o seguinte comando no console do Equinox OSGi para instalar o pacote configurável do plug-in `ProtoBufSamplePlugins-1.0.0.jar`:

```
osgi> install file:///wxs_sample_osgi_root/lib/ProtoBufSamplePlugins-1.0.0.jar
```

A saída a seguir é exibida:

```
Bundle ID is 22
```

Ponto de verificação de lições:

Nesta lição, você instalou o pacote configurável `protobuf-java-2.4.0a-bundle.jar` e o pacote configurável de plug-in `ProtoBufSamplePlugins-1.0.0.jar`.

Lição 2.5: Iniciar os Pacotes Configuráveis do OSGi

O servidor WebSphere eXtreme Scale é incluído em um pacote configurável do OSGi. Conclua esta lição para instalar o pacote configurável do servidor eXtreme Scale e também outros pacotes configuráveis OSGi que forem instalados.

1. Execute o comando **ss** para visualizar os IDs de cada pacote configurável.

   ```
   osgi> ss

   Framework is launched.

   id State Bundle
   0 ACTIVE org.eclipse.osgi_3.6.1.R36x_v20100806
   1 ACTIVE org.eclipse.osgi.services_3.2.100.v20100503
   2 ACTIVE org.eclipse.osgi.util_3.2.100.v20100503
   3 ACTIVE org.eclipse.equinox.cm_1.0.200.v20100520
   4 ACTIVE com.springsource.org.apache.commons.logging_1.1.1
   5 ACTIVE com.springsource.org.aopalliance_1.0.0
   6 ACTIVE org.springframework.aop_3.0.5.RELEASE
   7 ACTIVE org.springframework.asm_3.0.5.RELEASE
   8 ACTIVE org.springframework.beans_3.0.5.RELEASE
   9 ACTIVE org.springframework.context_3.0.5.RELEASE
   10 ACTIVE org.springframework.core_3.0.5.RELEASE
   11 ACTIVE org.springframework.expression_3.0.5.RELEASE
   12 ACTIVE org.apache.felix.fileinstall_3.0.2
   13 ACTIVE net.luminis.cmc_0.2.5
   15 ACTIVE org.eclipse.gemini.blueprint.core_1.0.0.RELEASE
   16 ACTIVE org.eclipse.gemini.blueprint.extender_1.0.0.RELEASE
   17 ACTIVE org.eclipse.gemini.blueprint.io_1.0.0.RELEASE
   19 RESOLVED com.ibm.websphere.xs.server_7.1.1
   21 RESOLVED Google_ProtoBuf_2.4.0
   22 RESOLVED ProtoBufPlugins_1.0.0
   ```

2. Inicie cada pacote configurável instalado. Você deve iniciar os pacotes configuráveis em uma ordem específica. Consulte a ordem dos IDs do pacote configurável do exemplo anterior.

   a. Inicie o pacote configurável do plug-in de amostra `ProtoBufPlugins_1.0.0`. Execute o seguinte comando no console do Equinox OSGi para iniciar o pacote configurável. Neste exemplo, o ID do pacote configurável do plug-in de amostra é 22.

      ```
      osgi> start 22
      ```

   b. Inicie o pacote configurável do Google Protocol Buffers, `Google_ProtoBuf_2.4.0`. Execute o seguinte comando no console do Equinox OSGi para iniciar o pacote configurável. Neste exemplo, o ID do pacote configurável do plug-in Google Protocol Buffers é 21.

      ```
      osgi> start 21
      ```

   c. Inicie o pacote configurável do servidor, `ProtoBufPlugins_1.0.0`. Execute o seguinte comando no console OSGi para iniciar o servidor. Neste exemplo, o ID do pacote configurável do servidor eXtreme Scale é 19.

      ```
      osgi> start 19
      ```

Depois de iniciar o servidor, o listener de event MyShardListener é iniciado e pronto para inserir ou atualizar registros. É possível ver a saída a seguir no console OSGi para confirmar se o pacote configurável do plug-in foi iniciado com êxito:

```
SystemOut O MyShardListener@1253853884(version=1.0.0) order
com.ibm.websphere.samples.xs.serializer.proto.DataObjects1$Order$Builder
@1aba1aba(22) inserted
```

Ponto de verificação de lições:

Nesta lição, você iniciou dois pacotes configuráveis de plug-in e o pacote configurável do servidor no contêiner do eXtreme Scale configurado para a estrutura do OSGi.

Módulo 3: Executando o Cliente de Amostra do eXtreme Scale

O servidor WebSphere eXtreme Scale agora está em execução em um ambiente do OSGi. Conclua as etapas neste módulo para executar um cliente do WebSphere eXtreme Scale que insere dados na grade.

Objetivos do aprendizado

Depois de concluir as lições neste módulo, você saberá como concluir as seguintes tarefas:

- Executar um aplicativo cliente que se conecta à grade e insere e recupera dados a partir dele.
- Inicie uma ordem usando um aplicativo cliente não OSGi.

Pré-requisitos

Conclua Módulo 2: Instalando e Iniciando Pacotes Configuráveis do eXtreme Scale na Estrutura OSGi.

Lição 3.1: Configurar o Eclipse para Executar o Cliente e Construir as Amostras

Conclua esta lição para importar o projeto Eclipse que será usado para executar o cliente e construir os plug-ins de amostra.

A amostra inclui um programa cliente Java SE que se conecta à grade e insere e recupera dados a partir dele. Ele também inclui projetos que podem ser usados para construir e reimplementar os pacotes configuráveis do OSGi.

O projeto fornecido foi testado com o Eclipse 3.x e posterior e requer somente a perspectiva de projetos de desenvolvimento Java padrão. Conclua as etapas a seguir para configurar o seu ambiente de desenvolvimento do WebSphere eXtreme Scale.

1. Abra o Eclipse para uma área de trabalho nova ou existente.
2. No menu Arquivo, selecione **Importar**.
3. Expanda a pasta Geral. Selecione **Pacotes Existentes na Área de Trabalho** e clique em **Avançar**.
4. No campo **Selecionar Diretório-Raiz**, digite ou navegue até o diretório *wxs_sample_osgi_root*. Clique em **Concluir**. Vários novos projetos são exibidos na sua área de trabalho. Erros de construção serão corrigidos ao definir duas bibliotecas de usuário. Conclua as próximas etapas para definir as bibliotecas de usuário.
5. No menu Janela, selecione **Preferências**.

6. Expanda a ramificação **Java** > **Caminho de Construção** e selecione **Bibliotecas de Usuário**.
7. Defina a biblioteca de usuário do eXtreme Scale.
   a. Clique em **Novo**.
   b. Digite `eXtremeScale` no campo **Nome da Biblioteca de Usuário** e clique em **OK**.
   c. Selecione a nova biblioteca de usuário e clique em **Incluir JARs**.
      1) Procure por e selecione o arquivo `objectgrid.jar` a partir do diretório *wxs_install_root*`/lib`. Clique em **OK**.
      2) Para incluir a documentação da API para as APIs do ObjectGrid, selecione o local da documentação da API para o arquivo `objectgrid.jar` que você incluiu na etapa anterior. Clique em **Editar**.
      3) Na caixa do caminho do local para a documentação da API, selecione o arquivo `Javadoc.zip` que está incluído no seguinte diretório: *wxs_install_root*`/docs/javadoc.zip`.
8. Defina a biblioteca de usuário do Google Protocol Buffers.
   a. Clique em **Novo**.
   b. Digite `com.google.protobuf` no campo **Nome da Biblioteca de Usuário** e clique em **OK**.
   c. Selecione a nova biblioteca de usuário e clique em **Incluir JARs**.
      1) Procure por e selecione o arquivo `com.google.protobuf_2.4.0.a.jar` a partir do diretório *wxs_sample_osgi_root*`/lib`. Clique em **OK**.

Ponto de verificação de lições:

Nessa lição, você importou o projeto Eclipse de amostra e definiu as bibliotecas de usuário que corrigiram os erros de construção.

Lição 3.2: Iniciar um Cliente e Inserir Dados na Grade

Conclua esta lição para iniciar um cliente não OSGi e executar um aplicativo cliente.

O aplicativo de cliente Java é `com.ibm.websphere.samples.xs.proto.client.Client`. O projeto Eclipse, wxs.sample.osgi.protobuf.client, contém o aplicativo de cliente Java. O arquivo de classe principal é `com.ibm.websphere.samples.xs.proto.client.Client`.

Este cliente usa uma substituição do cliente, o arquivo descritor XML do ObjectGrid para substituir a configuração OSGi, para que o cliente possa ser executado em um ambiente não OSGi. Consulte o conteúdo a seguir do arquivo com comentários e cabeçalhos removidos.

```
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
    xmlns="http://ibm.com/ws/objectgrid/config">

    <objectGrids>
        <objectGrid name="Grid" txTimeout="15">
            <bean id="ObjectGridEventListener" className="" osgiService=""/>
            <backingMap name="Map" readOnly="false"
                lockStrategy="PESSIMISTIC" lockTimeout="5"
                copyMode="COPY_TO_BYTES" pluginCollectionRef="serializer"/>

        </objectGrid>
    </objectGrids>

    <backingMapPluginCollections>
        <backingMapPluginCollection id="serializer">
```

```
    <bean id="MapSerializer"
    className="com.ibm.websphere.samples.xs.serializer.proto.ProtoMapSerializer"
        osgiService="">
     <property name="keyType" type="java.lang.String"
         value="com.ibm.websphere.samples.xs.serializer.proto.DataObjects2$OrderKey" />
           <property name="valueType" type="java.lang.String"
               value="com.ibm.websphere.samples.xs.serializer.proto.DataObjects2$Order" />
    </bean>
   </backingMapPluginCollection>
    </backingMapPluginCollections>
</objectGridConfig>
```

Clique em **Executar Como** > **Aplicativo Java** para executar o aplicativo cliente.

Quando você executa o aplicativo, a seguinte mensagem é exibida. A mensagem indica que uma solicitação foi inserida:

```
order
com.ibm.websphere.samples.xs.serializer.proto.DataObjects1$Order$Builder@5d165d16(5000000) inserted
```

Ponto de verificação de lições:

Nesta lição, você iniciou o aplicativo `com.ibm.websphere.samples.xs.proto.client.Client`, que produziu uma solicitação.

Módulo 4: Consultando e Fazendo Upgrade do Pacote Configurável de Amostra

Conclua as lições neste módulo para usar o comando **xscmd** para consultar a classificação de serviço do pacote configurável da amostra, fazer upgrade dela para uma nova classificação de serviço e verificar o novo serviço de classificação.

Objetivos do aprendizado

Depois de concluir as lições deste módulo, você saberá como concluir as tarefas:

- Consultar a classificação de serviço atual para um serviço.
- Consultar a classificação atual de todos os serviços.
- Consultar todas as classificações disponíveis para um serviço.
- Consultar todas as classificações de serviço disponíveis.
- Use a ferramenta xscmd para verificar se as classificações específicas do serviço estão disponíveis.
- Atualizar as classificações de serviço dos serviços OSGi de amostra.

Pré-requisitos

Executar o Módulo 3: Executando o Cliente de Amostra do eXtreme Scale.

Lição 4.1: Consultar Classificações de Serviço

Conclua esta lição para consultar as classificações de serviço atuais, bem como as classificações de serviço que estão disponíveis para upgrade.

- Consultar a classificação de serviço atual para um serviço. Insira o seguinte comando para consultar a classificação de serviço atual usada para serviço, myShardListener, que é usado pelo ObjectGrid denominado `Grid` e pelo conjunto de mapas denominado `MapSet`.
  1. Alterne para o diretório a seguir:
     ```
     cd wxs_home/bin
     ```

2. Insira o seguinte comando para consultar a classificação de serviço atual para o serviço myShardListener.

   ```
   ./xscmd.sh -c osgiCurrent -g Grid -ms MapSet -sn myShardListener
   ```

   A saída a seguir é exibida:

   ```
   OSGi Service Name: myShardListener
   ObjectGrid Name MapSet Name Server Name        Current Ranking
   --------------- ----------- -----------        ---------------
   Grid            MapSet      collocatedServer   1

   CWXSI0040I: The command osgiCurrent has completed successfully.
   ```

- Consultar a classificação atual de todos os serviços. Insira o seguinte comando para consultar as classificações de serviço atuais para todos os serviços usados pelo ObjectGrid denominado `Grid` e pelo conjunto de mapas denominado `MapSet`:

  1. Alterne para o diretório a seguir:

     ```
     cd wxs_home/bin
     ```

  2. Insira o seguinte comando para consultar a classificação de serviço atual para todos os serviços.

     ```
     ./xscmd.sh -c osgiCurrent -g Grid -ms MapSet
     ```

     A saída a seguir é exibida:

     ```
     OSGi Service Name    Current Ranking ObjectGrid Name MapSet Name Server Name
     -----------------    --------------- --------------- ----------- -----------
     myProtoBufSerializer 1               Grid            MapSet      collocatedServer
     myShardListener      1               Grid            MapSet      collocatedServer

     CWXSI0040I: The command osgiCurrent has completed successfully.
     ```

- Consultar todas as classificações disponíveis para um serviço. Insira o seguinte comando para consultar todas as classificações de serviço disponíveis para o serviço denominado myShardListener.

  1. Alterne para o diretório a seguir:

     ```
     cd wxs_home/bin
     ```

  2. Insira o seguinte comando para consultar todas as classificações disponíveis para um serviço.

     ```
     ./xscmd.sh -c osgiAll -sn myShardListener
     ```

     A saída a seguir é exibida:

     ```
     Server: collocatedServer
        OSGi Service Name Available Rankings
        ----------------- ------------------
        myShardListener 1

        Summary - All servers have the same service rankings.

     CWXSI0040I: The command osgiAll has completed successfully.
     ```

     A saída é agrupada pelo servidor. Neste exemplo, apenas o seguinte servidor existe: collocatedServer.

- Consultar todas as classificações de serviço disponíveis. Insira o comando a seguir para consultar todas as classificações de serviço disponíveis para todos os serviços.

  1. Alterne para o diretório a seguir:

     ```
     cd wxs_home/bin
     ```

2. Insira o seguinte comando para consultar todas as classificações de serviço disponíveis.

```
./xscmd.sh -c osgiAll
```

A saída a seguir é exibida:

```
Server: collocatedServer
   OSGi Service Name    Available Rankings
   -----------------    ------------------
   myProtoBufSerializer 1
   myShardListener 1

Summary - All servers have the same service rankings.
```

- Instale e inicie a Versão 2 do pacote configurável do plug-in. No console OSGi servidor, instale um novo pacote configurável que contém uma nova versão da classe Order e o plug-in MapSerializerPlugin. Consulte Lição 2.4: Instalar o Google Buffers Protocol e os pacotes configuráveis do plug-in de amostra para obter detalhes sobre como instalar o pacote configurável `ProtoBufSamplePlugins-2.0.0.jar`.
  1. Após a instalação, inicie o novo pacote configurável. Os serviços para seu novo pacote configurável estão disponíveis, mas eles ainda não são usados pelo servidor eXtreme Scale. Você deve executar uma solicitação de atualização de serviço para usar um serviço com uma versão específica.
- Agora, quando você consultar todas as classificações de serviço disponíveis novamente, o serviço de classificação 2 é incluído na saída.
  1. Alterne para o diretório a seguir:

     ```
     cd wxs_home/bin
     ```

  2. Insira o seguinte comando para consultar todas as classificações de serviço disponíveis.

     ```
     ./xscmd.sh -c osgiAll
     ```

     A saída a seguir é exibida:

     ```
     Server: collocatedServer
        OSGi Service Name    Available Rankings
        -----------------    ------------------
        myProtoBufSerializer 1, 2
        myShardListener      1, 2

     Summary - All servers have the same service rankings.
     ```

Ponto de verificação de lições:

Neste tutorial, você consultou atualmente todas as classificações de serviço, e classificações de serviço especificadas, disponíveis. Você também exibiu a classificação de serviço para um novo pacote configurável que você instalou e iniciou.

Lição 4.2: Determinar Se Classificações de um Serviço Específico Estão Disponíveis

Conclua esta lição para determinar se as classificações de um serviço específico estão disponíveis para os nomes de serviço que forem especificados.

1. Insira o seguinte comando para determinar se o serviço myShardListener, com a classificação de serviço 2, e o serviço myProtoBufSerializer, com a classificação de serviço 2, estão disponíveis. A lista de classificação do serviço é passada usando a opção `-sr`.
   a. Alterne para o diretório a seguir:

```
cd wxs_home/bin
```

b. Insira o seguinte comando para determinar se os serviços estão disponíveis:

```
./xscmd.sh -c osgiCheck -sr "myShardListener;2,myProtoBufSerializer;2"
```

A saída a seguir é exibida:

```
CWXSI0040I: The command osgiCheck has completed successfully.
```

2. Insira o seguinte comando para determinar se o serviço myShardListener, com a classificação de serviço 2, e o serviço myProtoBufSerializer, com a classificação de serviço 3 estão disponíveis.

a. Alterne para o diretório a seguir:

```
cd wxs_home/bin
```

b. Insira o seguinte comando para determinar se os serviços estão disponíveis:

```
./xscmd.sh -c osgiCheck -sr "myShardListener;2,myProtoBufSerializer;3"
```

A saída a seguir é exibida:

```
Server  OSGi Service Unavailable Rankings
------           ------------         --------------------
collocatedServer myProtoBufSerializer 3
```

Ponto de verificação de lições:

Nesta lição, você especificou os serviços myShardListener e myProtoBufSerializer, junto com classificações de serviço específicas para determinar se essas classificações estavam disponíveis.

Lição 4.3: Atualizar as Classificações do Serviço

Conclua esta lição para atualizar as classificações do serviço atuais que você consultou.

1. Atualize as classificações dos serviços, myShardListener e myProtoBufSerializer, para a classificação do serviço 2. A lista de classificações do serviço é passada com o uso da opção `-sr`.

a. Alterne para o diretório a seguir:

```
cd wxs_home/bin
```

b. Insira o seguinte comando para atualizar as classificações de serviço:

```
./xscmd.sh -c osgiUpdate -g Grid -ms MapSet -sr "myShardListener;2,myProtoBufSerializer;2"
```

A saída a seguir é exibida:

```
Update succeeded for the following service rankings:
Service Ranking
-------              -------
myProtoBufSerializer 2
myShardListener 2

CWXSI0040I: The command osgiUpdate has completed successfully.
```

A seguinte saída é exibida no console do OSGi:

```
SystemOut O MyShardListener@326505334(version=2.0.0) order
com.ibm.websphere.samples.xs.serializer.proto.DataObjects2$Order$Builder@
22342234(34) updated
```

Observe que o serviço MyShardListener está agora na versão 2.0.0, que possui um serviço de classificação 2.

2. Execute o comando **xscmd** para consultar a classificação do serviço atual de todos os serviços usados pelo ObjectGrid denominado `Grid` e o conjunto de mapas denominado `MapSet`.

a. Alterne para o diretório a seguir:

```
cd wxs_home/bin
```

b. Insira o seguinte comando para consultar as classificações de serviço para todos os serviços usados por `Grid` e `MapSet`:

```
./xscmd.sh -c osgiCurrent -g Grid -ms MapSet
```

A saída a seguir é exibida:

```
OSGi Service Name    Current Ranking ObjectGrid Name MapSet Name Server Name
-----------------    --------------- --------------- ----------- -----------
myProtoBufSerializer 2 Grid MapSet collocatedServer
myShardListener 2 Grid MapSet collocatedServer

CWXSI0040I: The command osgiCurrent has completed successfully.
```

Ponto de verificação de lições:

Nesta lição você atualizou as classificações de serviço para os serviços myShardListener e myProtoBufSerializer.

.

Capítulo 2. Cenários

Os cenários incluem informações do mundo real para construir uma figura completa. Conclua um cenário para entender os novos conceitos ou para realizar tarefas comuns do WebSphere eXtreme Scale.

Cenário: Configurando uma Grade de Dados Corporativos

Configure uma grade de dados corporativos quando desejar que ambos os aplicativos Java e .NET se conectem à mesma grade de dados.

Antes de Iniciar

- Instale o produto. Você deve instalar o tempo de execução do servidor e os clientes. Para clientes, é possível utilizar os clientes Java e .NET. Para obter informações adicionais, consulte Instalando.
- Se estiver atualizando a partir de uma liberação anterior, você deverá ter todos os seus servidores de contêiner e de catálogos no mesmo nível de liberação. Para obter informações adicionais, consulte Fazendo Upgrade e Migrando o WebSphere eXtreme Scale.

Sobre Esta Tarefa

Visão Geral da Grade de Dados Corporativos

As grades de dados corporativos usam o mecanismo de transporte eXtremeIO e um novo formato de serialização. Com o novo formato de transporte e serialização, é possível conectar ambos os clientes, Java e .NET, à mesma grade de dados.

Com a grade de dados corporativos, é possível criar vários tipos de aplicativos, gravados em diferentes linguagens de programação, para acessar os mesmos objetos na grade de dados. Em liberações anteriores, os aplicativos da grade de dados precisavam ser gravados apenas na linguagem de programação Java. Com a função de grade de dados corporativos, você pode gravar aplicativos .NET que podem criar, recuperar, atualizar e excluir objetos da mesma grade de dados que o aplicativo Java.

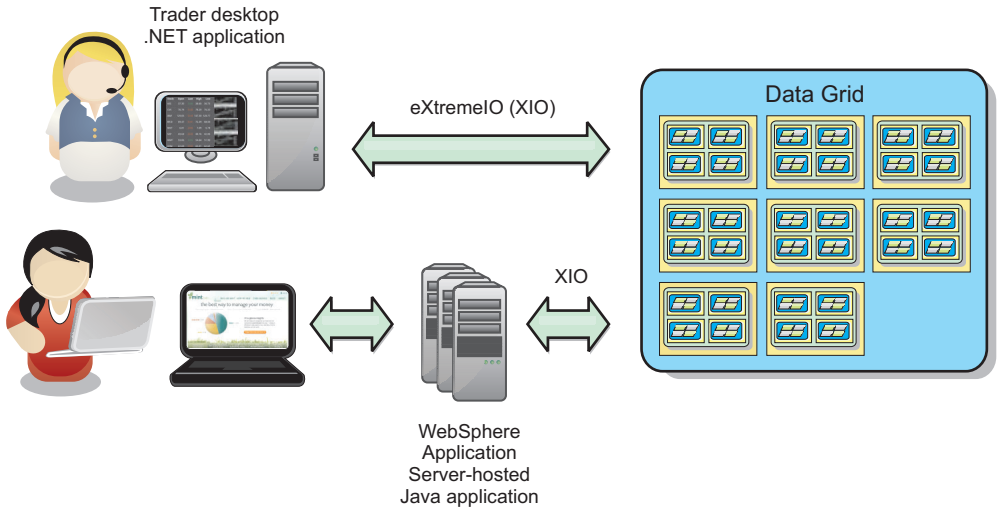


Figura 6. Visão Geral Resumida da Grade de Dados Corporativos

Atualizações de Objetos em Diferentes Aplicativos

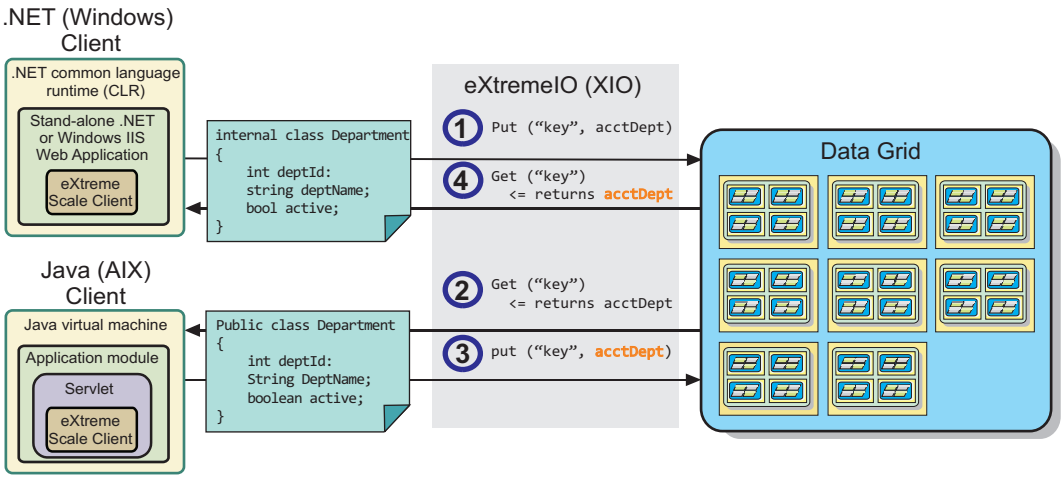


Figura 7. Fluxo de Atualização do Objeto da Grade de Dados Corporativos

1. O cliente .NET salva os dados em seu formato na grade de dados.
2. Os dados são armazenados em um formato universal, de forma que, quando o cliente Java solicitar esses dados, eles possam ser convertidos para o formato Java.
3. O cliente Java atualiza e salva novamente os dados.
4. O cliente .NET acessa os dados atualizados, durante o qual os dados são convertidos para o formato .NET.

Mecanismo de Transporte

eXtremeIO (XIO) é um protocolo de transporte de plataforma cruzada. XIO substitui o Object Request Broker (ORB) ligado ao Java. Com o ORB, o WebSphere eXtreme Scale é ligado aos aplicativos clientes nativos Java. XIO é um mecanismo de transporte customizado que é especificamente destinado para armazenamento de dados em cache e permite que os aplicativos clientes que estão em diferentes

linguagens de programação se conectem à grade de dados.

Formato de Serialização

Formato de dados eXtreme (XDF) é um formato de serialização de plataforma cruzada. XDF substitui a serialização Java em mapas que têm um valor de atributo copyMode igual a `COPY_TO_BYTES` no arquivo XML do descritor do ObjectGrid. Com XDF, o desempenho é mais rápido e os dados são mais compactos. Além disso, a introdução de XDF permite que aplicativos clientes que estão em diferentes linguagens de programação se conectem com a mesma grade de dados.

Tarefas relacionadas:

8.6+ "Desenvolvendo Aplicativos de Grade de Dados Corporativos" na página 122
Após configurar o IBM eXtremeIO, será possível gravar aplicativos que acessam a grade de dados corporativos.

"Configurando o IBM eXtremeIO (XIO)"
O IBM eXtremeIO (XIO) é um mecanismo de transporte que substitui o Object Request Broker (ORB).

Iniciando Servidores de Contêiner do que Utilizam o Transporte do IBM eXtremeIO (XIO)
É possível iniciar servidores de contêiner a partir da linha de comandos usando uma topologia de implementação ou usando um arquivo `server.properties`.

8.6+ "Configurando Grades de Dados para Utilizar o eXtreme Data Format (XDF)" na página 121
Se você estiver usando uma grade de dados corporativos, você deverá ativar o XDF para que Java e .NET possam acessar os mesmos objetos da grade de dados. Use XDF para serializar e armazenar chaves e valores na grade de dados em um formato independente do idioma.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Configurando o IBM eXtremeIO (XIO)

O IBM eXtremeIO (XIO) é um mecanismo de transporte que substitui o Object Request Broker (ORB).

Antes de Iniciar

- **8.6** Para configurar XIO, todos os seus servidores de contêineres e de catálogos devem estar no nível de liberação da Versão 8.6. Para obter informações adicionais, consulte Atualizando Servidores eXtreme Scale.

8.6+ É possível configurar XIO para todos os servidores de contêiner no domínio do serviço de catálogo, ativando o XIO nos servidores de catálogo. Os servidores de contêiner descobrem o tipo de transporte do servidor de catálogos e usam esse tipo de transporte.

Procedimento

8.6+ Como você ativa o XIO depende do tipo de servidores que você está utilizando:

- Ative o XIO em seus servidores de catálogo independentes.

  O XIO é ativado por padrão quando você inicia o servidor de catálogos com o comando **startXsServer**. Para obter informações adicionais, consulte Iniciando Servidores de Contêiner do que Utilizam o Transporte do IBM eXtremeIO (XIO).
- Ative o XIO em seus servidores que estão em execução no WebSphere Application Server.

  Também é possível ativar o XIO no domínio do serviço de catálogo no console administrativo do WebSphere Application Server. Clique em **Administração do Sistema** > **WebSphere eXtreme Scale** > **Domínios de Serviço de Catálogo** > *catalog_service_domain*. Selecione **Ativar Comunicação do IBM eXtremeIO (XIO)**. Aplique as alterações. Para obter informações adicionais, consulte Configurando o Serviço de Catálogo no WebSphere Application Server.
- Ative o XIO em seus servidores que são executados no Perfil do Liberty.

  Para ativar o XIO em um servidor Perfil do Liberty, configure o atributo `transport` como `XIO` em seu arquivo `server.xml`. Por exemplo, consulte a propriedade destacada no exemplo de código a seguir:

  ```
  <featureManager>
    ...
    <feature>eXtremeScale.server-1.1</feature>
  </featureManager>

  <xsServer isCatalog="true" transport="XIO" listenerPort="2809" ... />
  ```

  Atenção: O servidor deve ser um servidor de catálogo e, portanto, `isCatalog` deverá ser configurado como true quando você configurar XIO. A configuração de `listenerPort` não é requerida; no entanto, o XIO pode reconhecer essa porta se você ativá-la. Se você não ativar o XIO, o ORB será utilizado nessa porta.

  Em seguida, execute o comando **start** para iniciar seus servidores Perfil do Liberty. Para obter informações adicionais, consulte Iniciando e Parando Servidores no Perfil do Liberty.

8.6+ É possível utilizar argumentos da linha de comandos e as propriedades do servidor para configurar o comportamento do XIO:

- Opcional: Atualize o arquivo de propriedades de servidor para cada servidor de contêiner na configuração para ativar propriedades do XIO. Após decidir sobre as propriedades que você deseja configurar, é possível configurar os valores no arquivo de propriedade de servidor ou programaticamente com a interface ServerProperties. Para obter mais informações sobre as propriedades que podem ser configuradas, consulte “Ajustando o IBM eXtremeIO (XIO)” na página 129.

8.6+ Resultados

Os servidores que você configurou utilizam o transporte XIO. Para verificar se a configuração está correta, consulte Exibindo o Tipo de Transporte do Domínio de Serviço de Catálogo.

O que Fazer Depois

Também é possível usar o IBM eXtremeMemory para ajudar a evitar pausas da coleta de lixo, levando a um desempenho mais constante e a tempos de resposta

previsíveis. Para obter informações adicionais, consulte Configurando o IBM eXtremeMemory.

Conceitos relacionados:

8.6+ "Visão Geral da Grade de Dados Corporativos" na página 117
As grades de dados corporativos usam o mecanismo de transporte eXtremeIO e um novo formato de serialização. Com o novo formato de transporte e serialização, é possível conectar ambos os clientes, Java e .NET, à mesma grade de dados.

Referências relacionadas:

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

8.6+ "Ajustando o IBM eXtremeIO (XIO)" na página 129
É possível usar propriedades de servidor XIO para sintonizar o comportamento do transporte do XIO na grade de dados.

Configurando Grades de Dados para Utilizar o eXtreme Data Format (XDF)

Se você estiver usando uma grade de dados corporativos, você deverá ativar o XDF para que Java e .NET possam acessar os mesmos objetos da grade de dados. Use XDF para serializar e armazenar chaves e valores na grade de dados em um formato independente do idioma.

Antes de Iniciar

Ative o IBM eXtremeIO (XIO) no ambiente. Para obter informações adicionais, consulte "Configurando o IBM eXtremeIO (XIO)" na página 119.

Sobre Esta Tarefa

Ative o eXtreme Data Format (XDF) para armazenar objetos serializados de uma maneira independente de linguagem. XDF agora é a tecnologia de serialização padrão que é usada quando você está executando o XIO e tem um modo de cópia de mapa configurado para `COPY_TO_BYTES`. Quando você ativar esse recurso, os objetos Java e C# poderão compartilhar dados na mesma grade de dados. É possível configurar o modo XDF para instalações do WebSphere eXtreme Scale em um ambiente independente e para instalações do WebSphere eXtreme Scale dentro de um ambiente do WebSphere Application Server.

Ao usar XDF, você obtém os benefícios a seguir:

- Serialização dos dados para compartilhamento entre aplicativos Java e C#/.NET.
- Indexação de dados no servidor sem requerer que as classes de usuário estejam presentes, se o acesso a campo for usado.
- Versão automática de suas classes para que seja possível aumentar as definições de classes ao incluir aplicativos que requerem novas versões dos arquivos. Versões mais antigas dos dados podem ser usadas tirando proveito da interface de Mergable.
- Particionamento dos dados com anotações em Java e C# para particionar de forma consistente a partir do aplicativo.

Procedimento

No arquivo XML descritor de ObjectGrid, configure o atributo **CopyMode** para XDF no elemento backingMap do arquivo XML descritor de ObjectGrid.

```
<backingMap name="Employee" lockStrategy="PESSIMISTIC" copyMode="COPY_TO_BYTES">
```

O que Fazer Depois

Desenvolva aplicativos que possam compartilhar dados. Para obter informações adicionais, consulte "Desenvolvendo Aplicativos de Grade de Dados Corporativos".

Conceitos relacionados:

8.6+ "Visão Geral da Grade de Dados Corporativos" na página 117
As grades de dados corporativos usam o mecanismo de transporte eXtremeIO e um novo formato de serialização. Com o novo formato de transporte e serialização, é possível conectar ambos os clientes, Java e .NET, à mesma grade de dados.

Referências relacionadas:

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Desenvolvendo Aplicativos de Grade de Dados Corporativos

Após configurar o IBM eXtremeIO, será possível gravar aplicativos que acessam a grade de dados corporativos.

Antes de Iniciar

- Configure seu ambiente de desenvolvimento e visualize a documentação da API. Para obter informações adicionais, consulte "Introdução ao Desenvolvimento de Aplicativos" na página 254.
- Você deve ter aplicativos Java ou .NET existentes que acessem a grade de dados. Para obter informações adicionais sobre introdução à composição de aplicativos, consulte "Tutorial de Introdução - Módulo 2: Criar um Aplicativo Cliente" na página 237.

Conceitos relacionados:

8.6+ "Visão Geral da Grade de Dados Corporativos" na página 117
As grades de dados corporativos usam o mecanismo de transporte eXtremeIO e um novo formato de serialização. Com o novo formato de transporte e serialização, é possível conectar ambos os clientes, Java e .NET, à mesma grade de dados.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Evolução de Classe

eXtreme data format (XDF) permite evolução de classe. Com evolução de classe, é possível evoluir as definições de classe na grade de dados sem afetar aplicativos mais antigos que estão usando versões anteriores da classe. Essas classes mais antigas estão acessando dados no mesmo mapa que os novos aplicativos.

Visão Geral

Evolução de classe é uma extensão adicional da identificação de classes e campos que determina se dois tipos são compatíveis o suficiente para funcionarem juntos. Classes podem funcionar juntas quando uma das classes tem menos campos do que a outra classe. Os cenários de usuários a seguir são projetados na implementação de XDF:

Diversas versões da mesma classe de objetos
Neste cenário, você tem um mapa em um aplicativo de vendas que é usado para rastreamento de clientes. Esse mapa tem duas interfaces diferentes. Uma interface é para compras na web. A segunda interface é para compras por telefone. Na versão 2 desse aplicativo de vendas, você decide dar descontos a compradores da web com base em seus hábitos de compras. Esse desconto é armazenado com o objeto Customer. Os funcionários de vendas por telefone ainda estão usando a versão 1 do aplicativo, que não está ciente do novo campo de desconto na versão da web. Você deseja que objetos Customer da versão 2 do aplicativo trabalhem com objetos Customer que foram criados com o aplicativo versão 1 e vice-versa.

Diversas versões de uma classe de objetos diferente
Neste cenário, você tem um aplicativo de vendas escrito em Java que mantém um mapa de objetos Customer. Também tem outro aplicativo escrito em C# que é usado para gerenciar o inventário no warehouse e enviar mercadorias a clientes. Essas classes são atualmente compatíveis com base nos nomes das classes, campos e tipos. Em seu aplicativo de vendas Java, você deseja incluir uma opção no registro Customer para associar a pessoa de vendas a uma conta de cliente. No entanto, você não deseja atualizar o aplicativo de warehouse para armazenar esse campo, pois não é necessário no warehouse.

Diversas versões incompatíveis da mesma classe
Neste cenário, seus aplicativos de vendas e de inventário contêm um objeto Customer. O aplicativo de inventário usar um campo ID que é uma sequência e o aplicativo de vendas usa um campo IP que é um número inteiro. Esses tipos não são compatíveis. Como resultado, os objetos provavelmente não são armazenados no mesmo mapa. Os objetos devem ser manipulados pela serialização de XDF e tratados como dois tipos diferentes. Apesar de esse cenário não ser realmente evolução de classe, é uma consideração que deve fazer parte de seu design do aplicativo geral.

Determinação para Evolução

XDF tenta evoluir uma classe quando os nomes de classes correspondem e os nomes de campos não têm tipos conflitantes. Usar as anotações ClassAlias e FieldAlias é útil quando você estiver tentando corresponder classes entre aplicativos C# e Java nos quais os nomes das classes ou campos são ligeiramente diferentes. É possível colocar essas anotações no aplicativo Java e C#, ou em ambos. No entanto, a consulta para a classe no aplicativo Java pode ser menos eficiente do que definir ClassAlias no aplicativo C#. Para obter informações adicionais sobre as anotações ClassAlias e FieldAlias, consulte “Anotações ClassAlias e FieldAlias” na página 125

O Efeito de Campos Ausentes em Dados Serializados

O construtor da classe não é chamado durante a desserialização, portanto, quaisquer campos ausentes têm um padrão que é designado a ele com base na linguagem. O aplicativo que está incluindo novos campos deve ser capaz de detectar campos ausentes e reagir quando uma versão mais antiga de classe for recuperada.

Atualizar os Dados É a Única Maneira para que Aplicativos mais Antigos Mantenham os Campos mais Novos

Um aplicativo pode executar uma operação de busca e atualizar o mapa com uma versão mais antiga da classe que tem alguns campos ausentes no valor serializado do cliente. O servidor mescla, então, os valores do servidor e determina se quaisquer campos da versão original são mesclados no novo registro. Se um aplicativo executar uma operação de busca e, em seguida, remover e inserir uma entrada, os campos do valor original são perdidos.

Capacidades de Mesclagem

Objetos em uma matriz ou coleção não são mesclados por XDF. Nem sempre está claro se uma atualização de uma matriz ou coleção tem a intenção de alterar os elementos da matriz ou tipo. Se ocorrer uma mesclagem com base no posicionamento, quando uma entrada na matriz for movida, XDF pode mesclar campos que não devem ser associados. Como resultado, XDF não tenta mesclar o conteúdo de matrizes ou coleções. No entanto, se você incluir uma matriz em uma versão mais nova de uma definição de classe, a matriz é mesclada de volta com a versão anterior da classe.

Definindo Anotações ClassAlias e FieldAlias para Correlacionar Classes Java e .NET

Use as anotações ClassAlias e FieldAlias para ativar o compartilhamento de dados da grade de dados entre suas classes Java e .NET.

Antes de Iniciar

- Você deve ter o IBM eXtremeIO configurado. Para obter informações adicionais, consulte “Configurando o IBM eXtremeIO (XIO)” na página 119.
- Seu atributo copyMode em seu arquivo XML do descritor do ObjectGrid deve ser configurado como COPY_TO_BYTES. Para obter informações adicionais, consulte “Configurando Grades de Dados para Utilizar o eXtreme Data Format (XDF)” na página 121.

Sobre Esta Tarefa

Você pode considerar o uso das anotações ClassAlias e FieldAlias se tiver uma classe Java existente e desejar criar uma classe C# correspondente. Neste cenário, você inclui as anotações em sua classe C# que inclui o nome de classe Java. Para obter mais informações sobre as anotações ClassAlias e FieldAlias, consulte “Anotações ClassAlias e FieldAlias” na página 125.

Procedimento

Utilize as anotações ClassAlias e FieldAlias para correlacionar os objetos entre uma classe Java e uma classe C#. Java

Java

```
@ClassAlias("Employee")
class com.company.department.Employee {

     @FieldAlias("id")
     int myId;

      String name;
}
```

Figura 8. Exemplo de Java com as Anotações ClassAlias e FieldAlias

.NET

.NET

```
[ ClassAlias( "Employee") ]
class Com.MyCompany.Employee {

     [ FieldAlias("id") ]
      int identifier;

      string name;
}
```

Figura 9. Exemplo de .NET com os Atributos ClassAlias e FieldAlias

Conceitos relacionados:

8.6+ "Anotações ClassAlias e FieldAlias"
Use as anotações ClassAlias e FieldAlias para ativar o compartilhamento de dados da grade de dados entre classes. É possível compartilhar dados entre duas classes Java ou entre uma classe Java e uma .NET.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Informações relacionadas:

8.6+ "Lição 2.3: Criando um Aplicativo de Grade de Dados Corporativos" na página 243
Para criar um aplicativo de grade de dados corporativos no qual clientes Java e .NET podem atualizar a mesma grade de dados, você deve tornar suas classes compatíveis. Nos aplicativos de amostra de introdução, o aplicativo de amostra .NET tem aliases para corresponderem aos padrões Java.

Anotações ClassAlias e FieldAlias:

Use as anotações ClassAlias e FieldAlias para ativar o compartilhamento de dados da grade de dados entre classes. É possível compartilhar dados entre duas classes Java ou entre uma classe Java e uma .NET.

Se você definir duas classes com o mesmo nome e campos, os dados da grade de dados serão automaticamente compartilhados entre as classes. Por exemplo, se você tiver uma classe Customer1 em seu aplicativo Java e uma classe Customer1 em seu aplicativo .NET que tenha os mesmos campos, os dados serão compartilhados entre as classes. Isso supõe que o nome de classe também inclui o qualificador de classe, que também é o nome do pacote em Java e namespace em C#. O nome do pacote e o namespace são compartilhados automaticamente porque

o namespace e os nomes de pacotes correspondem. Consulte o exemplo a seguir, em que ambos os nomes não fazem distinção entre maiúsculas e minúsculas:

```
Java:
package com.mycompany.app
public class SampleClass {
int field1;
String field2;
}

C#
namespace Com.MyCompany.App
public class SampleClass {
int field1;
string field2;
}
```

No entanto, você também pode correlacionar dados entre as classes que possuem nomes diferentes. Para correlacionar dados a serem armazenados na grade de dados entre os nomes de classe diferentes, utilize as anotações ClassAlias ou FieldAlias.

Entre dois aplicativos Java: É possível definir duas classes diferentes com nomes diferentes em ambientes de aplicativos Java separados. Marcando as classes com a mesma anotação de ClassAlias, e todos os campos e tipos de campo são correspondidos entre estas duas classes, as classes são correlacionadas com o mesmo ID de tipo de classe, embora tenham os nomes de classe diferentes. O mesmo ID de tipo de classe e os metadados podem, então, ser reutilizados entre as classes nos diferentes tempos de execução de aplicativos Java.

Entre um aplicativo Java e um aplicativo .NET: É possível usar anotações semelhantes em seu aplicativo C# para correlacionar a classe C# com uma classe Java. Os atributos ClassAlias definidos para a classe C# e os campos são correspondidos a uma classe Java com a mesma anotação de ClassAlias.

Tarefas relacionadas:

8.6+ "Definindo Anotações ClassAlias e FieldAlias para Correlacionar Classes Java e .NET" na página 124
Use as anotações ClassAlias e FieldAlias para ativar o compartilhamento de dados da grade de dados entre suas classes Java e .NET.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Informações relacionadas:

8.6+ "Lição 2.3: Criando um Aplicativo de Grade de Dados Corporativos" na página 243
Para criar um aplicativo de grade de dados corporativos no qual clientes Java e .NET podem atualizar a mesma grade de dados, você deve tornar suas classes compatíveis. Nos aplicativos de amostra de introdução, o aplicativo de amostra .NET tem aliases para corresponderem aos padrões Java.

Mapeando Chaves para Partições com Anotações PartitionKey

Um alias PartitionKey é usado para identificar os campos ou atributos nos quais um cálculo de código hash é executado para determinar a partição na qual dados são salvos. A anotação PartitionKey é válida somente nos atributos-chave.

Antes de Iniciar

Você deve estar usando eXtreme Data Format. Para obter informações adicionais, consulte “Configurando Grades de Dados para Utilizar o eXtreme Data Format (XDF)” na página 121.

Sobre Esta Tarefa

Você configura um alias PartitionKey para assegurar que diversas classes salvem dados na mesma partição. Por exemplo, se você configurar o valor de PartitionKey para ser a chave departmentID, registros de funcionários serão colocados na mesma partição.

A interface PartionableKey é a interface Java existente e tem precedência sobre a anotação PartitionableKey em C#.

Procedimento

- Java Defina anotações PartitionKey em um campo em um aplicativo Java.

  Java

  ```
  class Employee {
      int empId;

      @PartitionKey(order = 0)
      int deptId;

  }
  ```

  É possível configurar anotações PartitionKey em diversas chaves ou configurar o alias PartitionKey em uma classe. Para obter exemplos adicionais sobre como configurar anotações PartitionKey em aplicativos Java, consulte Documentação de API Java: Tipo de Anotação PartitionKeys.

- .NET Defina atributos de PartitionKey em um campo em um aplicativo .NET.

  ```
  class Employee {
      int empId;

      [PartitionKey]
      int deptId;
  }
  ```

  Também é possível configurar atributos de PartitionKey em classes .NET. Para obter informações adicionais, consulte Documentação de API .NET: Classe PartitionKeyAttribute.

Equivalentes de Tipos de Dados Java e C#

Ao desenvolver aplicativos de grade de dados corporativos, os tipos de dados entre seus aplicativos Java e C# devem ser compatíveis.

Tabela 1. Equivalentes de Tipos de Dados entre Java e C#

Tipo Java	Tipo C#
boolean	bool
java.lang.Boolean	bool
byte	sbyte ou byte
java.lang.Byte	sbyte

Tabela 1. Equivalentes de Tipos de Dados entre Java e C# (continuação)

Tipo Java	Tipo C#
short	short, ushort
java.lang.Short	short, ushort
int	int, uint, ushort
java.lang.Integer	int, uint
long	long, ulong, uint
java.lang.Long	long, ulong, uint
short ou int	ushort
java.lang.Short ou java.lang.Integer	ushort
int ou long	uint
java.lang.Integer ou java.lang.Long	uint
long ou BigInteger	ulong
java.lang.Long ou java.lang.BigInteger	ulong
char, java.lang.Character	char
float, java.lang.Float	float
double, java.lang.Double	double
java.math.BigDecimal	decimal
java.math.BigInteger	decimal, long ou ulong
java.lang.String	Sequência
java.util.Date, java.util.Calendar	System.DateTime
java.util.Date(rounding), java.util.Calendar(rounding)	System.DateTime
java.util.GregorianCalendar	
java.util.ArrayList	System.Collections.ArrayList, System.Collections.Generic.List, System.Collections.SortedList
java.util.HashMap	System.Collections.Generic.Dictionary, System.Collections.Hashtable
java.util.LinkedList	System.Collections.Generic.LinkedList
java.util.ArrayList, java.util.Vector	System.Collections.Generic.List
java.util.Stack	System.Collections.Generic.Stack
java.util.Vector	System.Collections.ArrayList, System.Collections.Generic.List

Iniciando Servidores Independentes (XIO)

Quando estiver executando uma configuração independente, o ambiente é composto por servidores de catálogos, servidores de contêineres e processos do cliente. Os servidores do WebSphere eXtreme Scale também podem ser integrados em aplicativos Java existentes usando a API do servidor integrado. É necessário configurar e iniciar estes processos manualmente.

Antes de Iniciar

É possível iniciar os servidores do WebSphere eXtreme Scale em um ambiente que não possua o WebSphere Application Server instalado. Se você estiver utilizando o

WebSphere Application Server, consulte Configurando o WebSphere eXtreme Scale com o WebSphere Application Server.

Ajustando o IBM eXtremeIO (XIO)

É possível usar propriedades de servidor XIO para sintonizar o comportamento do transporte do XIO na grade de dados.

Propriedades de Servidor para Ajuste do XIO

É possível configurar as seguintes propriedades no arquivo de propriedades do servidor:

maxXIONetworkThreads
Configura o número máximo de encadeamentos para alocar no conjunto de encadeamentos de rede de transporte eXtremeIO.

Padrão: `50`

minXIONetworkThreads
Configura o número mínimo de encadeamentos para alocar no conjunto de encadeamentos de rede de transporte eXtremeIO.

Padrão: `50`

maxXIOWorkerThreads
Configura o número máximo de encadeamentos para alocar no conjunto de encadeamentos de processamento de solicitação de transporte eXtremeIO.

Padrão: `128`

minXIOWorkerThreads
Configura o número mínimo de encadeamentos para alocar no conjunto de encadeamentos de processamento de solicitação de transporte eXtremeIO.

Padrão: `128`

8.6+ transporte

Especifica o tipo de transporte a ser utilizado para todos os servidores no domínio do serviço de catálogo. É possível configurar o valor como `XIO` ou `ORB`.

Ao utilizar os comandos **`startOgServer`** ou **`startXsServer`**, não é necessário configurar esta propriedade. O script substitui esta propriedade. No entanto, se você iniciar servidores com outro método, o valor desta propriedade será utilizado.

Esta propriedade se aplica apenas ao serviço de catálogo.

Se você tiver o parâmetro **`-transport`** no script inicial e a propriedade de servidor **`transport`** definida em um servidor de catálogos, o valor do parâmetro **`-transport`** será usado.

8.6+ xioTimeout
Configura o tempo limite para solicitações do servidor que estão utilizando o transporte IBM eXtremeIO (XIO) em segundos. O valor pode ser configurado para qualquer valor maior ou igual a um segundo.

Padrão: 30 segundos

Tarefas relacionadas:

"Configurando o IBM eXtremeIO (XIO)" na página 119
O IBM eXtremeIO (XIO) é um mecanismo de transporte que substitui o Object Request Broker (ORB).

Cenário: Protegendo sua Grade de Dados no eXtreme Scale

As grades de dados do WebSphere eXtreme Scale armazenam informações sigilosas que devem ser protegidas.

Antes de Iniciar

- Instale o produto. Você deve instalar o tempo de execução do servidor e os clientes. Para clientes, é possível utilizar os clientes Java e .NET. Para obter informações adicionais, consulte Instalando.
- Se estiver atualizando a partir de uma liberação anterior, você deverá ter todos os seus servidores de contêiner e de catálogos no mesmo nível de liberação. Para obter informações adicionais, consulte Fazendo Upgrade e Migrando o WebSphere eXtreme Scale.

Sobre Esta Tarefa

Para uma implementação segura, use diversas camadas de proteção para segurança ideal. O primeiro elemento da proteção é o uso de firewalls para segmentar a rede. O modelo padrão em camadas para aplicativos da web é formado por web clients, uma camada de apresentação de servidores HTTP, uma camada de aplicativo formada por servidores de aplicativos, uma camada de dados e uma camada de armazenamento.

Os servidores de grade de dados do eXtreme Scale são implementados como parte da camada de dados. A prática padrão é colocar os servidores de camada de apresentação em uma zona desmilitarizada (DMZ) protegida por um firewall e colocar as camadas de aplicativo e de armazenamento nos segmentos de rede protegidos por firewalls adicionais. Não implemente servidores do eXtreme Scale em uma DMZ. Os servidores do eXtreme Scale devem ser protegidos como todos os elementos da camada são, de acordo com a prática padrão do segmento de mercado.

No entanto, para proteção ideal contra ameaças de segurança, use um mecanismo de defesa profundo, em que diversas outras medidas protegem a operação do eXtreme Scale e os dados armazenados na grade de dados. Essas medidas adicionais não apenas ajudam na defesa contra ameaças externas, mas também impedem acesso a dados desautorizado por funcionários e contratados que possam ter acesso a segmentos da rede na qual os servidores do eXtreme Scale residem.

Use as etapas de ponta a ponta a seguir para configurar segurança no WebSphere eXtreme Scale, independentemente de se você tem servidores independentes, o Perfil do Liberty, a estrutura OSGi ou o WebSphere Application Server instalado em seu ambiente:

Autenticando Conexões do eXtreme Scale entre Servidores

As conexões entre servidores devem ser autenticadas para evitar que um servidor desautorizado acesse os dados de grade.

O que Fazer Depois

"Autenticando Solicitações de Clientes para Servidores" na página 135

Autenticando Conexões do Servidor do eXtreme Scale em Ambientes Independentes

As conexões entre os servidores do eXtreme Scale devem ser autenticadas para evitar que um servidor desautorizado acesse a grade de dados.

Sobre Esta Tarefa

As configurações a seguir no arquivo `server.properties` determinam como servidores são autenticados uns para os outros:

- **`securityEnabled=true`**
- **`secureTokenManagerType=autoSecret`**
- **`authenticationSecret=OurGridServersExampleSecret`**

Todos os servidores do eXtreme Scale de um domínio, assim como todos os servidores em quaisquer domínios vinculados, devem usar os mesmos valores para essas três propriedades no arquivo `server.properties`, caso contrário, a comunicação falha. Para obter informações adicionais sobre como especificar essas propriedades no arquivo de propriedades de servidor, consulte Arquivo de Propriedades do Servidor.

Procedimento

1. Ative o servidor para autenticação de servidor. Configure a propriedade securityEnabled para `true`; por exemplo:

   ```
   securityEnabled=true
   ```

   O valor padrão para essa propriedade é `false`.
2. Estabeleça uma configuração do servidor seguro.

   secureTokenManagerType é uma propriedade definida no arquivo de Propriedades de Servidor.

   Um secureTokenManagerType que pode ser usado para uma configuração segura é o autoSecret, que executa criptografia e assinatura de token usando chaves derivadas da propriedade authenticationSecret. Tokens seguros são usados autenticação de servidor para servidor e também para tokens de conexão única do cliente. Um valor igual a `none` para secureTokenManagerType não é seguro, pois essa configuração evita a criação de tokens criptografados.

   Também é possível especificar uma configuração de secureTokenManagerType=default. No entanto, essa opção requer que você configure um armazenamento de chaves e artefatos relacionados.
3. Especifique um valor de sequência longo para authenticationSecret (nota: uma palavra) que seja difícil de outros adivinharem. É possível codificar esse valor usando o utilitário FilePasswordEncoder. Para obter informações adicionais, consulte "Armazenando Artefatos de Segurança para Usuários Autorizados" na página 155. Não use a propriedade ObjectGridDefaultSecret, que é o valor usado no arquivo `sampleServer.properties`.

Resultados

Ao iniciar um servidor independente do eXtreme Scale, especifique o nome do arquivo de propriedades na linha de comandos. Ao especificar o arquivo de propriedades de servidor, as propriedades de autenticação incluídas são carregas

quando o servidor for iniciado. Para obter informações adicionais, consulte “Iniciando Servidores Seguros em um Ambiente Independente” na página 158.

O que Fazer Depois

“Autenticando Solicitações de Clientes em Ambientes Independentes” na página 135

Referências relacionadas:

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Autenticando Conexões do Servidor do eXtreme Scale no Perfil do Liberty

As conexões entre os servidores do eXtreme Scale no Perfil do Liberty devem ser autenticadas para evitar que um servidor desautorizado acesse a grade de dados.

Sobre Esta Tarefa

As configurações a seguir no arquivo `server.properties` determinam como servidores são autenticados uns para os outros:

- **`securityEnabled=true`**
- **`secureTokenManagerType=autoSecret`**
- **`authenticationSecret=OurGridServersExampleSecret`**

Todos os servidores do eXtreme Scale de um domínio, assim como todos os servidores em quaisquer domínios vinculados, devem usar os mesmos valores para essas propriedades no arquivo `server.properties`, caso contrário, a comunicação falha.

Procedimento

1. Ative o servidor para autenticação de servidor. Configure a propriedade securityEnable para `true`; por exemplo:

   ```
   securityEnabled=true
   ```

   O valor padrão para essa propriedade é `false`.
2. Estabeleça uma configuração do servidor seguro. Um secureTokenManagerType que pode ser usado para uma configuração segura é o autoSecret, que executa criptografia e assinatura de token usando chaves derivadas do authenticationSecret. Tokens seguros são usados para autenticação de servidor para servidor e também para tokens de conexão única do cliente. Um valor igual a `none` para secureTokenManagerType não é seguro, pois essa configuração evita a criação de tokens criptografados.

   Também é possível especificar uma configuração de secureTokenManagerType=default. No entanto, essa opção requer que você configure um keystore e artefatos relacionados.
3. Especifique um segredo de autenticação longo e criptografado que seja difícil para outros decifrarem. Não use ObjectGridDefaultSecret, que é o valor usado no arquivo `sampleServer.properties`.

4. Configure o arquivo `server.xml` usando a mesma configuração que você pode usar para uma configuração do servidor independente. No arquivo `server.xml`, especifique o caminho de arquivo para o arquivo de propriedades em um atributo serverProps dentro do elemento `xsSever`. Consulte o exemplo a seguir a partir do arquivo `server.xml`:

```
<server>
...
<xsSever ... serverProps="/path/to/myServerProps.properties" ... />
</server>
```

O que Fazer Depois

"Autenticando Solicitações de Clientes no Perfil do Liberty" na página 137

Referências relacionadas:

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Autenticando Conexões do Servidor do eXtreme Scale na Estrutura OSGi

As conexões entre os servidores do eXtreme Scale na estrutura OSGi devem ser autenticadas para evitar que um servidor desautorizado acesse a grade de dados.

Antes de Iniciar

Você deve instalar a estrutura OSGi antes de assegurar a grade de dados. Para obter informações adicionais, consulte "Instalando a Estrutura do Eclipse Equinox OSGi com o Eclipse Gemini para Clientes e Servidores" na página 164.

Sobre Esta Tarefa

As configurações a seguir no arquivo `server.properties` determinam como servidores são autenticados uns para os outros:

- **`securityEnabled=true`**
- **`secureTokenManagerType=autoSecret`**
- **`authenticationSecret=OurGridServersExampleSecret`**

Todos os servidores do eXtreme Scale de um domínio, assim como todos os servidores em quaisquer domínios vinculados, devem usar os mesmos valores para essas propriedades no arquivo `server.properties`, caso contrário, a comunicação falha.

Procedimento

1. Ative o servidor para autenticação de servidor. Configure a propriedade **`securityEnabled`** para `true` no arquivo de propriedades do servidor; por exemplo:

   ```
   securityEnabled=true
   ```

   O valor padrão para essa propriedade é `false`.
2. Estabeleça uma configuração do servidor seguro. Um secureTokenManagerType que pode ser usado para uma configuração segura é o autoSecret, que executa

criptografia e assinatura de token usando chaves derivadas do authenticationSecret. Tokens seguros são usados para autenticação de servidor para servidor e também para tokens de conexão única do cliente. Um valor igual a `none` para secureTokenManagerType não é seguro, pois essa configuração evita a criação de tokens criptografados.

Também é possível especificar uma configuração de secureTokenManagerType=default. No entanto, essa opção requer que você configure um armazenamento de chaves e artefatos relacionados.

3. Especifique um valor de sequência longo para o elemento authenticationSecret. Esse valor deve ser difícil para outros adivinharem. É possível codificar esse valor usando o utilitário FilePasswordEncoder. Não use o elemento ObjectGridDefaultSecret, que é o valor usado no arquivo `sampleServer.properties`.
4. Faça referência ao arquivo de propriedades do servidor. Crie um identificador persistente (PID) de serviço gerenciado para o arquivo de propriedades do servidor no console de OSGim, executando os comandos a seguir:

```
osgi> cm create com.ibm.websphere.xs.server
osgi> cm put com.ibm.websphere.xs.server objectgrid.server.props /mypath/server.properties
```

O que Fazer Depois

"Autenticando Solicitações de Clientes na Estrutura OSGi" na página 139

Referências relacionadas:

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Autenticando Conexões do Servidor do eXtreme Scale no WebSphere Application Server

Os servidores do eXtreme Scale em execução sob o WebSphere Application Server são autenticados uns nos outros da mesma maneira que os servidores independentes do eXtreme Scale.

Antes de Iniciar

Sobre Esta Tarefa

Três configurações no arquivo `server.properties` determinam como servidores são autenticados uns para os outros. Todos os servidores do eXtreme Scale de um domínio, assim como todos os servidores em quaisquer domínios vinculados, devem usar os mesmos valores para essas três propriedades no arquivo `server.properties`, caso contrário, a comunicação falha. Consulte o Arquivo XML Descritor de Segurança para obter mais informações sobre as propriedades de segurança.

Procedimento

1. Crie o arquivo de propriedades do servidor e ative o servidor para autenticação de servidor. Usando esse arquivo de propriedades do servidor de amostra, crie um arquivo de propriedades de servidor que contenha a propriedade **`securityEnabled`**, que está configurada para `true`; por exemplo:

```
securityEnabled=true
```

O valor padrão para essa propriedade é `false`.

2. Estabeleça uma configuração do servidor seguro. Um secureTokenManagerType que pode ser usado para uma configuração segura é o autoSecret, que executa criptografia e assinatura de token usando chaves derivadas do authenticationSecret. Tokens seguros são usados para autenticação de servidor para servidor e também para tokens de conexão única do cliente. Um valor igual a `none` para secureTokenManagerType não é seguro, pois essa configuração evita a criação de tokens criptografados.

   Também é possível especificar uma configuração de secureTokenManagerType=default. No entanto, essa opção requer que você configure um armazenamento de chaves e artefatos relacionados.
3. Especifique um segredo de autenticação longo e criptografado que seja difícil para outros decifrarem. Não use ObjectGridDefaultSecret, que é o valor usado no arquivo `sampleServer.properties`.
4. Configure um arquivo de propriedades de servidor para proteger o servidor. Configure esse arquivo de propriedades usando o console de administração do WebSphere Application Server **WebSphere Application Servers** > *server_name* > **Gerenciamento de Java e Processo** > **Definição do Processo** > **Java Virtual Machine**. Inclua o argumento genérico de JVM a seguir:

   ```
   -Dobjectgrid.server.props=<server property file name>
   ```

O que Fazer Depois

"Autenticando Solicitações de Clientes no WebSphere Application Server" na página 140

Referências relacionadas:

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Autenticando Solicitações de Clientes para Servidores

Seus aplicativos clientes devem fazer solicitações seguras pela rede.

O que Fazer Depois

"Autorizando Acesso à Grade de Dados" na página 142

Autenticando Solicitações de Clientes em Ambientes Independentes

A menos que clientes sejam autenticados, o acesso aos dados de grade e às operações de gerenciamento de JMX que controlam a grade é deixado sem proteção. Isso é verdadeiro se SSL estiver ativado.

Sobre Esta Tarefa

O comportamento de autenticação que os servidores do eXtreme Scale requerem de clientes do eXtreme Scale é determinado pela configuração **`credentialAuthentication=required`** no arquivo `server.properties`.

Quando credentialAuthentication for configurado para `Required` ou `Supported`, uma configuração adicional é necessária, conforme descrito nas etapas a seguir. Essas etapas são descritas em mais detalhes, com exemplo das mudanças nos arquivos de configuração em "Tutorial de Segurança do Java SE - Etapa 3" na página 24.

Procedimento

- Faça referência a um arquivo XML do descritor de segurança em cada servidor de catálogos.

  Quando o servidor de catálogos é iniciado em um ambiente independente, é possível apontar para esse arquivo usando o parâmetro `-clusterSecurityFile` do comando **`startXsServer`** ou **`startOgServer`**.

  Para ativar a segurança, esse arquivo deve ter `securityEnabled="true"` no elemento de segurança. O arquivo XML do descritor de segurança deve conter também um descritor do autenticador que você deseja usar. O WebSphere eXtreme Scale inclui `LDAPAuthenticator`, `KeyStoreLoginAuthenticator` e `WSTokenAuthenticator`. Não é possível usar o autenticador `WSTokenAuthenticator` nos ambientes independentes. É possível usar esse autenticador somente quando clientes e servidores do eXtreme Scale estiverem ambos em execução com o WebSphere Application Server. Como alternativa, é possível desenvolver autenticadores customizados e módulos de login, de acordo com as interfaces descritas na documentação da API.
- Faça referência a um arquivo de configuração de JAAS em cada servidor de catálogos e de contêineres usando o argumento da JVM `-Djava.security.auth.login.config="path_name"`. Para obter informações sobre como criar esses arquivos e configurar servidores do eXtreme Scale para usá-los, consulte o tutorial, "Tutorial: Configurando a Segurança do Java SE" na página 20. O arquivo de configuração de JAAS especifica um LoginModule. É possível usar o KeyStoreLoginModule com o KeyStoreLoginAuthenticator. Use o SimpleLDAPLoginModule com o LDAPAuthenticator. Consulte "Ativando Autenticação LDAP nos Servidores de Catálogos e de Contêineres do eXtreme Scale" na página 780 nos servidores de contêineres e de catálogos do eXtreme Scale ou "Ativando Autenticação de Keystore nos Servidores de Contêineres e de Catálogos do eXtreme Scale" na página 782.
- Configure o cliente para passar as credenciais que são necessárias para autenticação. Isso geralmente é feito especificando valores em um arquivo de propriedades do cliente. Para obter informações adicionais sobre como ativar a autenticação LDAP em clientes do eXtreme Scale, consulte "Ativando Autenticação LDAP nos Servidores de Catálogos e de Contêineres do eXtreme Scale" na página 780, e para obter informações adicionais sobre como ativar a autenticação de keystore em clientes do eXtreme Scale, consulte "Ativando Autenticação de Keystore nos Servidores de Contêineres e de Catálogos do eXtreme Scale" na página 782.

O que Fazer Depois

"Autorizando Acesso à Grade de Dados em Ambientes Independentes" na página 142

Referências relacionadas:

Arquivo XML Descritor de Segurança
Use um arquivo XML descritor de segurança do ObjectGrid para configurar uma topologia de implementação do eXtreme Scale com a segurança ativada. Os elementos presentes nesse arquivo podem ser usados para configurar diferentes aspectos de segurança.

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Arquivo XML descritor do ObjectGrid
Para configurar o WebSphere eXtreme Scale, utilize um arquivo XML descritor do ObjectGrid e a API do ObjectGrid.

Arquivo Descritor XML de Política de Implementação
Para configurar uma política de implementação, utilize um arquivo XML do descritor da política de implementação.

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Informações relacionadas:

Documentação da API

Autenticando Solicitações de Clientes no Perfil do Liberty

A menos que clientes sejam autenticados, o acesso aos dados de grade e às operações de gerenciamento de JMX que controlam a grade é deixado sem proteção. Isso é verdadeiro mesmo se SSL estiver ativado no Perfil do Liberty.

Sobre Esta Tarefa

O comportamento de autenticação necessário para os clientes do eXtreme Scale é determinado pela configuração **`credentialAuthentication=required`** no arquivo `server.properties`, a configuração **`KeyStoreLogin`** no arquivo de configuração de JAAS `og_jaas.config` e a configuração **`KeyStoreLoginAuthenticator`** no arquivo `security.xml`.

O arquivo de propriedades do servidor é carregado fazendo referência a ele no arquivo `server.xml`, conforme descrito em "Autenticando Conexões do Servidor do eXtreme Scale no Perfil do Liberty" na página 132. Para segurança, esse arquivo deve ter `credentialAuthentication=Required`, exatamente como em implementações independentes.

Cada um dos arquivos de configuração é carregado por cada servidor de catálogos. Os servidores de contêineres usam o arquivo de configuração de JAAS e os arquivos descritores de implementação de segurança somente.

Use um dos métodos a seguir para autenticar clientes.

Procedimento

- Faça referência a um arquivo XML do descritor de segurança em cada servidor de catálogos.

Quando o servidor de catálogos for o Perfil do Liberty, é possível apontar para esse arquivo usando o atributo `clusterSecurityURL=` no arquivo `server.xml`. Consulte o exemplo a seguir, em que `objectGridSecurity.xml` é o arquivo XML do descritor de segurança:

```
<server description="new server">
<!-- Enable features -->
<featureManager>
<feature>eXtremeScale.server-1.1</feature>
</featureManager>

<xsServer
isCatalog="true"
serverProps="server.xs.props"
clusterSecurityURL="file://C:/wlp/usr/servers/objectGridSecurity.xml"
/>
</server>
```

Para ativar a segurança, esse arquivo deve ter `securityEnabled="true"` no elemento de segurança. O arquivo XML do descritor de segurança deve conter também um descritor do autenticador que você deseja usar. O WebSphere eXtreme Scale inclui `LDAPAuthenticator`, `KeyStoreLoginAuthenticator` e `WSTokenAuthenticator`.

- Faça referência a um arquivo de configuração de JAAS em cada servidor de catálogos e de contêineres usando o argumento da JVM `-Djava.security.auth.login.config="path_name"` no arquivo `jvm.options`.

  Edite ou crie o arquivo `jvm.options` no diretório `wlp_installdir/usr/servers/<server_name>`.

  Nota: Se precisar criar um novo arquivo `jvm.options` no nível da configuração do servidor, será necessário copiar a versão no arquivo `wlp_install_root/etc/jvm.options`. O arquivo `jvm.options` tem algumas opções que são necessárias para o eXtreme Scale para execução no Perfil do Liberty.

  Ao criar um arquivo `jvm.options` no nível do servidor e inserir o argumento da JVM para fazer referência ao arquivo de configuração de JAAS, seus arquivos `jvm.options` têm a aparência a seguir:

  ```
  C:\wlp\usr\servers\simpCatalog>cat jvm.options
  -Dorg.osgi.framework.bootdelegation=com.ibm.wsspi.runtime
  -Djava.endorsed.dirs=C:\wlp\wxs\lib\endorsed
  -Djava.security.auth.login.config=C:\wlp\usr\servers\ogjaas.config
  ```

  Para obter informações sobre como criar esses arquivos e configurar servidores do eXtreme Scale para usá-los, consulte o tutorial, "Tutorial: Configurando a Segurança do Java SE" na página 20. O arquivo de configuração de JAAS especifica um LoginModule. É possível usar o KeyStoreLoginModule com o KeyStoreLoginAuthenticator. Use o SimpleLDAPLoginModule com o LDAPAuthenticator. Consulte "Ativando Autenticação LDAP nos Servidores de Catálogos e de Contêineres do eXtreme Scale" na página 780 nos servidores de contêineres e de catálogos do eXtreme Scale ou "Ativando Autenticação de Keystore nos Servidores de Contêineres e de Catálogos do eXtreme Scale" na página 782.
- Configure o cliente para passar as credenciais que são necessárias para autenticação. Isso geralmente é feito especificando valores em um arquivo de propriedades do cliente. Para obter informações adicionais sobre como ativar a autenticação LDAP em clientes do eXtreme Scale, consulte "Ativando Autenticação LDAP nos Servidores de Catálogos e de Contêineres do eXtreme Scale" na página 780, e para obter informações adicionais sobre como ativar a

autenticação de keystore em clientes do eXtreme Scale, consulte “Ativando Autenticação de Keystore nos Servidores de Contêineres e de Catálogos do eXtreme Scale” na página 782.

O que Fazer Depois

“Autorizando Acesso à Grade de Dados no Perfil do Liberty” na página 143

Autenticando Solicitações de Clientes na Estrutura OSGi

A menos que clientes sejam autenticados, o acesso aos dados de grade e às operações de gerenciamento de JMX que controlam a grade é deixado sem proteção. Isso é verdadeiro mesmo se SSL estiver ativado na estrutura OSGi.

Antes de Iniciar

Você deve instalar a estrutura OSGi antes de assegurar a grade de dados. Para obter informações adicionais, consulte “Instalando a Estrutura do Eclipse Equinox OSGi com o Eclipse Gemini para Clientes e Servidores” na página 164.

Sobre Esta Tarefa

O comportamento de autenticação necessário para os clientes do eXtreme Scale é determinado pela configuração **credentialAuthentication=required** no arquivo `server.properties`, a configuração **KeyStoreLogin** no arquivo de configuração de JAAS `og_jaas.config` e a configuração **KeyStoreLoginAuthenticator** no arquivo `security.xml`.

Use um dos métodos a seguir para autenticar clientes.

Procedimento

- Faça referência a um arquivo XML do descritor de segurança em cada servidor de catálogos usando o argumento da JVM -DclusterSecurityFile="path_name".

  Use esse argumento da JVM na linha de comandos OSGi ao iniciar o servidor de catálogos.

  Para ativar a segurança, esse arquivo deve ter `securityEnabled="true"` no elemento de segurança. O arquivo XML do descritor de segurança deve conter também um descritor do autenticador que você deseja usar. O WebSphere eXtreme Scale inclui `LDAPAuthenticator`, `KeyStoreLoginAuthenticator` e `WSTokenAuthenticator`. Não é possível usar o autenticador `WSTokenAuthenticator` nos ambientes independentes. É possível usar esse autenticador somente quando clientes e servidores do eXtreme Scale estiverem ambos em execução com o WebSphere Application Server. Como alternativa, é possível desenvolver autenticadores customizados e módulos de login, de acordo com as interfaces descritas na documentação da API.
- Faça referência a um arquivo de configuração de JAAS em cada servidor de catálogos e de contêineres usando o argumento da JVM `-Djava.security.auth.login.config="path_name"`. Para obter informações sobre como criar esses arquivos e configurar servidores do eXtreme Scale para usá-los, consulte o tutorial, “Tutorial: Configurando a Segurança do Java SE” na página 20. O arquivo de configuração de JAAS especifica um LoginModule. É possível usar o KeyStoreLoginModule com o KeyStoreLoginAuthenticator. Use o SimpleLDAPLoginModule com o LDAPAuthenticator. Consulte “Ativando Autenticação LDAP nos Servidores de Catálogos e de Contêineres do eXtreme Scale” na página 780 nos servidores de contêineres e de catálogos do eXtreme

Scale ou "Ativando Autenticação de Keystore nos Servidores de Contêineres e de Catálogos do eXtreme Scale" na página 782.

- Configure o cliente para passar as credenciais que são necessárias para autenticação. Isso geralmente é feito especificando valores em um arquivo de propriedades do cliente. Para obter informações adicionais sobre como ativar a autenticação LDAP em clientes do eXtreme Scale, consulte "Ativando Autenticação LDAP nos Servidores de Catálogos e de Contêineres do eXtreme Scale" na página 780, e para obter informações adicionais sobre como ativar a autenticação de keystore em clientes do eXtreme Scale, consulte "Ativando Autenticação de Keystore nos Servidores de Contêineres e de Catálogos do eXtreme Scale" na página 782.

O que Fazer Depois

"Autorizando Acesso à Grade de Dados na Estrutura OSGi" na página 144

Autenticando Solicitações de Clientes no WebSphere Application Server

Solicitações que o WebSphere Application Server recebe da grade de dados do eXtreme Scale devem ser autenticadas.

Antes de Iniciar

Os requisitos de autenticação para clientes do eXtreme Scale são determinados pelas configurações no arquivo de propriedades do servidor. Um arquivo de propriedades do servidor de amostra é fornecido em *was_root*/optionalLibraries/ObjectGrid/properties/sampleServer.properties.

Sobre Esta Tarefa

Você deve configurar autenticação para servidores do eXtreme Scale que estão em execução sob o WebSphere Application Server usando as etapas a seguir.

Procedimento

1. Crie o arquivo de propriedades do servidor. Usando esse arquivo de propriedades do servidor de amostra, crie um arquivo de propriedades de servidor que contenha as linhas a seguir:

   ```
   securityEnabled=true
   credentialAuthentication=Required
   ```

   A menos que a propriedade credentialAuthentication=Required exista, a grade não estará protegida e usuários não autenticados poderão executar operações de grade.

   Restrição: Não é possível especificar a propriedade, credentialAuthentication=Required, para o provedor de cache dinâmico.

2. Crie o arquivo XML descritor de segurança. Quando a propriedade, credentialAuthentication, é configurada para Required ou Supported, você deve especificar um arquivo XML descritor de segurança. Consulte o seguinte exemplo:

   ```
   <securityConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config/security
   ../objectGridSecurity.xsd"
    xmlns="http://ibm.com/ws/objectgrid/config/security">

    <security securityEnabled="true">
     <authenticator
   ```

```
 className="com.ibm.websphere.objectgrid.security.plugins.builtins.WSTokenAuthenticator">
  </authenticator>
 </security>
</securityConfig>
```

O arquivo XML descritor de segurança especifica o autenticador a ser usado. Quando todos os clientes e servidores do eXtreme Scale estiverem em execução sob o WebSphere Application Server, será possível usar o autenticador WSTokenAuthenticator. Dois outros autenticadores são enviados com o eXtreme Scale, KeyStoreLoginAuthenticator e LDAPLoginAuthenticator. Para obter informações adicionais sobre como configurar autenticação LDAP para o eXtreme Scale, consulte "Ativando Autenticação LDAP nos Servidores de Catálogos e de Contêineres do eXtreme Scale" na página 780. Para usar os autenticadores de keystore e de login com o eXtreme Scale em execução sob o WebSphere Application Server, uma configuração de JAAS é necessária. Para obter informações adicionais sobre como configurar autenticação de keystore para o eXtreme Scale, consulte "Ativando Autenticação de Keystore nos Servidores de Contêineres e de Catálogos do eXtreme Scale" na página 782.

3. Crie a configuração de JAAS, a menos que esteja usando o autenticador WSTokenAuthenticator.
4. Aponte cada servidor de catálogos para o arquivo de propriedades do servidor usando os argumentos JVM a seguir. Configure essas propriedades usando o console de administração do WebSphere Application Server **Servidores** > **todos os servidores** > **server_name** > **Definição de Processo** > **Argumentos JVM genéricos da Java virtual machine**. Os argumentos a seguir são necessários:

   ```
   -Dobjectgrid.server.props=<server property file name>
   -Dobjectgrid.cluster.security.xml.url=file://<security descriptor XML file>
   ```

5. Aponte cada servidor de contêiner para o arquivo de propriedades de servidor usando este argumento JVM:

   ```
   -Dobjectgrid.server.props=<server property file name>
   ```

O que Fazer Depois

Clientes do WebSphere eXtreme Scale devem ser configurados para passar credenciais apropriadas. Conclua essa configuração usando um arquivo de propriedades de cliente. Consulte o exemplo a seguir do autenticador WSTokenAuthenticator:

```
securityEnabled=true
credentialAuthentication=supported
credentialGeneratorClass=com.ibm.websphere.ssecurity.plugins.builtins.
WSTokenCredentialGenerator
```

Um cliente deve ser configurado para usar esse arquivo. Quando o cliente estiver em execução sob o WebSphere Application Server. Configure o cliente com o argumento JVM a seguir:

```
-Dobjectgrid.client.props=<client properties file>
```

Para assegurar implementação da grade, configure a segurança do aplicativo e Java 2 Security para servidores WebSphere Application Server que estejam hospedando servidores do eXtreme Scale. Use o painel de configuração de segurança do console administrativo do WebSphere Application Server para ativas essas configurações.

Agora, é possível continuar com a próxima etapa, "Autorizando Acesso à Grade de Dados no WebSphere Application Server" na página 145.

Autorizando Acesso à Grade de Dados

Impingir controle de acesso para que identidades autenticadas possam executar somente operações para as quais estão especificamente autorizadas.

O que Fazer Depois

"Autorizando Acesso para Operações Administrativas Especiais" na página 146

Autorizando Acesso à Grade de Dados em Ambientes Independentes

Controle quais usuários têm permissões específicas para acessar a grade de dados por meio do arquivo de políticas.

Sobre Esta Tarefa

Mesmo se um cliente for autenticado, isso pode não ser suficiente para proteger o acesso à grade de dados. Se você usar o KeyStoreLoginAuthenticator, geralmente, você define somente algumas identidades e todas as identidades podem ter acesso total à grade de dados. Nesse caso, a autorização pode não ser necessária. No entanto, se a autenticação LDAP for usada, pode haver muitas identidades no servidor LDAP que não devem ter acesso concedido aos dados de grade ou às operações.

Procedimento

1. Ative o controle de acesso para a grade de dados. Especifique `securityEnabled="true"` no arquivo `ObjectGrid.xml` para a grade de dados implementada.

   Especifique essa configuração para cada grade definida. Após configurar essa configuração, nenhuma leitura ou gravação será executada nas entradas da grade de dados, exceto para identidades às quais foram concedidas permissões em um arquivo de políticas.

2. Crie um arquivo de políticas. Consulte o arquivo de políticas de exemplo a seguir:

   ```
   grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
       principal javax.security.auth.x500.X500Principal "CN=cashier,O=acme,OU=OGSample" {
       permission com.ibm.websphere.objectgrid.security.MapPermission "accounting.*", "read ";
   };

   grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
       principal javax.security.auth.x500.X500Principal "CN=manager,O=acme,OU=OGSample" {
       permission com.ibm.websphere.objectgrid.security.MapPermission "accounting.*", "all";
   };
   ```

   Arquivos de políticas podem conceder várias permissões, dependendo da autorização do usuário. Para obter informações adicionais sobre como criar esse arquivo, consulte "Tutorial de Segurança do Java SE - Etapa 5" na página 30.

3. Configure cada servidor de contêiner para carregar esse arquivo de políticas. É possível concluir essa configuração iniciando o contêiner com o argumento da JVM a seguir:

   ```
   -Djava.security.policy=<policy file>
   ```

   Dica: Esse arquivo de políticas também é usado no controle de acesso administrativo aos servidores de grade de dados. Ao usar esse arquivo de políticas para controlar o acesso administrativo, o arquivo de políticas deve conter entradas MBeanPermission e deve ser carregado pelos servidores de catálogos e pelos servidores de contêineres.

O que Fazer Depois

"Autorizando Acesso para Operações Administrativas em Ambientes Independentes" na página 146

Autorizando Acesso à Grade de Dados no Perfil do Liberty

Controle quais usuários têm permissões específicas para acessar a grade de dados no Perfil do Liberty por meio do arquivo de políticas.

Sobre Esta Tarefa

Mesmo se um cliente for autenticado, isso pode não ser suficiente para proteger o acesso à grade de dados. Se você usar a propriedade KeyStoreLoginAuthenticator, geralmente, você define somente algumas identidades e todas as identidades podem ter acesso total à grade. Nesse caso, a autorização pode não ser necessária. Como alternativa, se a autenticação LDAP for usada, pode haver muitas identidades no servidor LDAP que não devem ter acesso concedido aos dados de grade ou às operações.

Procedimento

1. Ative o controle de acesso para a grade de dados. Especifique `securityEnabled="true"` no arquivo `ObjectGrid.xml` para a grade de dados implementada.

   Especifique essa configuração para cada grade definida. Após configurar essa configuração, nenhuma leitura ou gravação será executada nas entradas da grade de dados, exceto para identidades às quais foram concedidas permissões em um arquivo de políticas.
2. Crie um arquivo de políticas. Consulte o arquivo de políticas de exemplo a seguir:

   ```
   grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
       principal javax.security.auth.x500.X500Principal "CN=cashier,O=acme,OU=OGSample" {
       permission com.ibm.websphere.objectgrid.security.MapPermission "accounting.*", "read ";
   };

   grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
       principal javax.security.auth.x500.X500Principal "CN=manager,O=acme,OU=OGSample" {
       permission com.ibm.websphere.objectgrid.security.MapPermission "accounting.*", "all";
   };
   ```

   Arquivos de políticas podem conceder várias permissões, dependendo da autorização do usuário. Para obter informações adicionais sobre como criar esse arquivo, consulte "Tutorial de Segurança do Java SE - Etapa 5" na página 30.
3. Configure cada servidor de contêiner para carregar esse arquivo de políticas. É possível concluir esta configuração incluindo o argumento a seguir da JVM no arquivo `jvm.options` no diretório `wlp_installdir/usr/servers/<server_name>`:

   ```
   -Djava.security.policy=<policy file>
   ```

   Dica: Esse arquivo de políticas também é usado no controle de acesso administrativo aos servidores de grade de dados. Ao usar esse arquivo de políticas para controlar o acesso administrativo, o arquivo de políticas deve conter entradas MBeanPermission e deve ser carregado pelos servidores de catálogos e pelos servidores de contêineres.

   Se precisar criar um novo arquivo `jvm.options` no nível da configuração do servidor, será necessário copiar a versão no arquivo `wlp_install_root/etc/jvm.options`.

O que Fazer Depois

"Autorizando Acesso para Operações Administrativas no Perfil do Liberty" na página 147

Autorizando Acesso à Grade de Dados na Estrutura OSGi

Controle quais usuários têm permissões específicas para acessar a grade de dados da estrutura OSGi por meio do arquivo de políticas.

Antes de Iniciar

Você deve instalar a estrutura OSGi antes de assegurar a grade de dados. Para obter informações adicionais, consulte "Instalando a Estrutura do Eclipse Equinox OSGi com o Eclipse Gemini para Clientes e Servidores" na página 164.

Sobre Esta Tarefa

Mesmo se um cliente for autenticado, isso pode não ser suficiente para proteger o acesso à grade de dados. Se usar a KeyStoreLoginAuthenticator, geralmente, você define somente algumas identidades e todas as identidades podem ter acesso total à grade. Nesse caso, a autorização pode não ser necessária. Como alternativa, se a autenticação LDAP for usada, pode haver muitas identidades no servidor LDAP que não devem ter acesso concedido aos dados de grade ou às operações.

Procedimento

1. Ative o controle de acesso para a grade de dados. Especifique `securityEnabled="true"` no arquivo `ObjectGrid.xml` para a grade de dados implementada.

   Especifique essa configuração para cada grade definida. Após configurar essa configuração, nenhuma leitura ou gravação será executada nas entradas da grade de dados, exceto para identidades às quais foram concedidas permissões em um arquivo de políticas.

2. Crie um arquivo de políticas. Inclua as linhas de código a seguir no arquivo de políticas de segurança para conceder AllPermission ao arquivo `osgi.jar` para a grade de dados implementada.

   ```
   grant codeBase "file:/opt/OSGI2/plugins/org.eclipse.osgi_3.7.1.R37x_v20110808-1106.jar" {
     permission java.security.AllPermission;
   };
   ```

   Especifique esse código para cada grade definida. Após configurar essa configuração, nenhuma leitura ou gravação será executada nas entradas da grade de dados, exceto para identidades para as quais foram concedidas especificamente permissões em um arquivo de políticas. Arquivos de políticas podem conceder várias permissões, dependendo da autorização do usuário. Para obter informações adicionais sobre como criar esse arquivo, consulte "Tutorial de Segurança do Java SE - Etapa 5" na página 30.

   O arquivo de políticas é semelhante ao exemplo a seguir:

   Lembre-se: O arquivo de política geralmente também contém entradas MapPermission, conforme documentado em "Tutorial de Segurança do Java SE - Etapa 5" na página 30.

```
grant codeBase "file:${objectgrid.home}/lib/*" {
permission java.security.AllPermission;
};

grant principal javax.security.auth.x500.X500Principal "CN=manager,O=acme,OU=OGSample" {
permission javax.management.MBeanPermission "*", "getAttribute,setAttribute,invoke,queryNames";
};
```

3. Configure cada servidor de contêiner para carregar esse arquivo de políticas. É possível concluir essa configuração iniciando o contêiner com o argumento da JVM a seguir:

   ```
   -Djava.security.policy=<policy file>
   ```

   Dica: Esse arquivo de políticas também é usado no controle de acesso administrativo aos servidores de grade de dados. Ao usar esse arquivo de políticas para controlar o acesso administrativo, o arquivo de políticas deve conter entradas MBeanPermission e deve ser carregado pelos servidores de catálogos e pelos servidores de contêineres.

O que Fazer Depois

"Autorizando Acesso para Operações Administrativas na Estrutura OSGi" na página 148

Referências relacionadas:

Arquivo XML Descritor de Segurança
Use um arquivo XML descritor de segurança do ObjectGrid para configurar uma topologia de implementação do eXtreme Scale com a segurança ativada. Os elementos presentes nesse arquivo podem ser usados para configurar diferentes aspectos de segurança.

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Arquivo XML descritor do ObjectGrid
Para configurar o WebSphere eXtreme Scale, utilize um arquivo XML descritor do ObjectGrid e a API do ObjectGrid.

Arquivo Descritor XML de Política de Implementação
Para configurar uma política de implementação, utilize um arquivo XML do descritor da política de implementação.

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Informações relacionadas:

Documentação da API

Autorizando Acesso à Grade de Dados no WebSphere Application Server

Controle quais usuários têm permissões específicas para acessar a grade de dados em implementações do WebSphere Application Server da mesma maneira que controla o acesso à grade de dados em implementações independentes.

Sobre Esta Tarefa

Mesmo se um cliente for autenticado, isso pode não ser suficiente para proteger o acesso à grade de dados. Se você usar o KeyStoreLoginAuthenticator, geralmente, você define somente algumas identidades e todas as identidades podem ter acesso total à grade de dados. Nesse caso, a autorização pode não ser necessária. No

entanto, se a autenticação LDAP for usada, pode haver muitas identidades no servidor LDAP que não devem ter acesso concedido aos dados de grade ou às operações.

Atenção: Não é necessário especificar MBeanPermissions para implementações do WebSphere Application Server de servidores do eXtreme Scale, porque o acesso de JMX é controlado pelo próprio WebSphere Application Server.

Procedimento

1. Ative o controle de acesso para a grade de dados. Especifique `securityEnabled="true"` no arquivo `ObjectGrid.xml` para a grade de dados implementada.

   Especifique essa configuração para cada grade definida. Após configurar essa configuração, nenhuma leitura ou gravação será executada nas entradas da grade de dados, exceto para identidades às quais foram concedidas permissões em um arquivo de políticas.
2. Crie um arquivo de políticas. Arquivos de políticas podem conceder várias permissões, dependendo da autorização do usuário. Para obter informações adicionais sobre como criar esse arquivo, consulte "Lição 4.2: Ativar Autorização Baseada no Usuário" na página 66.
3. Configure cada servidor de contêiner para carregar esse arquivo de políticas. É possível especificar o arquivo de políticas nos argumentos Genéricos da JVM do servidor de aplicativos no qual o contêiner é executado. Para obter informações adicionais sobre como configurar o arquivo de propriedades do servidor com propriedades JVM, consulte "Lição 2.2: Configurar a Segurança do Servidor de Catálogos" na página 56.

   ```
   -Djava.security.policy=<policy file>
   ```

O que Fazer Depois

"Autorizando Acesso para Operações Administrativas no WebSphere Application Server" na página 149

Autorizando Acesso para Operações Administrativas Especiais

Autorização especial requerida para usuários executarem operações administrativas na grade de dados.

O que Fazer Depois

"Protegendo Dados que Fluem entre os Clientes e os Servidores do eXtreme Scale com Criptografia SSL" na página 149

Autorizando Acesso para Operações Administrativas em Ambientes Independentes

A maioria dos implementadores de grade de dados restringem o acesso administrativo apenas a um subconjunto dos usuários que podem acessar os dados da grade.

Procedimento

Você deve executar os servidores de catálogos e servidores de contêiner usando o gerenciador de segurança Java, o que requer um arquivo de políticas.
O arquivo de políticas é especificado passando o argumento da JVM

-Djava.security.policy=<*policy_file*>.
O gerenciador de segurança Java é iniciado especificando o argumento da JVM, -Djava.security.manager, quando o servidor do eXtreme Scale é iniciado. Especifique esse argumento para ambos os servidores de contêineres e de catálogos.
O arquivo de políticas é semelhante ao exemplo a seguir:

Lembre-se: O arquivo de política geralmente também contém entradas MapPermission, conforme documentado em "Tutorial de Segurança do Java SE - Etapa 5" na página 30.

```
grant codeBase "file:${objectgrid.home}/lib/*" {
permission java.security.AllPermission;
};

grant principal javax.security.auth.x500.X500Principal "CN=manager,O=acme,OU=OGSample" {
permission javax.management.MBeanPermission "*", "getAttribute,setAttribute,invoke,queryNames";
};
```

Neste exemplo, somente o proprietário gerenciador é autorizado para operações administrativas com o comando **xscmd**. É possível incluir outras linhas conforme necessário para fornecer aos proprietários adicionais permissões de MBean.

Digite o seguinte comando: UNIX Linux

```
startOgServer.sh <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
-Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=$OBJECTGRID_HOME
```

UNIX Linux 8.6+

```
startXsServer.sh <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
-Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=$OBJECTGRID_HOME
```

Windows

```
startOgServer.bat <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
-Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=%OBJECTGRID_HOME%
```

Windows 8.6+

```
startXsServer.bat <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
 -Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=%OBJECTGRID_HOME%
```

O que Fazer Depois

"Protegendo Dados que Fluem entre Servidores eXtreme Scale em Ambientes Independentes com Criptografia SSL" na página 149

Autorizando Acesso para Operações Administrativas no Perfil do Liberty

Por meio da segurança administrativa, é possível autorizar os usuários a acessar a grade de dados no Perfil do Liberty.

Sobre Esta Tarefa

A maioria dos implementadores de grade de dados restringem o acesso administrativo apenas a um subconjunto dos usuários que podem acessar os dados da grade.

Procedimento

- Execute o gerenciador de segurança Java e especifique um arquivo de políticas que conceda MBeanPermissions, para restringir o acesso administrativo quando

servidores do eXtreme Scale estão em execução no Perfil do Liberty. Essa abordagem é a mesma que em implementações independentes. Insira as linhas a seguir no arquivo `jvm.options` para cada servidor de Perfil do Liberty que esteja executando um servidor de catálogos ou de contêiner do eXtreme Scale.

```
-Djava.security.manager
-Djava.security.policy="policy file"
```

- Configure o arquivo de políticas para conceder ao Perfil do Liberty e ao código do eXtreme Scale todas as permissões. Essa configuração permite que o Perfil do Liberty e o eXtreme Scale funcionem com o gerenciador de segurança. Insira as linhas a seguir no arquivo `jvm.options` que está no nível do servidor:

```
grant codeBase "file:${objectgrid.home}/lib/*" {
permission java.security.AllPermission;
};
```

O que Fazer Depois

"Protegendo Dados que Fluem entre o eXtreme Scale e o Perfil do Liberty com Criptografia SSL" na página 151

Autorizando Acesso para Operações Administrativas na Estrutura OSGi

Por meio da segurança administrativa, é possível autorizar os usuários a acessar a grade de dados na estrutura OSGi.

Antes de Iniciar

Você deve instalar a estrutura OSGi antes de assegurar a grade de dados. Para obter informações adicionais, consulte "Instalando a Estrutura do Eclipse Equinox OSGi com o Eclipse Gemini para Clientes e Servidores" na página 164.

Sobre Esta Tarefa

A maioria dos implementadores de grade de dados restringem o acesso administrativo apenas a um subconjunto dos usuários que podem acessar os dados da grade.

Procedimento

- Você deve executar os servidores de catálogos e servidores de contêiner usando o gerenciador de segurança Java, o que requer um arquivo de políticas.

  O arquivo de políticas é especificado passando o argumento da JVM `-Djava.security.policy=<policy_file>`.

  O gerenciador de segurança Java é iniciado especificando o argumento da JVM, -Djava.security.manager, quando o servidor do eXtreme Scale é iniciado. Especifique esse argumento para ambos os servidores de contêineres e de catálogos.

  O arquivo de políticas é semelhante ao exemplo a seguir:

  Lembre-se: O arquivo de política geralmente também contém entradas MapPermission, conforme documentado em "Tutorial de Segurança do Java SE - Etapa 5" na página 30.

```
grant codeBase "file:${objectgrid.home}/lib/*" {
permission java.security.AllPermission;
};

grant principal javax.security.auth.x500.X500Principal "CN=manager,O=acme,OU=OGSample" {
permission javax.management.MBeanPermission "*", "getAttribute,setAttribute,invoke,queryNames";
};
```

Neste exemplo, somente o proprietário gerenciador é autorizado para operações administrativas com o comando **xscmd**. É possível incluir outras linhas conforme necessário para fornecer aos proprietários adicionais permissões de MBean.

- Inicie os contêineres de catálogos e de servidores especificando os argumentos anteriores da JVM na linha de comandos; por exemplo:

```
/opt/XS86/java/jre/bin/java -DclusterSecurityFile=/og
/security/secFiles_SA/objectGridSecurity.xml -Djava.security.auth.login.config=/og/security/sec
```

O que Fazer Depois

"Protegendo Dados que Fluem entre o eXtreme Scale e a Estrutura OSGi com Criptografia SSL" na página 153

Autorizando Acesso para Operações Administrativas no WebSphere Application Server

Por meio de segurança administrativa, somente administradores do WebSphere Application Server podem executar operações administrativas do eXtreme Scale.

Sobre Esta Tarefa

Autorização para acesso administrativo funciona de forma diferente nas implementações do WebSphere Application Server do que em ambientes independentes. Somente usuários do WebSphere Application Server que são administradores do WebSphere Application Server podem executar operações administrativas do eXtreme Scale. Não é necessário especificar MbeanPermissions no arquivo de políticas.

Procedimento

Ativar segurança administrativa no WebSphere Application Server. No console administrativo, clique em **Segurança** > **Segurança Global**. Clique em **Ativar Segurança Administrativa** e selecione **Java 2 Security** para restringir acesso do aplicativo a recursos locais.

O que Fazer Depois

"Protegendo Dados que Fluem entre o eXtreme Scale e o WebSphere Application Server com Criptografia SSL" na página 154

Protegendo Dados que Fluem entre os Clientes e os Servidores do eXtreme Scale com Criptografia SSL

Proteger a comunicação entre os clientes e os servidores do WebSphere eXtreme Scale com criptografia SSL.

O que Fazer Depois

"Armazenando Artefatos de Segurança para Usuários Autorizados" na página 155

Protegendo Dados que Fluem entre Servidores eXtreme Scale em Ambientes Independentes com Criptografia SSL

Configure as propriedades SSL e as portas JMX para proteger informações confidenciais que fluem entre servidores pela rede.

Sobre Esta Tarefa

Quando uma grade de dados for implementada, as informações confidenciais que contém fluem pela rede. Além disso, as credenciais que os clientes da grade de dados usam para autenticação na grade de dados fluem pela rede. Para proteger dados e credenciais à medida que fluem, use a criptografia no nível do transporte usando SSL para implementações seguras.

A segurança de SSL depende da proteção dos keystores e dos armazenamentos confiáveis, de forma que somente usuários autorizados tenham acesso aos keystores e aos armazenamentos confiáveis. Após ativar criptografia SSL, você deve especificar um valor de JMXConnectorPort e de JMXServicePort no arquivo de propriedades do servidos para ter proteção SSL para tráfego de JMX.

O transporte entre o cliente e o servidor JMX pode ser assegurado com transport layer security (TLS) ou SSL. Se o transportType do servidor de catálogos ou servidor de contêiner for configurado como SSL_Required ou SSL_Supported, você deverá usar o SSL para conectar-se ao servidor JMX.

Procedimento

1. Especifique SSL no arquivo de propriedades do servidor. Configure a propriedade transportType para `SSL-Required`; por exemplo:

   ```
   transportType=SSL-Required
   ```

2. Especifique propriedades de SSL no arquivo de propriedades do servidor.

   ```
   alias=serverprivate
   contextProvider=IBMJSSE2
   protocol=SSL
   keyStoreType=JKS
   keyStore=etc/test/security/key.jks
   keyStorePassword=serverpw
   trustStoreType=JKS
   trustStore=etc/test/security/trust.jks
   trustStorePassword=public
   clientAuthentication=false
   ```

   Configure o armazenamento confiável, o tipo de armazenamento confiável e a senha do armazenamento confiável. Não é necessário especificar um keystore, um tipo de keystore e a senha do armazenamento de chaves para o cliente. O alias, o keystore, a senha do keystore e o tipo de keystore não são necessários no cliente, a menos que as propriedades de SSL do servidor incluam `clientAuthentication=true`. Esse valor é raramente usado.

   O armazenamento confiável do cliente deve confiar no certificado do servidor. Quando o certificado do servidor é autoassinado, como no tutorial, esse certificado deve ser importado para o armazenamento confiável do cliente. Quando o certificado do servidor é emitido por uma autoridade de certificação local, o certificado de assinante para essa autoridade de certificação deve ser importado para o armazenamento confiável do cliente. Para obter informações adicionais sobre como criar arquivos de keystore e de armazenamento confiável, consulte “Tutorial de Segurança do Java SE - Etapa 6” na página 34.

3. Especifique SSL no arquivo de propriedades do cliente quando SSL for necessário. Configure a propriedade transportType para `SSL-Required` ou `SSL-Supported`; por exemplo:

   ```
   transportType=SSL-Required
   ```

4. Especifique propriedades de SSL no arquivo de propriedades do cliente. Por exemplo, é possível especificar as propriedades a seguir:

```
alias=clientprivate
contextProvider=IBMJSSE2
protocol=SSL
keyStoreType=JKS
keyStore=etc/test/security/client.private
keyStorePassword={xor}PDM2OjErLyg\=
trustStoreType=JKS
trustStore=etc/test/security/server.public
trustStorePassword={xor}Lyo9MzY8
```

5. Configure a porta de serviço JMX. Use a opção **-JMXServicePort** no script **startOgServer** ou **startXsServer**.

   O valor padrão para a porta de serviço JMX nos servidores de catálogos é 1099. Você deve usar um número da porta diferente para cada JVM na configuração. Se desejar usar o JMX/RMI, especifique explicitamente a opção **-JMXServicePort** e o número da porta, mesmo se desejar usar o valor da porta padrão.

6. Configure a porta do conector JMX.

   Use a opção **-JMXConnectorPort** no script **startOgServer** ou **startXsServer**.

   A configuração da porta de serviço JMX é requerida quando você deseja exibir informações do servidor de contêiner a partir do servidor de catálogos. Por exemplo, a porta é necessária quando estiver usando o comando **xscmd -c showMapSizes**. Configure a porta do conector JMX para evitar a criação de porta efêmera.

O que Fazer Depois

"Armazenando Artefatos de Segurança em Ambientes Independentes" na página 156

Referências relacionadas:

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Protegendo Dados que Fluem entre o eXtreme Scale e o Perfil do Liberty com Criptografia SSL

Configure as propriedades SSL e as portas JMX para proteger informações confidenciais que fluem entre o WebSphere eXtreme Scale e o Perfil do Liberty.

Sobre Esta Tarefa

Quando uma grade de dados for implementada, as informações confidenciais que contém fluem pela rede. Além disso, as credenciais que os clientes da grade de dados usam para autenticação na grade de dados fluem pela rede. Para proteger dados e credenciais à medida que fluem, use a criptografia no nível do transporte usando SSL para implementações seguras.

A segurança de SSL depende da proteção dos keystores e dos armazenamentos confiáveis, de forma que somente usuários autorizados tenham acesso aos

keystores e aos armazenamentos confiáveis. Após ativar criptografia SSL, você deve especificar um valor de JMXConnectorPort e de JMXServicePort no arquivo de propriedades do servidos para ter proteção SSL para tráfego de JMX.

O transporte entre o cliente e o servidor JMX pode ser assegurado com transport layer security (TLS) ou SSL. Se o transportType do servidor de catálogos ou servidor de contêiner for configurado como SSL_Required ou SSL_Supported, você deverá usar o SSL para conectar-se ao servidor JMX.

Procedimento

1. Especifique SSL no arquivo de propriedades do servidor. Configure a propriedade transportType para `SSL-Required`; por exemplo:

   ```
   transportType=SSL-Required
   ```

2. Especifique propriedades de SSL no arquivo de propriedades do servidor.

   ```
   alias=serverprivate
   contextProvider=IBMJSSE2
   protocol=SSL
   keyStoreType=JKS
   keyStore=etc/test/security/key.jks
   keyStorePassword=serverpw
   trustStoreType=JKS
   trustStore=etc/test/security/trust.jks
   trustStorePassword=public
   clientAuthentication=false
   ```

   Configure o armazenamento confiável, o tipo de armazenamento confiável e a senha do armazenamento confiável. Não é necessário especificar um keystore, um tipo de keystore e a senha do armazenamento de chaves para o cliente. O alias, o keystore, a senha do keystore e o tipo de keystore não são necessários no cliente, a menos que as propriedades de SSL do servidor incluam `clientAuthentication=true`. Esse valor é raramente usado.

   O armazenamento confiável do cliente deve confiar no certificado do servidor. Quando o certificado do servidor é autoassinado, como no tutorial, esse certificado deve ser importado para o armazenamento confiável do cliente. Quando o certificado do servidor é emitido por uma autoridade de certificação local, o certificado de assinante para essa autoridade de certificação deve ser importado para o armazenamento confiável do cliente. Para obter informações adicionais sobre como criar arquivos de keystore e de armazenamento confiável, consulte “Tutorial de Segurança do Java SE - Etapa 6” na página 34.

3. Especifique SSL no arquivo de propriedades do cliente quando SSL for necessário. Configure a propriedade transportType para `SSL-Required` ou `SSL-Supported`; por exemplo:

   ```
   transportType=SSL-Required
   ```

4. Especifique propriedades de SSL no arquivo de propriedades do cliente. Por exemplo, é possível especificar as propriedades a seguir:

   ```
   alias=clientprivate
   contextProvider=IBMJSSE2
   protocol=SSL
   keyStoreType=JKS
   keyStore=etc/test/security/client.private
   keyStorePassword={xor}PDM2OjErLyg\=
   trustStoreType=JKS
   trustStore=etc/test/security/server.public
   trustStorePassword={xor}Lyo9MzY8
   ```

5. Configure a porta de serviço JMX no arquivo de propriedades do servidor.

O valor padrão para a porta de serviço JMX nos servidores de catálogos é 1099. Você deve usar um número da porta diferente para cada JVM na configuração. Se desejar usar o JMX/RMI, especifique explicitamente a opção **rver JMXServicePort** e o número da porta, mesmo se desejar usar o valor da porta padrão.

6. Configure a porta do conector JMX no arquivo de propriedades do servidor.

   A configuração da porta de serviço JMX é requerida quando você deseja exibir informações do servidor de contêiner a partir do servidor de catálogos. Por exemplo, a porta é necessária quando estiver usando o comando **xscmd -c showMapSizes**. Configure a porta do conector JMX para evitar a criação de porta efêmera.

O que Fazer Depois

"Armazenando Artefatos de Segurança no Perfil do Liberty" na página 156

Referências relacionadas:

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Protegendo Dados que Fluem entre o eXtreme Scale e a Estrutura OSGi com Criptografia SSL

Configure as propriedades SSL e as portas JMX para proteger informações confidenciais que fluem entre o WebSphere eXtreme Scale e a estrutura OSGi.

Antes de Iniciar

Você deve instalar a estrutura OSGi antes de assegurar a grade de dados. Para obter informações adicionais, consulte "Instalando a Estrutura do Eclipse Equinox OSGi com o Eclipse Gemini para Clientes e Servidores" na página 164.

Sobre Esta Tarefa

Quando uma grade de dados for implementada, as informações confidenciais que contém fluem pela rede. Além disso, as credenciais que os clientes da grade de dados usam para autenticação na grade de dados fluem pela rede. Para proteger dados e credenciais à medida que fluem, use a criptografia no nível do transporte usando SSL para implementações seguras.

A segurança de SSL depende da proteção dos keystores e dos armazenamentos confiáveis, de forma que somente usuários autorizados tenham acesso aos keystores e aos armazenamentos confiáveis. Após ativar criptografia SSL, você deve especificar um valor de JMXConnectorPort e de JMXServicePort no arquivo de propriedades do servidos para ter proteção SSL para tráfego de JMX.

O transporte entre o cliente e o servidor JMX pode ser assegurado com transport layer security (TLS) ou SSL. Se o transportType do servidor de catálogos ou servidor de contêiner for configurado como SSL_Required ou SSL_Supported, você

deverá usar o SSL para conectar-se ao servidor JMX.

Procedimento

1. Especifique SSL no arquivo de propriedades do servidor. Configure a propriedade transportType para `SSL-Required`; por exemplo:

   ```
   transportType=SSL-Required
   ```

2. Para usar SSL, é necessário configurar o armazenamento confiável, o tipo de armazenamento confiável e a senha do armazenamento confiável no cliente MBean com as propriedades do sistema -D; por exemplo:

   ```
   -Djavax.net.ssl.trustStore=TRUST_STORE_LOCATION
   -Djavax.net.ssl.trustStorePassword=TRUST_STORE_PASSWORD
   -Djavax.net.ssl.trustStoreType=TRUST_STORE_TYPE
   ```

   Se com.ibm.websphere.ssl.protocol.SSLSocketFactory for usado como seu factory de soquete SSL em seu arquivo *java_home*`/jre/lib/security/java.security`, use as seguintes propriedades:

   ```
   -Dcom.ibm.ssl.trustStore=TRUST_STORE_LOCATION
   -Dcom.ibm.ssl.trustStorePassword=TRUST_STORE_PASSWORD
   -Dcom.ibm.ssl.trustStoreType=TRUST_STORE_TYPE
   ```

3. Configure a porta de serviço JMX no arquivo de propriedades do servidor.

   O valor padrão para a porta de serviço JMX nos servidores de catálogos é `1099`. Você deve usar um número da porta diferente para cada JVM na configuração. Se desejar usar JMX/RMI, especifique explicitamente a opção **JMXServicePort** e o número da porta, mesmo se desejar usar o valor da porta padrão.

4. Configure a porta do conector JMX no arquivo de propriedades do servidor.

   A configuração da porta de serviço JMX é requerida quando você deseja exibir informações do servidor de contêiner a partir do servidor de catálogos. Por exemplo, a porta é necessária quando estiver usando o comando **xscmd -c showMapSizes**. Configure a porta do conector JMX para evitar a criação de porta efêmera.

5. Especifique a porta SSL na linha de comandos da estrutura OSGi usando o argumento a seguir da JVM:

   ```
   -Dcom.ibm.CSI.SSL.Port=7602
   ```

O que Fazer Depois

"Armazenando Artefatos de Segurança na Estrutura OSGi" na página 157

Referências relacionadas:

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Protegendo Dados que Fluem entre o eXtreme Scale e o WebSphere Application Server com Criptografia SSL

O WebSphere eXtreme Scale usa a configuração de Secure Sockets Layer (SSL) no WebSphere Application Server .

Sobre Esta Tarefa

Para assegurar que você tenha proteção SSL para todo o tráfego da grade de dados que passa pela rede, configure segurança global, configure segurança de entrada e saída de CSIv2 no console administrativo do WebSphere Application Server e configure o certificado SSL e gerenciamento de chaves.

Procedimento

1. Configure a segurança global do WebSphere Application Server. Para obter informações adicionais sobre como configurar a segurança global, consulte Configurações de Segurança Global.
2. Configure a segurança de entrada de CSIv2. No console administrativo do WebSphere Application Server, clique em **Segurança** > **Segurança Global** > **Segurança RMI/IIOP** > **Comunicações de Entrada CSIv2**. Clique em **SSL-Required**.
3. Configure a segurança de saída de CSIv2. No console administrativo do WebSphere Application Server, clique em **Segurança** > **Segurança Global** > **Segurança RMI/IIOP** > **Comunicações de Entrada CSIv2**. As comunicações de saída de CSIv2 devem ser **SSL-Supported** ou **SSL-Required**.
4. Configure o certificado SSL e o gerenciamento de chaves no WebSphere Application Server. Quando executar somente um cliente do WebSphere eXtreme Scale em uma instância do WebSphere Application Server e os servidores de grade de dados do eXtreme Scale forem independentes. Você deve assegurar que as informações de certificado de keystore e de armazenamento confiável estejam incluídas nos arquivos de keystore e de armazenamento confiável especificados no arquivo de propriedades do servidor que é usado para iniciar seus servidores de catálogos e de contêineres independentes.

   Quando o cliente, os servidores de catálogos e de contêineres estiverem todos em execução em processos do WebSphere Application Server, eles usam a configuração de segurança do WebSphere Application Server para a comunicação cliente-servidor.

   No entanto, quando diversos servidores de catálogos estão configurados e em execução em um processo do WebSphere Application Server, a comunicação de catálogo para catálogo tem seus próprios caminhos de transporte proprietários que não podem ser gerenciados pelas configurações de transporte Common Secure Interoperability Protocol Version 2 (CSIV2) do WebSphere Application Server. Portanto, você deve configurar as propriedades SSL no arquivo de propriedades do servidor para cada servidor de catálogos. Para obter informações adicionais, consulte “Lição 3.2: Incluir Propriedades SSL no Arquivo de Propriedades do Servidor de Catálogos” na página 63.

O que Fazer Depois

“Armazenando Artefatos de Segurança no WebSphere Application Server” na página 157

Armazenando Artefatos de Segurança para Usuários Autorizados

Armazenamentos de chaves, senhas, segredos compartilhados e arquivos de propriedades devem ser armazenados em um diretório que possa ser acessado somente por usuários autorizados.

O que Fazer Depois

"Iniciando e Parando Servidores Seguros" na página 158

Armazenando Artefatos de Segurança em Ambientes Independentes

Proteja senhas seguras para evitar acesso de usuários não autorizados.

Sobre Esta Tarefa

O utilitário FilePasswordEncoder está incluído com o WebSphere eXtreme Scale Client para codificar senhas nos arquivos de configuração do eXtreme Scale. O utilitário FilePasswordEncoder codifica senhas; no entanto, é possível recuperar as senhas que são usadas para acessar o arquivo. Portanto,você deve proteger o sistema de arquivos no qual as propriedades do cliente, as propriedades do servidor e os keystores e armazenamentos confiáveis são mantidos, de forma que somente usuários autorizados tenha acesso.

Procedimento

Execute o comando **FilePasswordEncoder.bat|sh** para codificar essa propriedade usando um algoritmo `exclusive or` (xor) para fornecer uma medida de proteção para senhas.
Execute o utilitário FilePasswordEncoder no arquivo `client.properties` e no arquivo `server.properties`; por exemplo:

```
./FilePasswordEncoder.sh <server properties file>
./FilePasswordEncoder.sh <client properties file>
```

Um usuário sofisticado pode recuperar senhas codificadas. Essas senhas não são criptografadas, pois o código do eXtreme Scale deve ser capaz de recuperá-las para executar. Portanto, assegure que somente pessoas autorizadas possam acessar os arquivos nos quais essas senhas estão armazenadas.

O que Fazer Depois

"Iniciando Servidores Seguros em um Ambiente Independente" na página 158

Armazenando Artefatos de Segurança no Perfil do Liberty

Proteja senhas seguras para evitar acesso de usuários não autorizados do eXtreme Scale no Perfil do Liberty.

Sobre Esta Tarefa

O utilitário FilePasswordEncoder está incluído com o WebSphere eXtreme Scale Client para codificar senhas nos arquivos de configuração do eXtreme Scale.

Procedimento

1. Execute o comando **securityUtility.bat|sh** do perfil do Liberty para codificar essa propriedade usando um algoritmo `exclusive or` (xor) para fornecer uma medida de proteção para senhas. Esteja ciente de que um usuário sofisticado pode recuperar senhas codificadas. Essas senhas não são criptografadas, pois o código do eXtreme Scale deve ser capaz de recuperá-las para executar. Portanto, assegure que somente pessoas autorizadas possam acessar os arquivos nos quais essas senhas estão armazenadas.

2. Limite o acesso aos arquivos keystore e aos arquivos de armazenamento confiável protegendo o acesso ao sistema de arquivos no qual estão armazenados.

O que Fazer Depois

"Iniciando e Parando Servidores Seguros no Perfil do Liberty" na página 159

Armazenando Artefatos de Segurança na Estrutura OSGi

Proteja senhas seguras para evitar acesso de usuários não autorizados na estrutura OSGi.

Antes de Iniciar

Você deve instalar a estrutura OSGi antes de assegurar a grade de dados. Para obter informações adicionais, consulte "Instalando a Estrutura do Eclipse Equinox OSGi com o Eclipse Gemini para Clientes e Servidores" na página 164.

Sobre Esta Tarefa

O utilitário FilePasswordEncoder está incluído com o WebSphere eXtreme Scale Client para codificar senhas nos arquivos de configuração do eXtreme Scale.

Procedimento

1. Execute o comando **`FilePasswordEncoder.bat|sh`** para codificar essa propriedade usando um algoritmo `exclusive or` (xor) para fornecer uma medida de proteção para senhas. Esteja ciente de que um usuário sofisticado pode recuperar senhas codificadas. Essas senhas não são criptografadas, pois o código do eXtreme Scale deve ser capaz de recuperá-las para executar. Portanto, assegure que somente pessoas autorizadas possam acessar os arquivos nos quais essas senhas estão armazenadas.
2. Limite o acesso aos arquivos keystore e aos arquivos de armazenamento confiável protegendo o acesso ao sistema de arquivos no qual estão armazenados.

O que Fazer Depois

"Iniciando e Parando Servidores Seguros na Estrutura OSGi" na página 160

Armazenando Artefatos de Segurança no WebSphere Application Server

Proteja senhas seguras para evitar acesso de usuários não autorizados em implementações do WebSphere Application Server.

Sobre Esta Tarefa

Senhas e o authenticationSecret nos arquivos de propriedades de servidor e de propriedades de cliente devem ser codificados.

Procedimento

Chame o PropFilePasswordEncoder para codificar senhas e o secreto de autenticação. Execute o comando *was_root*`/bin/PropFilePasswordEncoder.sh` ou, no Windows, execute o comando *was_root*`\bin\PropFilePasswordEncoder.bat`; por exemplo:

```
./PropFilePasswordEncoder <properties_file> <property_to_encode>
```

Propriedades que devem ser codificadas incluem **keyStorePassword**, **trustStorePassword**, **credentialGeneratorProps** e **authenticationSecret**. Mesmo quando essas propriedades são codificadas, é possível recuperar os valores originais. O sistema de arquivos no qual os arquivos de propriedades, armazenamentos de chaves e armazenamentos confiáveis são mantidos devem ser protegidos, portanto, somente usuários autorizados podem acessá-los. Consulte a documentação do WebSphere Application Server para obter informações adicionais.

O que Fazer Depois

"Iniciando Servidores Seguros no WebSphere Application Server" na página 161

Informações relacionadas:

Documentação do WebSphere Application Server

Iniciando e Parando Servidores Seguros

A segurança é ativada ao definir as configurações específicas de segurança quando você inicia e para servidores.

Iniciando Servidores Seguros em um Ambiente Independente

Para iniciar servidores independentes seguros, transmita os arquivos de configuração adequados, especificando os parâmetros no comando **startOgServer** ou **startXsServer**.

8.6+

Sobre Esta Tarefa

Reprovado: 8.6+ Os comandos **startOgServer** e **stopOgServer** iniciam servidores que usam o mecanismo de transporte do Object Request Broker (ORB). O ORB foi descontinuado, mas você pode continuar utilizando esses scripts se estava utilizando o ORB em uma liberação anterior. O mecanismo de transporte do IBM eXtremeIO (XIO) substitui o ORB. Use os scripts **startXsServer** e **stopXsServer** para iniciar e parar os servidores que utilizam o transporte XIO.

Procedimento

- Inicie seus servidores de contêiner seguros.

  Iniciar um servidor de contêiner seguro requer o seguinte arquivo de configuração de segurança:

  – **Arquivo de propriedades do servidor:** O arquivo de propriedades do servidor configura as propriedades de segurança específicas para o servidor. Consulte o Arquivo de Propriedades do Servidor para obter mais detalhes.

  Especifique o local deste arquivo de configuração fornecendo o argumento a seguir ao script **startOgServer** ou **startXsServer**:

  -serverProps
  Especifica o local do arquivo de propriedades do servidor, que contém as propriedades de segurança específicas do servidor. O nome do arquivo especificado para esta propriedade está em formato de caminho de arquivo simples, como `../security/server.properties`.

  Insira as linhas a seguir ao executar o comando **startOgServer** ou o comando **startXsServer**: UNIX Linux

```
startOgServer.sh <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
-Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=$OBJECTGRID_HOME
```

UNIX Linux 8.6+

```
startXsServer.sh <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
-Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=$OBJECTGRID_HOME
```

Windows

```
startOgServer.bat <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
-Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=%OBJECTGRID_HOME%
```

Windows 8.6+

```
startXsServer.bat <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
 -Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=%OBJECTGRID_HOME%
```

- Inicie os servidores de catálogos seguros.

  Para iniciar um serviço de catálogo seguro, você deve ter os seguintes arquivos de configuração:

  – **Arquivo descritor XML de segurança:** O arquivo descritor XML de segurança descreve as propriedades de segurança comuns para todos os servidores, incluindo servidores de catálogo e servidores de contêiner. Um exemplo de propriedade é a configuração do autenticador que representa o registro do usuário e o mecanismo de autenticação.

  – **Arquivo de propriedades do servidor:** O arquivo de propriedades do servidor configura as propriedades de segurança que são específicas para o servidor.

  Especifique o local destes arquivos de configuração fornecendo os argumentos a seguir ao script **startOgServer** ou **startXsServer**:

  -clusterSecurityFile e -clusterSecurityUrl
  Estes argumentos especificam o local do arquivo descritor XML de Segurança. Use o parâmetro **-clusterSecurityFile** para especificar um arquivo local ou o parâmetro **-clusterSecurityUrl** para especificar a URL do arquivo `objectGridSecurity.xml`.

  -serverProps
  Especifica o local do arquivo de propriedades do servidor, que contém as propriedades de segurança específicas do servidor. O nome do arquivo especificado para esta propriedade está em formato de caminho de arquivo simples, tal como `c:/tmp/og/catalogserver.props`.

Iniciando e Parando Servidores Seguros no Perfil do Liberty

Use o comando inicial para iniciar servidores seguros no Perfil do Liberty

Sobre Esta Tarefa

Utilize esta tarefa para iniciar servidores eXtreme Scale com o comando **server** do Perfil do Liberty. O diretório `wlp/bin` contém um script chamado **server** para ajudar a controlar o processo do servidor. A seguinte sintaxe para esse comando é suportada:

```
server <task> [server] [options]
```

Procedimento

- Inicie os servidors eXtreme Scale. Quando você executa o comando **start**, o servidor é ativado como um processo de segundo plano. Utilize o exemplo a seguir para iniciar o servidor:

```
bin/server start server_name
bin/server.bat start server_name
```

- Pare os servidores eXtreme Scale; por exemplo: Quando você executa o comando **stop**, o servidor em execução é interrompido. Use o exemplo a seguir para parar o servidor:

```
bin/server stop server_name
bin/server.bat stop server_name
```

Iniciando e Parando Servidores Seguros na Estrutura OSGi

Para iniciar os servidores independentes seguros na estrutura OSGi do Eclipse Equinox, passe os arquivos de configuração adequados especificando parâmetros a partir da linha de comandos.

Antes de Iniciar

Você deve instalar a estrutura OSGi antes de assegurar a grade de dados. Para obter informações adicionais, consulte "Instalando a Estrutura do Eclipse Equinox OSGi com o Eclipse Gemini para Clientes e Servidores" na página 164.

Procedimento

1. Inicie o console de OSGi.
2. Passe a configuração de autorização, o arquivo de políticas de segurança e a porta SSL a partir da linha de comandos. Consulte o seguinte exemplo:

   ```
   java -Djava.security.auth.login.config=/og/security/secFiles_SA/ogjaas.config -Djava.security.man
   ```

3. Inicie o servidor de catálogos. Especifique as linhas de código a seguir a partir da linha de comandos:

   ```
   - cm create com.ibm.websphere.xs.server
   - cm put com.ibm.websphere.xs.server clusterSecurityFile /og
   /security/secFiles_SA/objectGridSecurity.xml
   - cm put com.ibm.websphere.xs.server objectgrid.server.props /opt/OSGI2/load/secServer.properties
   ```

   O servidor de catálogos é iniciado com base nas propriedades configuradas no arquivo CML de segurança de ObjectGrid e do arquivo de propriedades do servidor de segurança.
4. Inicie o servidor de contêiner. Especifique as linhas de código a seguir a partir da linha de comandos:

   ```
   cm createf com.ibm.websphere.xs.container
   cm put com.ibm.websphere.xs.container-1347819831596-0 objectgridFile /opt/OSGI2/load/objectgridSe
   cm put com.ibm.websphere.xs.container-1347819831596-0 deploymentPolicyFile /opt/OSGI2/load/deploy
   ```

   O servidor de contêiner é iniciado com base nas propriedades configuradas no arquivo XML descritor de ObjectGrid e do arquivo XML descritor da política de implementação.
5. Pare os servidores seguros na estrutura OSGi. Depois de um pacote configurável do servidor do eXtreme Scale ser iniciado e o servidor do eXtreme Scale ser inicializado, ele não poderá ser reiniciado. O processo do Eclipse Equinox deve ser reiniciado para reiniciar um servidor do eXtreme Scale.

   É possível usar o suporte do eXtreme Scale para o namespace do Spring para configurar os servidores de contêiner do eXtreme Scale em um arquivo XML do Blueprint. Quando os elemento XML do servidor e do contêiner são incluídos no arquivo XML do Blueprint, o manipulador de namespace do eXtreme Scale inicia automaticamente um servidor de contêiner usando os parâmetros que são definidos no arquivo XML do Blueprint quando o pacote configurável é iniciado. A manipulação para o contêiner quando o pacote configurável é interrompido.

O que Fazer Depois

Para obter informações adicionais sobre como configurar os servidores de contêineres do eXtreme Scale com XML do Blueprint e iniciar servidores de contêineres da estrutura OSGi, consulte “Iniciando Servidores do eXtreme Scale Usando a Estrutura do Eclipse Equinox OSGi” na página 181.

Iniciando Servidores Seguros no WebSphere Application Server

Para iniciar servidores seguros no WebSphere Application Server, você deve especificar os arquivos de configuração de segurança nos argumentos genéricos da Java virtual machine (JVM).

Procedimento

- Associe os servidores de catálogos do WebSphere eXtreme Scale aos WebSphere Application Servers usando o console administrativo. No console administrativo, clique em **Administração do Sistema** > **WebSphere eXtreme Scale** > **Domínios do serviço de catálogo**.
- Associe os servidores de contêineres do WebSphere eXtreme Scale aos WebSphere Application Servers específicos implementando um arquivo archive corporativo (EAR) que contém os descritores XML necessários para a grade de dados. Para obter informações adicionais sobre esse procedimento, consulte “Tutorial: Integrar a Segurança do WebSphere eXtreme Scale com o WebSphere Application Server” na página 47.
- Especifique os argumentos da Java virtual machine (JVM) que aponta para arquivos de configuração para tornar os servidores de catálogos e de contêineres seguros. Para obter informações adicionais sobre esse procedimento. consulte Autenticando Solicitações de Clientes no WebSphere Application Server e “Autorizando Acesso à Grade de Dados no WebSphere Application Server” na página 145. Além disso, especifique `securityEnabled="true"` no arquivo `objectgrid xml` para cada grade de dados. Após especificar os argumentos JVM e ativar segurança em suas grades de dados, é possível iniciar os servidores ou clusters que agem como servidores de catálogos ou servidores de contêineres do eXtreme Scale.
- Inicie os servidores de catálogos e de contêineres com o console administrativo do WebSphere Application Server ou use a linha de comandos do WebSphere Application Server.

O que Fazer Depois

“Parando Servidores Seguros”

Parando Servidores Seguros

Parar servidores de catálogos ou servidores de contêiner seguros requer um arquivo de configuração de segurança.

Procedimento

- Pare um servidor de catálogos ou um servidor de contêiner seguro nas implementações independentes. Em ambientes independentes, pare os servidores de catálogos e de contêineres do WebSphere eXtreme Scale usando a função teardown do comando **xscmd** ou usando os comandos **stopXsServer** ou **stopOgServer**.

  Restrinja acesso a essas operações aos administradores autorizados somente, conforme descrito na seção “Autorizando Acesso para Operações Administrativas em Ambientes Independentes” na página 146. Quando autenticação ou SSL é usado, os comandos **stopXsServer** e **stopOgServer**

requerem que um arquivo de propriedades do cliente seja passado como um parâmetro. O conteúdo do arquivo de propriedades do cliente está descrito em "Autenticando Solicitações de Clientes em Ambientes Independentes" na página 135 e "Protegendo Dados que Fluem entre Servidores eXtreme Scale em Ambientes Independentes com Criptografia SSL" na página 149.

- Use o console administrativo do WebSphere Application Server para parar o servidor do eXtreme Scale executado com o WebSphere Application Server. A segurança administrativa do WebSphere Application Server deve estar configurada para restringir acesso para iniciar e parar servidores a administradores autorizados, conforme descrito em "Autorizando Acesso para Operações Administrativas no WebSphere Application Server" na página 149.

Cenário: Usando um Ambiente OSGi para Desenvolver e Executar Plug-ins do eXtreme Scale

Use estes cenários para concluir tarefas comuns em um ambiente OSGi. Por exemplo, a estrutura do OSGi é ideal para iniciar os servidores e clientes em um contêiner OSGi, que permite incluir e atualizar dinamicamente plug-ins do WebSphere eXtreme Scale para o ambiente de tempo de execução.

Antes de Iniciar

Leia o tópico "Visão Geral da Estrutura do OSGi" para aprender mais sobre o suporte de OSGi e os benefícios que ele pode oferecer.

Sobre Esta Tarefa

Os cenários a seguir são sobre construir e executar dinamicamente os plug-ins, que permite instalar, iniciar, parar, modificar e desinstalar os plug-ins de modo dinâmico. Você também pode concluir um outro cenário provável, que permite usar a estrutura do OSGi sem os recursos dinâmicos. Também é possível incluir os aplicativos em pacotes configuráveis, que são definidos e comunicados por meio de serviços. Esses pacotes configuráveis baseados em serviço oferecem vários benefícios, incluindo capacidades de desenvolvimento e de implementação mais eficientes.

Objetivos do Cenário

Depois de concluir esse cenário, você saberá como concluir os objetivos:

- Construa plug-ins dinâmicos do eXtreme Scale para uso em um ambiente OSGi.
- Execute os contêineres do eXtreme Scale em um ambiente OSGi sem os recursos dinâmicos.

Visão Geral da Estrutura do OSGi

O OSGi define um sistema módulo dinâmico para Java. A plataforma de serviço OSGi possui uma arquitetura em camadas e é projetada para ser executada em vários perfis padrão Java. É possível iniciar servidores e clientes do WebSphere eXtreme Scale em um contêiner OSGi.

Benefícios de Executar Aplicativos no Contêiner OSGi

O suporte do WebSphere eXtreme Scale OSGi permite implementar o produto na estrutura do Eclipse Equinox OSGi. Anteriormente, se você desejava atualizar os plug-ins usados pelo eXtreme Scale, era necessário reiniciar a Java Virtual Machine

(JVM) para aplicar as novas versões dos plug-ins. Com a capacidade de atualização dinâmica que a estrutura OSGi fornece, agora é possível atualizar as classes de plug-in sem reiniciar a JVM. Esses plug-ins são exportados pelos pacotes configuráveis do usuário como serviços. O WebSphere eXtreme Scale acessa o serviço ou serviços consultando-os no registro OSGi.

Os contêineres do eXtreme Scale podem ser configurados para iniciar mais fácil e dinamicamente usando o serviço administrativo de configuração do OSGi ou com o OSGi Blueprint. Se desejar implementar uma nova grade de dados com sua estratégia de posicionamento, será possível fazer isso criando uma configuração de OSGi ou implementando um pacote configurável com arquivos XML do descritor eXtreme Scale. Com o suporte do OSGi, os pacotes configuráveis de aplicativo que contém dados de configuração do eXtreme Scale podem ser instalados, iniciados, interrompidos, atualizados e desinstalados sem reiniciar o sistema inteiro. Com esta capacidade, é possível fazer upgrade do aplicativo sem interromper a grade de dados.

Beans de plug-in e serviços podem ser configurados com escopos de shard customizados, permitindo opções de integração sofisticadas com outros serviços em execução na grade de dados. Cada plug-in pode usar classificações do OSGi Blueprint para verificar se cada instância do plug-in ativada está na versão correta. Um bean gerenciado por OSGi (MBean) e o utilitário **xscmd** são fornecidos, o que permite que você consulte os serviços OSGi de plug-in do eXtreme Scale e suas classificações.

Este recurso permite que os administradores reconheçam rapidamente erros de configuração e administração em potencial e atualize as classificações de serviço de plug-in em uso pelo eXtreme Scale.

Pacotes Configuráveis OSGi

Para interagir com, e implementar, plug-ins na estrutura do OSGi, você deve usar os *pacotes configuráveis*. Na plataforma de serviço OSGi, um pacote configurável é um arquivo Java archive (JAR) que contém código Java, recursos e um manifesto que descrevem o pacote configurável e suas dependências. O pacote configurável é a unidade de implementação para um aplicativo. O produto eXtreme Scale suporta os seguintes tipos de pacotes configuráveis:

Pacote configurável do servidor
O pacote configurável do servidor é o arquivo `objectgrid.jar` e é instalado com a instalação do servidor independente do eXtreme Scale e é necessário para executar servidores do eXtreme Scale e também pode ser usado para executar clientes do eXtreme Scale ou caches na memória locais. O ID do pacote configurável para o arquivo `objectgrid.jar` é com.ibm.websphere.xs.server_`<version>`, em que a versão está no formato: `<Version>.<Release>.<Modification>`. Por exemplo, o pacote configurável do servidor para o eXtreme Scale versão 7.1.1 é com.ibm.websphere.xs.server_7.1.1.

Pacote configurável do cliente
O pacote configurável do cliente é o arquivo `ogclient.jar` e é instalado com instalações independentes e do cliente do eXtreme Scale e é usado para executar os clientes do eXtreme Scale ou caches na memória locais. O ID do pacote configurável para o arquivo `ogclient.jar` é com.ibm.websphere.xs.client_`version`, em que a versão está no formato:

`<Version>.<Release>.<Modification>`. Por exemplo, o pacote configurável do cliente para o eXtreme Scale versão 7.1.1 é com.ibm.websphere.xs.client_7.1.1.

Limitações

Não é possível reiniciar o pacote configurável do eXtreme Scale porque você não pode reiniciar o object request broker (ORB) ou o eXtremeIO (XIO). Para reiniciar o servidor do eXtreme Scale, você deve reiniciar a estrutura do OSGi.

Tarefas relacionadas:

"Instalando a Estrutura do Eclipse Equinox OSGi com o Eclipse Gemini para Clientes e Servidores"
Se desejar implementar o WebSphere eXtreme Scale na estrutura do OSGi, você deverá configurar o Ambiente do Eclipse Equinox.

"Gerenciando Ciclos de Vida de Plug-in" na página 548
É possível gerenciar ciclos de vida de plug-in com métodos especializados de cada plug-in, que estão disponíveis para serem chamados em pontos funcionais designados. Ambos os métodos initialize e destroy definem o ciclo de vida de plug-ins, que são controlados pelos seus objetos *proprietário*. Um objeto proprietário é o objeto que realmente usa o plug-in fornecido. Um proprietário pode ser um cliente de grade, um servidor ou um mapa de apoio.

Referências relacionadas:

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Informações relacionadas:

"Introdução: Iniciando e Configurando o Servidor e o Contêiner do eXtreme Scale para Executar Plug-ins na Estrutura do OSGi" na página 97
Neste tutorial, inicie um servidor eXtreme Scale na estrutura do OSGi, inicie um contêiner do eXtreme Scale e ligue os plug-ins de amostra com o ambiente de tempo de execução do eXtreme Scale.

Documentação da API

Instalando a Estrutura do Eclipse Equinox OSGi com o Eclipse Gemini para Clientes e Servidores

Java

Se desejar implementar o WebSphere eXtreme Scale na estrutura do OSGi, você deverá configurar o Ambiente do Eclipse Equinox.

Sobre Esta Tarefa

A tarefa requer fazer o download e instalar a estrutura do blueprint, que permite configurar posteriormente o JavaBeans e expô-los como serviços. O uso de serviços é importante porque é possível expor plug-ins como serviços OSGi, de modo que eles possam ser usados pelo ambiente de tempo de execução do eXtreme Scale. O produto suporta dois contêineres blueprint dentro da estrutura OSGi principal do Eclipse Equinox: Eclipse Gemini e Aries Apache. Use este procedimento para configurar o contêiner do Eclipse Gemini.

Procedimento

1. Faça download do Eclipse Equinox SDK Versão 3.6.1 ou posterior a partir do website do Eclipse. Crie um diretório para a estrutura do Equinox, por exemplo: `/opt/equinox`. Essas instruções referenciam esse diretório como `equinox_root`. Extraia o arquivo compactado no diretório `equinox_root`.
2. Faça download do arquivo compactado gemini-blueprint incubation 1.0.0 a partir do Website Eclipse. Extraia o conteúdo do arquivo em um diretório temporário e copie os seguintes arquivos extraídos para o diretório `equinox_root/plugins`:

   ```
   dist/gemini-blueprint-core-1.0.0.jar
   dist/gemini-blueprint-extender-1.0.0.jar
   dist/gemini-blueprint-io-1.0.0.jar
   ```

   Atenção: Dependendo do local em que você fizer o download do arquivo Blueprint compactado, os arquivos extraídos podem ter a extensão, `RELEASE.jar`, mais como os arquivos JAR da estrutura Spring na próxima etapa. Você deve verificar se os nomes do arquivo correspondem às referências de arquivo no arquivo `config.ini`.
3. Faça download do Spring Framework Versão 3.0.5 a partir da página da web SpringSource a seguir: http://www.springsource.com/download/community. Extraia-o em um diretório temporário e copie os seguintes arquivos extraídos para o diretório `equinox_root/plugins`:

   ```
   org.springframework.aop-3.0.5.RELEASE.jar
   org.springframework.asm-3.0.5.RELEASE.jar
   org.springframework.beans-3.0.5.RELEASE.jar
   org.springframework.context-3.0.5.RELEASE.jar
   org.springframework.core-3.0.5.RELEASE.jar
   org.springframework.expression-3.0.5.RELEASE.jar
   ```
4. Faça download do arquivo Java archive (JAR) AOP Alliance a partir da página da web do SpringSource. Copie o arquivo com.springsource.org.aopalliance-1.0.0.jar para o diretório `equinox_root/plugins` .
5. Faça download do arquivo JAR Apache Commons Logging 1.1.1 a partir da página da web do SpringSource. Copie o arquivo `com.springsource.org.apache.commons.logging-1.1.1.jar` para o diretório `equinox_root/plugins`.
6. Faça download do cliente de linha de comandos Luminis OSGi Configuration Admin. Use esse pacote configurável de arquivo JAR para gerenciar as configurações administrativas do OSGi. Copie o arquivo `net.luminis.cmc-0.2.5.jar` para o diretório `equinox_root/plugins`.
7. Faça download do pacote configurável do arquivo de instalação Apache Felix Versão 3.0.2 a partir da seguinte página da web: http://felix.apache.org/site/index.html. Copie o arquivo `org.apache.felix.fileinstall-3.0.2.jar` para o diretório `equinox_root/plugins`.
8. Crie um diretório de configuração dentro do diretório `equinox_root/plugins`, por exemplo:

   ```
   mkdir equinox_root/plugins/configuration
   ```
9. Crie o arquivo `config.ini` a seguir no diretório `equinox_root/plugins/configuration`, substituindo *equinox_root* com o caminho absoluto para seu diretório `equinox_root` e removendo todos os espaços à direita após a barra invertida em cada linha. Você deve incluir uma linha em branco no final do arquivo; por exemplo:

   ```
   osgi.noShutdown=true
   osgi.java.profile.bootdelegation=none
   org.osgi.framework.bootdelegation=none
   eclipse.ignoreApp=true
   osgi.bundles=\
   ```

```
org.eclipse.osgi.services_3.2.100.v20100503.jar@1:start, \
org.eclipse.osgi.util_3.2.100.v20100503.jar@1:start, \
org.eclipse.equinox.cm_1.0.200.v20100520.jar@1:start, \
com.springsource.org.apache.commons.logging-1.1.1.jar@1:start, \
com.springsource.org.aopalliance-1.0.0.jar@1:start, \
org.springframework.aop-3.0.5.RELEASE.jar@1:start, \
org.springframework.asm-3.0.5.RELEASE.jar@1:start, \
org.springframework.beans-3.0.5.RELEASE.jar@1:start, \
org.springframework.context-3.0.5.RELEASE.jar@1:start, \
org.springframework.core-3.0.5.RELEASE.jar@1:start, \
org.springframework.expression-3.0.5.RELEASE.jar@1:start, \
org.apache.felix.fileinstall-3.0.2.jar@1:start, \
net.luminis.cmc-0.2.5.jar@1:start, \
gemini-blueprint-core-1.0.0.jar@1:start, \
gemini-blueprint-extender-1.0.0.jar@1:start, \
gemini-blueprint-io-1.0.0.jar@1:start
```

Se já tiver configurado o ambiente, será possível limpar o repositório de plug-in do Equinox ao remover o seguinte diretório: `equinox_root\plugins\configuration\org.eclipse.osgi`.

10. Execute os seguintes comandos para iniciar o console do equinox.

    Se você estiver executando uma versão diferente do Equinox, o nome do seu arquivo JAR será diferente do nome no exemplo a seguir:

    ```
    java -jar plugins\org.eclipse.osgi_3.6.1.R36x_v20100806.jar -console
    ```

Conceitos relacionados:

"Visão Geral da Estrutura do OSGi" na página 162
O OSGi define um sistema módulo dinâmico para Java. A plataforma de serviço OSGi possui uma arquitetura em camadas e é projetada para ser executada em vários perfis padrão Java. É possível iniciar servidores e clientes do WebSphere eXtreme Scale em um contêiner OSGi.

Referências relacionadas:

Arquivo de Propriedades do Servidor
O arquivo de propriedades do servidor contém várias propriedades que definem configurações diferentes para o servidor, como configurações de rastreio, criação de log e configuração de segurança. O arquivo de propriedades do servidor é usado pelo serviço de catálogo e pelos servidores de contêiner em servidores independentes e também em servidores hospedados no WebSphere Application Server.

Informações relacionadas:

"Introdução: Iniciando e Configurando o Servidor e o Contêiner do eXtreme Scale para Executar Plug-ins na Estrutura do OSGi" na página 97
Neste tutorial, inicie um servidor eXtreme Scale na estrutura do OSGi, inicie um contêiner do eXtreme Scale e ligue os plug-ins de amostra com o ambiente de tempo de execução do eXtreme Scale.

Instalando Pacotes Configuráveis do eXtreme Scale

Java

O WebSphere eXtreme Scale inclui pacotes configuráveis que podem ser instalados em uma estrutura do Eclipse Equinox OSGi. Esses pacotes configuráveis são necessários para iniciar os servidores do eXtreme Scale ou usar os clientes do eXtreme Scale no OSGi. É possível instalar os pacotes configuráveis do eXtreme Scale usando o console Equinox ou usando o arquivo de configuração config.ini.

Antes de Iniciar

Essa tarefa assume que os produtos a seguir foram instalados:

- Estrutura do Eclipse Equinox OSGi
- Cliente ou servidor independente do eXtreme Scale

Sobre Esta Tarefa

O eXtreme Scale inclui dois pacotes configuráveis. Apenas um dos pacotes configuráveis a seguir é requerido em uma estrutura do OSGi:

objectgrid.jar
O pacote configurável do servidor é o arquivo `objectgrid.jar` e é instalado com a instalação do servidor independente do eXtreme Scale e é requerido para executar servidores do eXtreme Scale e também pode ser usado para executar clientes do eXtreme Scale ou caches na memória locais. O ID do pacote configurável para o arquivo `objectgrid.jar` é com.ibm.websphere.xs.server_<version>, em que a versão está no formato: <Version>.<Release>.<Modification>. Por exemplo, o pacote configurável do servidor para esta liberação é `com.ibm.websphere.xs.server_8.5.0.`

ogclient.jar
O pacote configurável do `ogclient.jar` é instalado com as instalações independentes e de cliente do eXtreme Scale e é usado para executar clientes do eXtreme Scale ou caches na memória locais. O ID do pacote configurável para o arquivo `ogclient.jar` é com.ibm.websphere.xs.client_<version>, em que a versão está no formato: <Version>_<Release>_<Modification. Por exemplo, o pacote configurável do cliente para esta liberação é `com.ibm.websphere.xs.server_8.5.0`.

Para obter mais informações sobre como desenvolver plug-ins do eXtreme Scale, consulte o tópico APIs e Plug-ins do Sistema.

Instale o pacote configurável do cliente ou servidor do eXtreme Scale na estrutura do Eclipse Equinox OSGi usando o console do Equinox: Procedimento

1. Inicie a estrutura do Eclipse Equinox com o console ativado; por exemplo:
   ```
   java_home/bin/java -jar <equinox_root>/plugins/
   org.eclipse.osgi_3.6.1.R36x_v20100806.jar -console
   ```
2. Instale o pacote configurável do cliente ou servidor do eXtreme Scale no console do Equinox:
   ```
   osgi> install file:///<path to bundle>
   ```
3. O Equinox exibe o ID do pacote configurável para o pacote configurável recém-instalado:
   ```
   Bundle id is 25
   ```
4. Inicie o pacote configurável no console do Equinox, em que <id> é o ID do pacote configurável designado quando o pacote configurável foi instalado:
   ```
   osgi> start <id>
   ```
5. Recupere o status de serviço no console do Equinox para verificar se o pacote configurável foi iniciado; por exemplo:
   ```
   osgi> ss
   ```

   Quando o pacote configurável é iniciado com êxito, o pacote configurável exibe o estado ATIVO; por exemplo:
   ```
   25      ACTIVE      com.ibm.websphere.xs.server_8.5.0
   ```

Instale o pacote configurável do cliente ou servidor do eXtreme Scale na estrutura do Eclipse Equinox OSGi usando o arquivo `config.ini`:

Procedimento

1. Copie o pacote configurável do cliente ou servidor do eXtreme Scale (objectgrid.jar ou ogclient.jar) do <wxs_install_root>/ObjectGrid/lib para o diretório de plug-ins do Eclipse Equinox; por exemplo: <equinox_root>/plugins
2. Edite o arquivo de configuração config.ini do Eclipse Equinox e inclua o pacote configurável na propriedade osgi.bundles; por exemplo:

   ```
   osgi.bundles=\
   org.eclipse.osgi.services_3.2.100.v20100503.jar@1:start, \
   org.eclipse.osgi.util_3.2.100.v20100503.jar@1:start, \
   org.eclipse.equinox.cm_1.0.200.v20100520.jar@1:start, \
   objectgrid.jar@1:start
   ```

   Importante: Verifique se existe uma linha em branco após o nome do último pacote configurável. Cada pacote configurável é separado por uma vírgula.
3. Inicie a estrutura do Eclipse Equinox com o console ativado; por exemplo:

   ```
   java_home/bin/java -jar <equinox_root>/plugins/
   org.eclipse.osgi_3.6.1.R36x_v20100806.jar -console
   ```
4. Recupere o status do serviço no console do Equinox para verificar se o pacote configurável foi iniciado:

   ```
   osgi> ss
   ```

   Quando o pacote configurável é iniciado com êxito, o pacote configurável exibe o estado ATIVO; por exemplo:

   ```
   25      ACTIVE      com.ibm.websphere.xs.server_8.5.0
   ```

Resultados

O pacote configurável do servidor ou cliente do eXtreme Scale é instalado e iniciado em sua estrutura do Eclipse Equinox OSGi.

Executando os Contêineres do eXtreme Scale com Plug-ins Não Dinâmicos em um Ambiente do OSGi

Se você não precisar usar o recurso dinâmico de um ambiente de OSGi, será possível ainda aproveitar o acoplamento mais fechado, o empacotamento declarativo e as dependências de serviço que a estrutura de OSGi oferece.

Antes de Iniciar

1. Desenvolva seu aplicativo usando as APIs e plug-ins do WebSphere eXtreme Scale.
2. Crie o pacote do aplicativo em um ou mais pacotes configuráveis do OSGi com as dependências de importação ou exportação apropriadas que são declaradas em um ou mais manifestos do pacote configurável. Assegure-se de que todas as classes ou pacotes que são necessários para os plug-ins, agentes, objetos de dados e assim por diante, sejam exportados.

Sobre Esta Tarefa

Com os plug-ins dinâmicos, é possível atualizar seus plug-ins sem parar a grade. Para usar este recurso, os plug-ins originais e novos devem ser compatíveis. Se você não precisar atualizar os plug-ins ou puder parar a grade para atualizá-los, talvez não seja necessária a complexidade dos plug-ins dinâmicos. Entretanto, ainda há boas razões para executar seu aplicativo eXtreme Scale em um ambiente OSGi. Essas razões incluem acoplamento mais compacto, pacote declarativo, dependências de serviço e assim por diante.

Uma preocupação ao hospedar a grade ou o cliente em um ambiente OSGi sem usar plug-ins dinâmicos (mais especificamente sem declarar os plug-ins usando serviços OSGi) é como o pacote configurável do eXtreme Scale carrega as classes de plug-in. O pacote configurável do eXtreme Scale conta com os serviços OSGi para carregar as classes de plug-in, o que permite que o pacote configurável chame os métodos de objeto nas classes em outros pacotes configuráveis sem importar diretamente os pacotes dessas classes.

Quando os plug-ins não ficam disponíveis pelos serviços OSGi, o pacote configurável do eXtreme Scale deve ser capaz de carregar as classes de plug-in diretamente. Em vez de modificar o manifesto do pacote configurável do eXtreme Scale para importar as classes de usuário e pacotes, crie um fragmento de pacote configurável que inclua as importações necessárias do pacote. O fragmento também pode importar as classes necessárias para outras classes de usuário não plug-in, como objetos de dados e classes de agente.

Procedimento

1. Crie um fragmento de OSGi que usa o pacote configurável do eXtreme Scale (cliente ou servidor, dependendo do ambiente de implementação desejado) como seu host. O fragmento declara dependências (Import-Package) em todos os pacotes que um ou mais plug-ins devem carregar. Por exemplo, se você estiver instalando um plug-in serializador cujas classes residem no pacote `com.mycompany.myapp.serializers` e que dependa das classes no pacote `com.mycompany.myapp.common`, seu arquivo META-INF/MANIFEST.MF de fragmento será parecido com exemplo a seguir:

   ```
   Bundle-ManifestVersion: 2
   Bundle-Name: Plug-in fragment for XS serializers
   Bundle-SymbolicName: com.mycompany.myapp.myfragment; singleton:=true
   Bundle-Version: 1.0.0
   Fragment-Host: com.ibm.websphere.xs.server; bundle-version=7.1.1
   Manifest-Version: 1.0
   Import-Package: com.mycompany.myapp.serializers,
    com.mycompany.myapp.common
   ...
   ```

   Este manifesto deve ser empacotado em um arquivo JAR de fragmento, o que neste exemplo é `com.mycompany.myapp.myfragment_1.0.0.jar`.
2. Implemente o fragmento recentemente criado, o pacote configurável do eXtreme Scale e os pacotes configuráveis do aplicativo em seu ambiente OSGi. Agora, inicie os pacotes configuráveis.

Resultados

É possível agora testar e executar seu aplicativo no ambiente OSGi sem usar os serviços OSGi para carregar as classes de usuário, como plug-ins e agentes.

Conceitos relacionados:

"Visão Geral dos Plug-ins Java" na página 324
Um plug-in do WebSphere eXtreme Scale é um componente que fornece um certo tipo de função para os componentes conectáveis que incluem ObjectGrid e BackingMap. O WebSphere eXtreme Scale fornece vários pontos de conexão para permitir que os aplicativos e provedores de cache se integrem com vários armazéns de dados, APIs de cliente alternativo e para melhorar o desempenho geral do cache. O produto é fornecido com vários plug-ins padrão pré-construídos, mas também é possível criar plug-ins customizados com o aplicativo.

Administrando os Servidores e Aplicativos do eXtreme Scale em um ambiente do OSGi

Use esse tópico para instalar o pacote configurável do servidor WebSphere eXtreme Scale, um fragmento opcional que permite o carregamento de pacotes configuráveis do aplicativo e classes não dinâmicas do usuário, como plug-ins, agentes, objetos de dados e assim por diante.

Antes de Iniciar

1. Instale e inicie uma estrutura de OSGi suportada. Atualmente, o Equinox é a única implementação de OSGi suportada. Se o aplicativo usar o Blueprint, certifique-se de instalar e iniciar uma implementação de Blueprint suportada. Apache Aries e Eclipse Gemini são suportados.
2. Abra o console do OSGi.

Procedimento

1. Instale o pacote configurável do servidor eXtreme Scale. Você deve conhecer a URL do arquivo do pacote configurável Java archive (JAR) file. Por exemplo:

   ```
   osgi> install file:///home/user1/myOsgiEnv/plugins/objectgrid.jar
   Bundle id is 41

   osgi>
   ```

   O pacote configurável do eXtreme Scale está agora instalado, mas ainda não está resolvido.
2. Se o servidor eXtreme Scale tiver que carregar as classes de usuário diretamente, em vez de usar os plug-ins dinâmicos expostos via serviços OSGi, você deverá também instalar um fragmento desenvolvido pelo usuário que fornece essas classes ou as importa. Se você estiver usando plug-ins dinâmicos e não estiver usando agentes, esta etapa poderá ser ignorada. Eis um exemplo de como instalar um fragmento customizado:

   ```
   osgi> install file:///home/user1/myOsgiEnv/plugins/myFragment.jar
   Bundle id is 42

   osgi> ss

   Framework is launched.

   id State       Bundle
   ...
   41 INSTALLED   com.ibm.websphere.xs.server_7.1.1
   42 INSTALLED   com.mycompany.myfragment_1.0.0

   osgi>
   ```

   Agora o pacote configurável do servidor do eXtreme Scale e o fragmento customizado que se conecta ao pacote configurável estão instalados.

3. Inicie o pacote configurável do servidor do eXtreme Scale, por exemplo:

```
osgi> start 41

osgi> ss

Framework is launched.

id State       Bundle
...
41 ACTIVE      com.ibm.websphere.xs.server_7.1.1
               Fragments=42
42 RESOLVED    com.mycompany.myfragment_1.0.0
               Master=41

osgi>
```

4. Agora instale e inicie todos os pacotes configuráveis do aplicativo de usuário usando os mesmos comandos anteriormente mencionados. Para iniciar uma grade neste servidor, a definição do servidor e do contêiner deve ser declarada com o uso do Blueprint ou o aplicativo deve iniciar o servidor e o contêiner de forma programática a partir de um ativador de pacote configurável ou algum outro mecanismo.

Resultados

O pacote configurável do servidor do eXtreme Scale e o aplicativo estão implementados, iniciados e prontos para aceitar trabalho.

Construindo e Executando Plug-ins Dinâmicos do eXtreme Scale para Uso em um Ambiente OSGi

Todos os plug-ins do eXtreme Scale podem ser configurados para um ambiente OSGi. O benefício principal dos plug-ins dinâmicos é que o upgrade deles pode ser feito sem encerrar a grade. Isso permite desenvolver um aplicativo sem reiniciar os processos do contêiner de grade.

Sobre Esta Tarefa

O suporte do WebSphere eXtreme Scale OSGi permite implementar o produto em uma estrutura OSGi, como o Eclipse Equinox. Anteriormente, se você desejava atualizar os plug-ins usados pelo eXtreme Scale, era necessário reiniciar a Java Virtual Machine (JVM) para aplicar as novas versões dos plug-ins. Com o suporte de plug-in dinâmico fornecido pelo eXtreme Scale e a possibilidade de atualizar pacotes configuráveis que a estrutura do OSGi fornece, agora é possível atualizar as classes de plug-in sem reiniciar a JVM. Esses plug-ins são exportados pelo *pacotes configuráveis* como serviços. O WebSphere eXtreme Scale acessa o serviço ao consultar o registro do OSGi. Na plataforma de serviço OSGi, um pacote configurável é um arquivo Java archive (JAR) que contém código Java, recursos e um manifesto que descrevem o pacote configurável e suas dependências. O pacote configurável é a unidade de implementação para um aplicativo.

Procedimento

1. Construa plug-ins dinâmicos do eXtreme Scale.
2. Configure plug-ins do eXtreme Scale with OSGi Blueprint.
3. Instale e inicie plug-ins ativados por OSGi.

Construindo Plug-ins Dinâmicos do eXtreme Scale

Java

O WebSphere eXtreme Scale inclui plug-ins ObjectGrid e BackingMap. Estes plug-ins são implementados em Java e são configurados usando o arquivo XML do descritor do ObjectGrid. Para criar um plug-in dinâmico que pode ser dinamicamente atualizado, eles precisam estar cientes dos eventos de ciclo de vida de ObjectGrid e BackingMap porque eles podem precisar concluir algumas ações durante uma atualização. Aprimorar um pacote configurável de plug-in com métodos de retorno de chamada, listeners de eventos, ou ambos, do ciclo de vida permite que o plug-in conclua essas ações em momentos apropriados.

Antes de Iniciar

Este tópico supõe que você construiu o plug-in apropriado. Para obter informações adicionais sobre como desenvolver plug-ins do eXtreme Scale, consulte o tópico APIs e Plug-ins do Sistema.

Sobre Esta Tarefa

Todos os plug-ins do eXtreme Scale se aplicam a uma instância de BackingMap ou de ObjectGrid. Muitos plug-ins também interagem com outros plug-ins. Por exemplo, um plug-in Loader e TransactionCallback trabalham juntos para interagir corretamente com uma transação do banco de dados e as várias chamadas de banco de dados JDBC. Alguns plug-ins também pode precisar armazenar em cache dados de configuração a partir de outros plug-ins para melhorar o desempenho.

Os plug-ins BackingMapLifecycleListener e ObjectGridLifecycleListener fornecem operações de ciclo de vida para as respectivas instâncias de BackingMap e ObjectGrid. Este processo permite que plug-ins sejam notificados quando o BackingMap ou ObjectGrid pai e seus respectivos plug-ins podem ser alterados. Os plug-ins BackingMap implementam a interface de BackingMapLifecyleListener e os plug-ins ObjectGrid implementam a interface de ObjectGridLifecycleListener. Estes plug-ins são chamados automaticamente quando o ciclo de vida do BackingMap ou ObjectGrid pai é alterado. Para obter mais informações sobre os plug-ins de ciclo de vida, consulte o tópico “Gerenciando Ciclos de Vida de Plug-in” na página 548.

É possível aprimorar os pacotes configuráveis usando os métodos ou os listeners de evento do ciclo de vida nas seguintes tarefas comuns:

- Iniciar e parar recursos, como encadeamentos ou assinantes de sistema de mensagens.
- Especificar que uma notificação ocorra quando os plug-ins equivalentes forem atualizados, permitindo o acesso direto ao plug-in e a detecção de quaisquer mudanças.

Sempre que outro plug-in for acessado diretamente, acesse esse plug-in por meio do contêiner OSGi para assegurar que todas as partes do sistema referenciem o plug-in correto. Se, por exemplo, algum componente no aplicativo referenciar diretamente, ou armazenar em cache, uma instância de um plug-in, ele manterá sua referência para essa versão do plug-in, mesmo depois que o plug-in tiver sido atualizado dinamicamente. Esse comportamento pode causar problemas relacionados ao aplicativo, bem como fugas de memória. Portanto, grave o código que depende dos plug-ins dinâmicos que obtêm sua referência usando semânticas getService() do OSGi. Se o aplicativo precisar armazenar em cache um ou mais plug-ins, ele atenderá eventos de ciclo de vida usando interfaces ObjectGridLifecycleListener e BackingMapLifecycleListener. O aplicativo também deve poder atualizar seu cache quando necessário, de modo thread safe.

Todos os plug-ins do eXtreme Scale usados com o OSGi também devem implementar as respectivas interfaces BackingMapPlugin ou ObjectGridPlugin. Novos plug-ins, tal como a interface MapSerializerPlugin impingem essa prática. Essas interfaces fornecem ao ambiente de tempo de execução do eXtreme Scale e ao OSGi uma interface consistente para injeção de estado no plug-in e controle de seu ciclo de vida.

Ao usar esta tarefa para especificar que uma notificação ocorre quando os plug-ins equivalentes são atualizados, é possível criar um factory de listener que produz uma instância do listener.

Procedimento

- Atualize a classe de plug-in ObjectGrid para implementar a interface ObjectGridPlugin. Esta interface inclui métodos que permitem que o eXtreme Scale inicialize, configure a instância do ObjectGrid e destrua o plug-in. Consulte o exemplo de código a seguir:

```
package com.mycompany;
import com.ibm.websphere.objectgrid.plugins.ObjectGridPlugin;
...

public class MyTranCallback implements TransactionCallback, ObjectGridPlugin {

    private ObjectGrid og = null;

    private enum State {
        NEW, INITIALIZED, DESTROYED
    }

    private State state = State.NEW;

    public void setObjectGrid(ObjectGrid grid) {
        this.og = grid;
    }

    public ObjectGrid getObjectGrid() {
        return this.og;
    }
    void initialize() {
        // Handle any plug-in initialization here.  This is called by
        // eXtreme Scale, and not the OSGi bean manager.
        state = State.INITIALIZED;
    }
    boolean isInitialized() {
        return state == State.INITIALIZED;
    }

    public void destroy() {
        // Destroy the plug-in and release any resources.  This
        // can be callsed by the OSGi Bean Manager or by eXtreme Scale.
        state = State.DESTROYED;
    }

    public boolean isDestroyed() {
        return state == State.DESTROYED;
    }
}
```

- Atualize a classe de plug-in do ObjectGrid para implementar a interface ObjectGridLifecycleListener. Consulte o exemplo de código a seguir:

```
package com.mycompany;
import com.ibm.websphere.objectgrid.plugins.ObjectGridLifecycleListener;
      import com.ibm.websphere.objectgrid.plugins.ObjectGridLifecycleListener.LifecycleEvent;
      ...

      public class MyTranCallback implements TransactionCallback, ObjectGridPlugin, ObjectGridLifecycleListener{
          public void objectGridStateChanged(LifecycleEvent event) {
              switch(event.getState()) {
              case NEW:
              case DESTROYED:
              case DESTROYING:
              case INITIALIZING:
                  break;
              case INITIALIZED:
                  // Lookup a Loader or MapSerializerPlugin using
                  // OSGi or directly from the ObjectGrid instance.
                  lookupOtherPlugins()
                  break;
              case STARTING:
              case PRELOAD:
                  break;
              case ONLINE:
```

```
                if (event.isWritable()) {
                    startupProcessingForPrimary();
                } else {
                    startupProcessingForReplica();
                }
                break;
            case QUIESCE:
                if (event.isWritable()) {
                    quiesceProcessingForPrimary();
                } else {
                    quiesceProcessingForReplica();
                }
                break;
            case OFFLINE:
                shutdownShardComponents();
                break;
            }
        }
        ...
    }
```

- Atualize um plug-in do BackingMap. Atualize a classe de plug-in do BackingMap para implementar a interface de plug-in do BackingMap. Esta interface inclui métodos que permitem que o eXtreme Scale inicialize, configure a instância do BackingMap e destrua o plug-in. Consulte o exemplo de código a seguir:

```
package com.mycompany;
import com.ibm.websphere.objectgrid.plugins.BackingMapPlugin;
...

public class MyLoader implements Loader, BackingMapPlugin {

    private BackingMap bmap = null;

    private enum State {
        NEW, INITIALIZED, DESTROYED
    }

    private State state = State.NEW;

    public void setBackingMap(BackingMap map) {
        this.bmap = map;
    }

    public BackingMap getBackingMap() {
        return this.bmap;
    }
    void initialize() {
        // Handle any plug-in initialization here.  This is called by
        // eXtreme Scale, and not the OSGi bean manager.
        state = State.INITIALIZED;
    }
    boolean isInitialized() {
        return state == State.INITIALIZED;
    }

    public void destroy() {
        // Destroy the plug-in and release any resources.  This
        // can be callsed by the OSGi Bean Manager or by eXtreme Scale.
        state = State.DESTROYED;
    }

    public boolean isDestroyed() {
        return state == State.DESTROYED;
    }
}
```

- Atualize a classe de plug-in do BackingMap para implementar a interface BackingMapLifecycleListener. Consulte o exemplo de código a seguir:

```
package com.mycompany;

      import com.ibm.websphere.objectgrid.plugins.BackingMapLifecycleListener;
      import com.ibm.websphere.objectgrid.plugins.BackingMapLifecycleListener.LifecycleEvent;
      ...

      public class MyLoader implements Loader, ObjectGridPlugin, ObjectGridLifecycleListener{
          ...
          public void backingMapStateChanged(LifecycleEvent event) {
              switch(event.getState()) {
              case NEW:
              case DESTROYED:
              case DESTROYING:
              case INITIALIZING:
                  break;
              case INITIALIZED:
                  // Lookup a MapSerializerPlugin using
                  // OSGi or directly from the ObjectGrid instance.
                  lookupOtherPlugins()
                  break;
```

```
            case STARTING:
            case PRELOAD:
                break;
            case ONLINE:
                if (event.isWritable()) {
                    startupProcessingForPrimary();
                } else {
                    startupProcessingForReplica();
                }
                break;
            case QUIESCE:
                if (event.isWritable()) {
                    quiesceProcessingForPrimary();
                } else {
                    quiesceProcessingForReplica();
                }
                break;
            case OFFLINE:
                shutdownShardComponents();
                break;
            }
        }
        ...
    }
```

Resultados

Implementando a interface ObjectGridPlugin ou BackingMapPlugin, o eXtreme Scale pode controlar o ciclo de vida de seu plug-in nos momentos certos.

Implementando a interface ObjectGridLifecycleListener ou BackingMapLifecycleListener, o plug-in é automaticamente registrado como um listener dos eventos de ciclo de vida do ObjectGrid ou do BackingMap associados. O evento INITIALIZING é usado para sinalizar que todos os plug-ins do ObjectGrid e do BackingMap foram inicializados e estão disponíveis para consultar e usar. O evento ONLINE é usado para sinalizar que o ObjectGrid está on-line e pronto para iniciar eventos de processamento.

Configurando os Plug-ins do eXtreme Scale com o OSGi Blueprint

Java

Todos os plug-ins do ObjectGrid e do BackingMap do eXtreme Scale podem ser definidos como beans e serviços OSGi usando o Serviço OSGi Blueprint disponível com o Eclipse Gemini ou o Aries Apache.

Antes de Iniciar

Antes de poder configurar seus plug-ins como serviços OSGi, você deve primeiro empacotar seus plug-ins em um pacote configurável OSGi e entender os princípios fundamentais dos plug-ins necessários. O pacote configurável deve importar os pacotes do cliente ou servidor do WebSphere eXtreme Scale e outros pacotes dependentes requeridos pelos plug-ins ou criar uma dependência do pacote configurável nos pacotes configuráveis do servidor ou cliente doeXtreme Scale. Este tópico descreve como configurar o XML Blueprint para criar beans de plug-in e expô-los como serviços OSGi para o eXtreme Scale usar.

Sobre Esta Tarefa

Beans e serviços são definidos em um arquivo XML do Blueprint e o contêiner do Blueprint descobre, cria e liga os beans juntos e os expõe como serviços. O processo torna os beans disponíveis para outros pacotes configuráveis OSGi, incluindo os pacotes configuráveis de servidor e cliente do eXtreme Scale.

Ao criar serviços de plug-in customizados para uso com o eXtreme Scale, o pacote configurável que deve hospedar os plug-ins deve ser configurado para usar Blueprint. Além disso, um arquivo XML do Blueprint deve ser criado e armazenado dentro do pacote configurável. Leia sobre construção de aplicativos OSGi com a especificação do Contêiner do Blueprint para obter um entendimento geral da especificação.

Procedimento

1. Crie um arquivo XML do Blueprint. É possível nomear o arquivo de qualquer jeito. No entanto, você deve incluir o namespace do projeto:

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <blueprint xmlns="http://www.osgi.org/xmlns/blueprint/v1.0.0">
   ...
   </blueprint>
   ```

2. Crie definições de bean no arquivo XML do Blueprint para cada plug-in do eXtreme Scale.

   Beans são definidos usando o elemento `<bean>` e podem ser ligados a outras referências de bean e podem incluir parâmetros de inicialização.

   Importante: Ao definir um bean, você deve usar o escopo correto. O Blueprint suporta os escopos singleton e de protótipo. O eXtreme Scale também suporta um escopo de shard customizado.

   Defina a maioria dos plug-ins do eXtreme Scale como protótipo ou beans com escopo definido em shard, uma vez que todos os beans devem ser exclusivos para cada shard do ObjectGrid ou instância do BackingMap à qual eles estão associados. Beans com escopo definido em shard podem ser úteis ao usar os beans em outros contextos para permitir a recuperação da instância correta.

   Para definir um bean com escopo definido em protótipo, use o atributo `scope="prototype"` no bean:

   ```
   <bean id="myPluginBean" class="com.mycompany.MyBean" scope="prototype">
   ...
   </bean>
   ```

   Para definir um bean com escopo definido em shard, você deve incluir o namespace `objectgrid` no esquema XML e usar o atributo `scope="objectgrid:shard"` no bean:

   ```
   <?xml version="1.0" encoding="UTF-8"?>

   <blueprint xmlns="http://www.osgi.org/xmlns/blueprint/v1.0.0"
              xmlns:objectgrid="http://www.ibm.com/schema/objectgrid"

       xsi:schemaLocation="http://www.ibm.com/schema/objectgrid
                   http://www.ibm.com/schema/objectgrid/objectgrid.xsd">

       <bean id="myPluginBean" class="com.mycompany.MyBean"
      scope="objectgrid:shard">
       ...
       </bean>

   ...
   ```

3. Crie definições de bean PluginServiceFactory para cada bean de plug-in. Todos os beans do eXtreme Scale devem ter um bean do PluginServiceFactory definido para que o escopo do bean correto possa ser aplicado. O eXtreme Scale inclui um BlueprintServiceFactory que você pode usar. Ele inclui duas propriedades que devem ser configuradas. Você deve configurar a propriedade blueprintContainer com a referência `blueprintContainer` e a propriedade beanId deve ser configurada com o nome do identificador de bean. Quando o

eXtreme Scale consulta o serviço para instanciar os beans apropriados, o servidor procura a instância do componente do bean usando o contêiner Blueprint.

```
bean id="myPluginBeanFactory"
    class="com.ibm.websphere.objectgrid.plugins.osgi.BluePrintServiceFactory">
    <property name="blueprintContainer" ref="blueprintContainer"/>
    <property name="beanId" value="myPluginBean" />
</bean>
```

4. Crie um gerenciador de serviços para cada bean PluginServiceFactory. Cada gerenciador de serviços expõe o bean PluginServiceFactory, usando o elemento `<service>`. O elemento de serviço identifica o nome a ser exposto para o OSGi, a referência para o bean PluginServiceFactory, a interface a ser exposta e a classificação do serviço. O eXtreme Scale usa a classificação do gerenciador de serviços para executar upgrades de serviço quando a grade do eXtreme Scale está ativa. Se a classificação não for especificada, a estrutura do OSGi assumirá uma classificação igual a 0. Leia sobre como atualizar as classificações de serviço para obter mais informações.

   Blueprint inclui várias opções para configurar gerenciadores de serviços. Para definir um gerenciador de serviços simples para um bean PluginServiceFactory, crie um elemento `<service>` para cada bean PluginServiceFactory:

   ```
   <service ref="myPluginBeanFactory"
       interface="com.ibm.websphere.objectgrid.plugins.osgi.PluginServiceFactory"
       ranking="1">
   </service>
   ```

5. Armazene o arquivo XML do Blueprint no pacote configurável de plug-ins. O arquivo XML do Blueprint deve ser armazenado no diretório `OSGI-INF/blueprint` para o contêiner do Blueprint a ser descoberto.

   Para armazenar o arquivo XML do Blueprint em um diretório diferente, você deve especificar o seguinte cabeçalho de manifesto Bundle-Blueprint:

   ```
   Bundle-Blueprint: OSGI-INF/blueprint.xml
   ```

Resultados

Os plug-ins do eXtreme Scale agora são configurados para serem expostos em um contêiner OSGi Blueprint, além disso, o arquivo XML do descritor do ObjectGrid é configurado para referenciar os plug-ins usando o serviço OSGi Blueprint.

Instalando e Iniciando Plug-ins Ativados pelo OSGi

Nesta tarefa, você instala o pacote configurável de plug-in dinâmico na estrutura do OSGi. Em seguida, inicia o plug-in.

Antes de Iniciar

Este tópico assume que as seguintes tarefas foram concluídas:

- O pacote configurável do servidor ou cliente do eXtreme Scale foi instalado na estrutura do Eclipse Equinox OSGi. Consulte “Instalando Pacotes Configuráveis do eXtreme Scale” na página 166.
- Um ou mais plug-ins BackingMap ou ObjectGrid dinâmicos foram implementados. Consulte “Construindo Plug-ins Dinâmicos do eXtreme Scale” na página 171.
- Os plug-ins dinâmicos foram empacotados como serviços OSGi nos pacotes configuráveis OSGi.

Sobre Esta Tarefa

Esta tarefa descreve como instalar o pacote configurável usando o console do Eclipse Equinox. O pacote configurável pode ser instalado usando vários métodos diferentes, incluindo a modificação do arquivo de configuração `config.ini`. Os produtos que incorporam o Eclipse Equinox incluem métodos alternativos para gerenciar pacotes configuráveis. Para obter mais informações sobre como incluir pacotes configuráveis no arquivo `config.ini` no Eclipse Equinox, consulte as opções de tempo de execução do Eclipse.

O OSGi permite que pacotes configuráveis que possuem serviços duplicados sejam iniciados. O WebSphere eXtreme Scale usa a classificação de serviço mais recente. Ao iniciar diversas estruturas OSGi em uma grade de dados do eXtreme Scale, você deve se certificar de que as classificações de serviço corretas sejam iniciados em cada servidor. Não fazer isso faz com que a grade seja iniciada com uma mistura de diferentes versões.

Para ver quais versões estão em uso pela grade de dados, use o utilitário xscmd para verificar as classificações atuais e disponíveis. Para obter mais informações sobre classificações de serviço disponíveis, consulte Atualizando Serviços OSGi para Plug-ins do eXtreme Scale com **xscmd**.

Procedimento

Instale o pacote configurável de plug-in na estrutura do Eclipse Equinox OSGi usando o console do OSGi.

1. Inicie a estrutura do Eclipse Equinox com o console ativado; por exemplo:
   ```
   <java_home>/bin/java -jar <equinox_root>/plugins/org.eclipse.osgi_3.6.1.R36x_v20100806.jar -console
   ```
2. Instale o pacote configurável de plug-in no console do Equinox.
   ```
   osgi> install file:///<path to bundle>
   ```
   O Equinox exibe o ID do pacote configurável para o pacote configurável recém-instalado:
   ```
   Bundle id is 17
   ```
3. Insira a linha a seguir para iniciar o pacote configurável no console do Equinox, em que `<id>` é o ID do pacote configurável designado quando o pacote configurável foi instalado:
   ```
   osgi> start <id>
   ```
4. Recupere o status do serviço no console do Equinox para verificar se o pacote configurável foi iniciado:
   ```
   osgi> ss
   ```
   Quando o pacote configurável foi iniciado com êxito, o pacote configurável exibe o estado ACTIVE; por exemplo:
   ```
   17      ACTIVE      com.mycompany.plugin.bundle_VRM
   ```

Instale o pacote configurável de plug-in na estrutura do Eclipse Equonix OSGi usando o arquivo config.ini.

5. Copie o pacote configurável de plug-in no diretório de plug-ins do Eclipse Equinox; por exemplo:
   ```
   <equinox_root>/plugins
   ```
6. Edite o arquivo de configuração `config.ini` do Eclipse Equinox e inclua o pacote configurável na propriedade osgi.bundles; por exemplo:

```
osgi.bundles=\
org.eclipse.osgi.services_3.2.100.v20100503.jar@1:start, \
org.eclipse.osgi.util_3.2.100.v20100503.jar@1:start, \
org.eclipse.equinox.cm_1.0.200.v20100520.jar@1:start, \
com.mycompany.plugin.bundle_VRM.jar@1:start
```

Importante: Verifique se existe uma linha em branco após o nome do último pacote configurável. Cada pacote configurável é separado por uma vírgula.

7. Inicie a estrutura do Eclipse Equinox com o console ativado; por exemplo:

```
<java_home>/bin/java -jar <equinox_root>/plugins/org.eclipse.osgi_3.6.1.R36x_v20100806.jar -console
```

8. Recupere o status de serviço no console do Equinox para verificar se o pacote configurável foi iniciado; por exemplo:

```
osgi> ss
```

Quando o pacote configurável foi iniciado com êxito, o pacote configurável exibe o estado ACTIVE; por exemplo:

```
17      ACTIVE      com.mycompany.plugin.bundle_VRM
```

Resultados

O pacote configurável de plug-in agora está instalado e iniciado. O contêiner ou cliente do eXtreme Scale agora pode ser iniciado. Para obter mais informações sobre como desenvolver plug-ins do eXtreme Scale, consulte o tópico APIs e Plug-ins do Sistema "APIs e Plug-ins do Sistema" na página 548.

Executando os Contêineres do eXtreme Scale com Plug-ins Dinâmicos em um Ambiente do OSGi

Se seu aplicativo estiver hospedado na estrutura do Eclipse Equinox OSGi com o Eclipse Gemini ou o Apache Aries, será possível usar esta tarefa para ajudá-lo a instalar e configurar seu aplicativo WebSphere eXtreme Scale no OSGi.

Antes de Iniciar

Antes de iniciar esta tarefa, certifique-se de concluir as tarefas a seguir:

- Instale a estrutura do Eclipse Equinox OSGi com o Eclipse Gemini
- Construa e execute plug-ins dinâmicos do eXtreme Scale para usar em um ambiente OSGi

Sobre Esta Tarefa

Com plug-ins dinâmicos, é possível atualizar dinamicamente o plug-in enquanto a grade ainda está ativa. Isso permite atualizar um aplicativo sem reiniciar os processos do contêiner de grade. Para obter informações adicionais sobre como desenvolver plug-ins do eXtreme Scale, consulte APIs e Plug-ins do Sistema.

Procedimento

1. Configure plug-ins ativados por OSGi usando o arquivo XML do descritor do ObjectGrid.
2. Inicie os servidores de contêiner do eXtreme Scale usando a estrutura do Eclipse Equinox OSGi.
3. Administre serviços OSGi para plug-ins do eXtreme Scale com o utilitário xscmd.
4. Configure servidores com o OSGi Blueprint.

Configurando Plug-ins Ativados pelo OSGi Usando o Arquivo Descritor XML do ObjectGrid

Java

Nesta tarefa, você inclui serviços OSGi existentes em um arquivo XML descritor de forma que os contêineres do WebSphere eXtreme Scale possam reconhecer e carregar os plug-ins ativados pelo OSGi corretamente.

Antes de Iniciar

Para configurar seus plug-ins, certifique-se de:

- Criar seu pacote e ativar plug-ins dinâmicos para implementação do OSGi.
- Ter os nomes dos serviços OSGi que representam seus plug-ins disponíveis.

Sobre Esta Tarefa

Você criou um serviço OSGi para agrupar seu plug-in. Agora, esses serviços devem ser definidos no arquivo `objectgrid.xml` de modo que os contêineres do eXtreme Scale possam carregar e configurar o plug-in ou plug-ins com êxito.

Procedimento

1. Quaisquer plug-ins específicos da grade, tal como TransactionCallback, devem ser especificados sob o elemento objectGrid. Consulte o exemplo a seguir a partir do arquivo `objectgrid.xml`:

```
<?xml version="1.0" encoding="UTF-8"?>

<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
    xmlns="http://ibm.com/ws/objectgrid/config">

    <objectGrids>
        <objectGrid name="MyGrid" txTimeout="60">
            <bean id="myTranCallback" osgiService="myTranCallbackFactory"/>
            ...
        </objectGrid>
        ...
    </objectGrids>
    ...
/objectGridConfig>
```

   Importante: O valor de atributo `osgiService` deve corresponder ao valor de atributo `ref` que é especificado no arquivo XML `blueprint`, no qual o serviço foi definido para myTranCallback PluginServiceFactory.

2. Quaisquer plug-ins específicos do mapa, como carregadores ou serializadores, por exemplo, devem ser especificados no elemento backingMapPluginCollections e referenciados a partir do elemento backingMap. Consulte o exemplo a seguir a partir do arquivo `objectgrid.xml`:

```
<?xml version="1.0" encoding="UTF-8"?>

objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
    xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="MyGrid" txTimeout="60">
            <backingMap name="MyMap1" lockStrategy="PESSIMISTIC"
                copyMode="COPY_TO_BYTES" nullValuesSupported="false"
                pluginCollectionRef="myPluginCollectionRef1"/>
            <backingMap name="MyMap2" lockStrategy="PESSIMISTIC"
                copyMode="COPY_TO_BYTES" nullValuesSupported="false"
                pluginCollectionRef="myPluginCollectionRef2"/>
            ...
       </objectGrid>
       ...
```

```
    </objectGrids>
    ...
    <backingMapPluginCollections>
        <backingMapPluginCollection id="myPluginCollectionRef1">
            <bean id="MapSerializerPlugin" osgiService="mySerializerFactory"/>
        </backingMapPluginCollection>
        <backingMapPluginCollection id="myPluginCollectionRef2">
            <bean id="MapSerializerPlugin" osgiService="myOtherSerializerFactory"/>
            <bean id="Loader" osgiService="myLoader"/>
        </backingMapPluginCollection>
        ...
    </backingMapPluginCollections>
    ...
</objectGridConfig>
```

Resultados

O arquivo `objectgrid.xml` neste exemplo informa ao eXtreme Scale para criar uma grade denominada `MyGrid` com dois mapas, `MyMap1` e `MyMap2`. O mapa `MyMap1` usa o serializador agrupado pelo serviço OSGi, mySerializerFactory. O mapa `MyMap2` usa um serializador do serviço OSGi, myOtherSerializerFactory, e um carregador a partir do serviço OSGi, myLoader.

Iniciando Servidores do eXtreme Scale Usando a Estrutura do Eclipse Equinox OSGi

Os servidores de contêiner do WebSphere eXtreme Scale podem ser iniciados em uma estrutura do Eclipse Equinox OSGi usando vários métodos.

Antes de Iniciar

Antes de poder iniciar um contêiner do eXtreme Scale, você deve ter concluído as tarefas a seguir:

1. O pacote configurável do servidor do WebSphere eXtreme Scale deve estar instalado no Eclipse Equinox.
2. Seu aplicativo deve ser empacotado como um pacote configurável OSGi.
3. Seus plug-ins do WebSphere eXtreme Scale (se houver) devem ser empacotados como um pacote configurável OSGi. Eles podem ser empacotados no mesmo pacote configurável que seu aplicativo ou como pacotes configuráveis separados.
4. Se seus servidores de contêiner estiverem usando o IBM eXtremeMemory, você deverá primeiro configurar as bibliotecas nativas. Para obter informações adicionais, consulte Configurando o IBM eXtremeMemory.

Sobre Esta Tarefa

Esta tarefa descreve como iniciar um servidor de contêiner do eXtreme Scale em uma estrutura do Eclipse Equinox OSGi. É possível usar qualquer um dos seguintes métodos para iniciar os servidores de contêiner usando a implementação do Eclipse Equinox:

- Serviço do OSGi Blueprint

  É possível incluir toda a configuração e os metadados em um pacote configurável OSGi. Consulte a imagem a seguir para compreender o processo do Eclipse Equinox para este método:

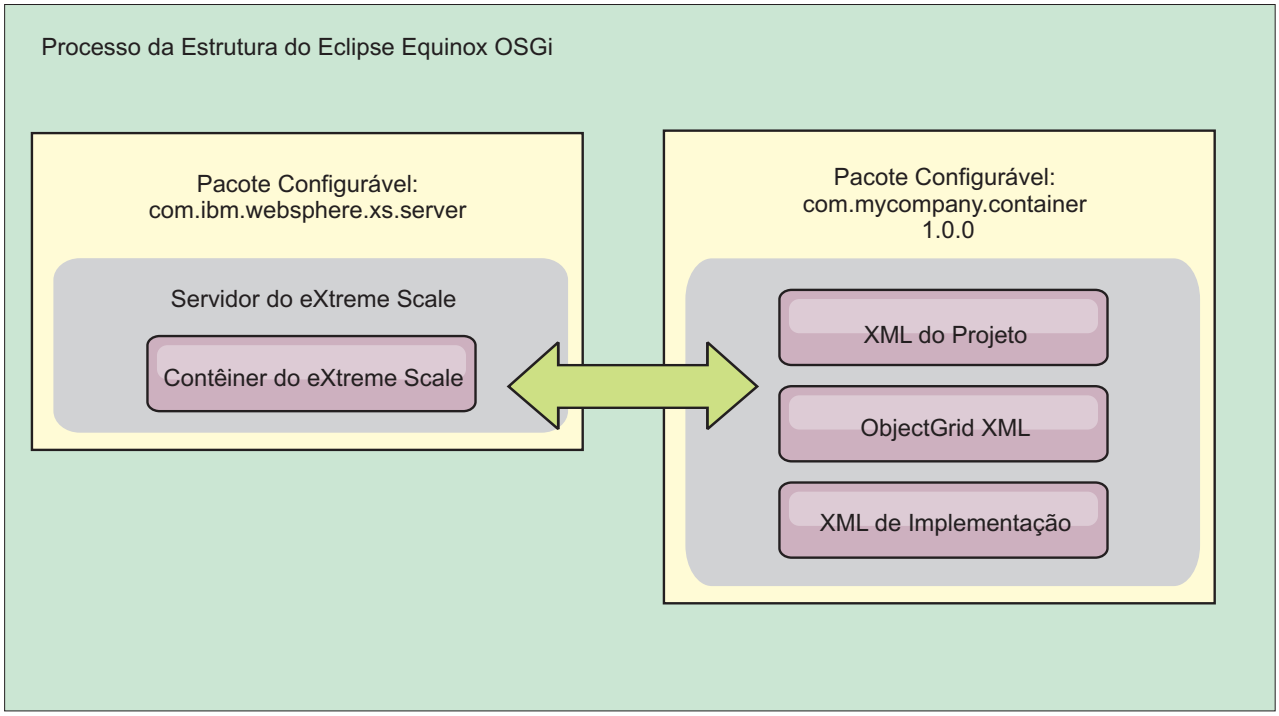


Figura 10. Processo do Eclipse Equinox para Incluir Toda a Configuração e Todos os Metadados em um Pacote Configurável OSGi

- Serviço de Administração de Configuração do OSGi

  É possível especificar a configuração e os metadados fora de um pacote configurável OSGi. Consulte a imagem a seguir para compreender o processo do Eclipse Equinox para este método:

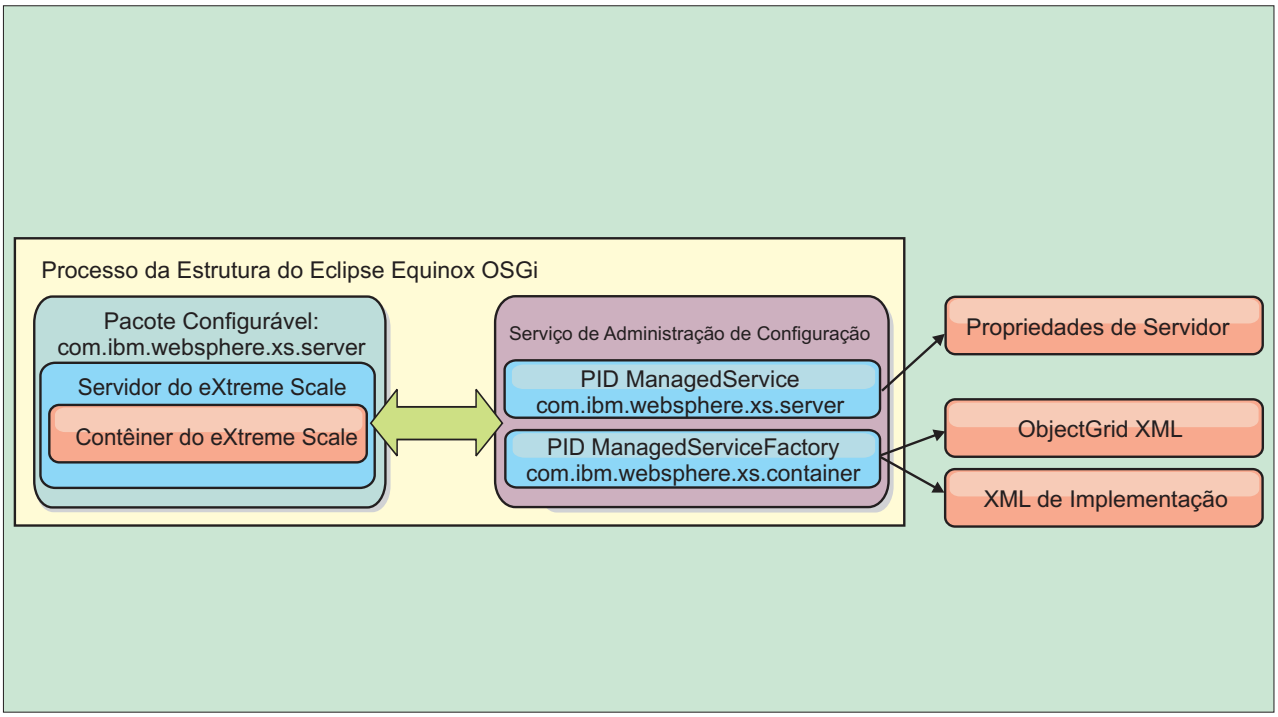


Figura 11. Processo do Eclipse Equinox para Especificar a Configuração e os Metadados Fora de um Pacote Configurável OSGi

- Programaticamente
  Suporta soluções de configuração customizadas.

Em cada caso, um singleton do servidor do eXtreme Scale é configurado e um ou mais contêineres são configurados.

O pacote configurável do servidor do eXtreme Scale, `objectgrid.jar`, inclui todas as bibliotecas necessárias para iniciar e executar um contêiner de grade do eXtreme Scale em uma estrutura OSGi. O ambiente de tempo de execução do servidor se comunica com os plug-ins e objetos de dados fornecidos pelo usuário usando o gerenciador de serviço OSGi.

Importante: Depois de um pacote configurável do servidor do eXtreme Scale ser iniciado e o servidor do eXtreme Scale ser inicializado, ele não poderá ser reiniciado. O processo do Eclipse Equinox deve ser reiniciado para reiniciar um servidor do eXtreme Scale.

É possível usar o suporte do eXtreme Scale para o namespace do Spring para configurar os servidores de contêiner do eXtreme Scale em um arquivo XML do Blueprint. Quando os elemento XML do servidor e do contêiner são incluídos no arquivo XML do Blueprint, o manipulador de namespace do eXtreme Scale inicia automaticamente um servidor de contêiner usando os parâmetros que são definidos no arquivo XML do Blueprint quando o pacote configurável é iniciado. A manipulação para o contêiner quando o pacote configurável é interrompido.

Para configurar servidores de contêiner do eXtreme Scale com o XML do Blueprint, conclua as etapas a seguir:

Procedimento

- Inicie um servidor de contêiner do eXtreme Scale usando o OSGi Blueprint.
  1. Crie um pacote configurável de contêiner.
  2. Instale o pacote configurável de contêiner na estrutura do Eclipse Equinox OSGi. Consulte "Instalando e Iniciando Plug-ins Ativados pelo OSGi" na página 177.
  3. Inicie o pacote configurável do contêiner.
- Inicie uma servidor de contêiner do eXtreme Scale usando a administração de configuração do OSGi.
  1. Configure o servidor e o contêiner usando a administração de configuração.
  2. Quando o pacote configurável do servidor do eXtreme Scale é iniciado ou os identificadores persistentes são criados com config admin, o servidor e o contêiner iniciam automaticamente.
- Inicie um servidor de contêiner do eXtreme Scale usando a API do ServerFactory. Consulte a documentação da API do servidor.
  1. Crie uma classe de ativador do pacote configurável OSGi e use a API do ServerFactory do eXtreme Scale para iniciar um servidor.

Administrando Serviços Ativados pelo OSGi Usando o Utilitário `xscmd`

É possível usar o utilitário **xscmd** para concluir as tarefas de administrador, como visualizar serviços e suas classificações que estão sendo usados por cada contêiner e atualizar o ambiente de tempo de execução para utilizar novas versões dos pacotes configuráveis.

Sobre Esta Tarefa

Com a estrutura do Eclipse Equinox OSGi, é possível instalar diversas versões do mesmo pacote configurável e você pode atualizar esses pacotes configuráveis durante o tempo de execução. O WebSphere eXtreme Scale é um ambiente distribuído que executa os servidores de contêiner em muitas instâncias da estrutura do OSGi.

Os administradores são responsáveis por copiar, instalar e iniciar manualmente pacotes configuráveis na estrutura do OSGi. O eXtreme Scale inclui um ServiceTrackerCustomizer OSGi para controlar quaisquer serviços que foram identificados como plug-ins do eXtreme Scale no arquivo XML do descritor do ObjectGrid. Use o utilitário **xscmd** para validar qual versão do plug-in é usada, quais versões estão disponíveis para serem usadas e para executar upgrades do pacote configurável.

O eXtreme Scale usa o número de classificação do serviço para identificar a versão de cada serviço. Quando dois ou mais serviços são carregados com a mesma referência, o eXtreme Scale usa automaticamente o serviço com a classificação mais alta.

Procedimento

- Execute o comando **osgiCurrent** e verifique se cada servidor eXtreme Scale está usando a classificação do serviço de plug-in correta.

  Como o eXtreme Scale escolhe automaticamente a referência de serviço com a classificação mais alta, é possível que a grade de dados possa iniciar com diversas classificações de um serviço de plug-in.

Se o comando detecta uma incompatibilidade de classificações ou se ele é incapaz de localizar um serviço, um nível de erro diferente de zero é configurado. Se o comando foi concluído com êxito, o nível de erro é configurado como 0.

O exemplo a seguir mostra a saída do comando **osgiCurrent** quando dois plug-ins estão instalados na mesma grade em quatro servidores. O plug-in loaderPlugin está usando classificação de 1 e txCallbackPlugin está usando classificação 2.

```
OSGi Service Name Current Ranking ObjectGrid Name MapSet Name Server Name
----------------- --------------- --------------- ----------- -----------
loaderPlugin      1               MyGrid          MapSetA     server1
loaderPlugin      1               MyGrid          MapSetA     server2
loaderPlugin      1               MyGrid          MapSetA     server3
loaderPlugin      1               MyGrid          MapSetA     server4
txCallbackPlugin  2               MyGrid          MapSetA     server1
txCallbackPlugin  2               MyGrid          MapSetA     server2
txCallbackPlugin  2               MyGrid          MapSetA     server3
txCallbackPlugin  2               MyGrid          MapSetA     server4
```

O exemplo a seguir mostra a saída do comando **osgiCurrent** quando server2 foi iniciado com uma classificação mais nova do loaderPlugin:

```
OSGi Service Name Current Ranking ObjectGrid Name MapSet Name Server Name
----------------- --------------- --------------- ----------- -----------
loaderPlugin      1               MyGrid          MapSetA     server1
loaderPlugin      2               MyGrid          MapSetA     server2
loaderPlugin      1               MyGrid          MapSetA     server3
loaderPlugin      1               MyGrid          MapSetA     server4
txCallbackPlugin  2               MyGrid          MapSetA     server1
txCallbackPlugin  2               MyGrid          MapSetA     server2
txCallbackPlugin  2               MyGrid          MapSetA     server3
txCallbackPlugin  2               MyGrid          MapSetA     server4
```

- Execute o comando **osgiAll** para verificar se os serviços de plug-in foram iniciados corretamente em cada servidor de contêiner do eXtreme Scale.

  Quando pacotes configuráveis que contêm serviços que uma configuração do ObjectGrid está referenciando são iniciados, o ambiente de tempo de execução do eXtreme Scale controla automaticamente o plug-in, mas não o usa imediatamente. O comando **osgiAll** mostra quais plug-ins estão disponíveis para cada servidor.

  Quando executados sem quaisquer parâmetros, todos os serviços são mostrados para todas as grades e todos os servidores. Filtros adicionais, incluindo o filtro **-serviceName** <service_name>, podem ser especificados para limitar a saída para um único serviço ou um subconjunto da grade de dados.

  O exemplo a seguir mostra a saída do comando **osgiAll** quando dois plug-ins são iniciados em dois servidores. O loaderPlugin possui ambas as classificações, 1 e 2, iniciadas e o txCallbackPlugin tem a classificação 1 iniciada. A mensagem de resumo no final da saída confirma que ambos os servidores consultam as mesmas classificações de serviço:

```
Server: server1
   OSGi Service Name   Available Rankings
   -----------------   ------------------
   loaderPlugin        1, 2
   txCallbackPlugin    1

Server: server2
   OSGi Service Name   Available Rankings
   -----------------   ------------------
   loaderPlugin        1, 2
   txCallbackPlugin    1

Summary - All servers have the same service rankings.
```

O exemplo a seguir mostra a saída do comando **osgiAll** quando o pacote configurável que inclui o loaderPlugin com classificação 1 é interrompido no server1. A mensagem de resumo na parte inferior da saída confirma que o server1 agora está ausente no loaderPlugin com classificação 1:

```
Server: server1
   OSGi Service Name   Available Rankings
   -----------------   ------------------
   loaderPlugin        2
   txCallbackPlugin    1

Server: server2
   OSGi Service Name   Available Rankings
   -----------------   ------------------
   loaderPlugin        1, 2
   txCallbackPlugin    1

Summary - The following servers are missing service rankings:
   Server  OSGi Service Name Missing Rankings
   ------  ----------------- ----------------
   server1 loaderPlugin      1
```

O exemplo a seguir mostra a saída se o nome do serviço é especificado com o argumento **-sn**, mas o serviço não existe:

```
Server: server2
   OSGi Service Name   Available Rankings
   ----------------- ------------------
   invalidPlugin     No service found

Server: server1
   OSGi Service Name   Available Rankings
   ----------------- ------------------
   invalidPlugin     No service found

Summary - All servers have the same service rankings.
```

- Execute o comando **osgiCheck** para verificar conjuntos de serviços de plug-in e classificações para ver se eles estão disponíveis.

  O comando **osgiCheck** aceita um ou mais conjuntos de classificações de serviço no formato: `-serviceRankings <service name>;<ranking>[,<serviceName>;<ranking>]`

  Quando as classificações estão todas disponíveis, o método retorna com um nível de erro igual a 0. Se uma ou mais classificações não estiverem disponíveis, um nível de erro diferente de zero será configurado. Uma tabela de todos os servidores que não incluem as classificações do serviço especificadas é exibida. Filtros adicionais podem ser usados para limitar a verificação de serviço para um subconjunto dos servidores disponíveis no domínio do eXtreme Scale.

  Por exemplo, se a classificação ou o serviço especificado estiver ausente, a seguinte mensagem será exibida:

```
Server  OSGi Service Unavailable Rankings
------  ------------ --------------------
server1 loaderPlugin 3
server2 loaderPlugin 3
```

- Execute o comando **osgiUpdate** para atualizar a classificação de um ou mais plug-ins para todos os servidores em um único ObjectGrid e MapSet em uma única operação.

  O comando aceita um ou mais conjuntos de classificações de serviço no formato: `-serviceRankings <service name>;<ranking>[,<serviceName>;<ranking>] -g <grid name> -ms <mapset name>`

  Com este comando, é possível concluir as operações a seguir:

– Verifique se os serviços especificados estão disponíveis para atualização em cada um dos servidores.
– Altere o estado da grade para offline usando a interface StateManager. Consulte Gerenciando a Disponibilidade do ObjectGrid para obter mais informações. Este processo coloca a grade em modo quiesce e aguarda até que qualquer transação em execução tenha concluído e impede o início de qualquer nova transação. Este processo também sinaliza quaisquer plug-ins ObjectGridLifecycleListener e BackingMapLifecycleListener para descontinuar qualquer atividade transacional. Consulte “Plug-ins para Fornecer Listeners de Eventos” na página 569 para obter informações sobre plug-ins do listener de eventos.
– Atualize cada contêiner do eXtreme Scale em execução em uma estrutura OSGi para usar as novas versões de serviço.
– Altere o estado da grade para online, permitindo que as transações continuem.

O processo de atualização é idempotente, de forma que, se um cliente falhar ao concluir qualquer tarefa, isto resultará na operação sendo recuperada. Se um cliente for incapaz de executar a recuperação ou for interrompido durante o processo de atualização, o mesmo comando poderá ser emitido novamente e ele continuará na etapa apropriada.

Se o cliente for incapaz de continuar, e o processo for reiniciado a partir de um outro cliente, use a opção `-force` para permitir que o cliente execute a atualização. O comando **`xscmd.bat/xscmd.sh`** impede que diversos clientes atualizem o mesmo conjunto de mapas simultaneamente. Para obter mais detalhes sobre o comando **`osgiUpdate`**, consulte Atualizando Serviços OSGi para Plug-ins do eXtreme Scale com **`xscmd`**.

Configurando Servidores com o OSGi Blueprint

Java

É possível configurar os servidores de contêiner do WebSphere eXtreme Scale usando um arquivo XML do OSGi Blueprint, permitindo o empacotamento e o desenvolvimento simplificados de pacotes configuráveis do servidor autocontidos.

Antes de Iniciar

Este tópico assume que as seguintes tarefas foram concluídas:

- A estrutura do Eclipse Equinox OSGi foi instalada e iniciada com o contêiner de projeto do Eclipse Gemini ou do Apache Aries.
- O pacote configurável do servidor eXtreme Scale foi instalado e iniciado.
- O pacote configurável de plug-ins dinâmicos do eXtreme Scale foi criado.
- O arquivo XML do descritor do ObjectGrid do eXtreme Scale e o arquivo XML da política de implementação foram criados.

Sobre Esta Tarefa

Esta tarefa descreve como configurar um servidor do eXtreme Scale com um contêiner usando um arquivo XML do projeto. O resultado do procedimento é um pacote configurável do contêiner. Quando o pacote configurável do contêiner for iniciado, o pacote configurável do servidor eXtreme Scale controlará o pacote configurável, analisará o XML do servidor e iniciará um servidor e um contêiner.

Um pacote configurável do contêiner pode ser, opcionalmente, combinado com o aplicativo e os plug-ins do eXtreme Scale quando atualizações do plug-in dinâmico

não são necessárias ou os plug-ins não suportam a atualização dinâmica.

Procedimento

1. Crie um arquivo XML do Blueprint com o namespace `objectgrid` incluído. É possível nomear o arquivo de qualquer jeito. No entanto, ele deve incluir o namespace do projeto:

```
<?xml version="1.0" encoding="UTF-8"?>

<blueprint xmlns="http://www.osgi.org/xmlns/blueprint/v1.0.0"
           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance
           xmlns:objectgrid="http://www.ibm.com/schema/objectgrid"
           xsi:schemaLocation="http://www.ibm.com/schema/objectgrid
                http://www.ibm.com/schema/objectgrid/objectgrid.xsd">
...
</blueprint>
```

2. Inclua a definição de XML para o servidor eXtreme Scale com as propriedades de servidor apropriadas. Consulte o arquivo XML do descritor do Spring para obter detalhes sobre todas as propriedades de configuração disponíveis. Consulte o exemplo a seguir da definição de XML:

```
<objectgrid:server id="xsServer" tracespec="ObjectGridOSGi=all=enabled"
tracefile="logs/osgi/wxsserver/trace.log" jmxport="1199" listenerPort="2909">
<objectgrid:catalog host="catserver1.mycompany.com" port="2809" />
<objectgrid:catalog host="catserver2.mycompany.com" port="2809" />
</objectgrid:server>
```

3. Inclua a definição de XML para o contêiner do eXtreme Scale com a referência para a definição de servidor e os arquivos XML do descritor do ObjectGrid e de implementação do ObjectGrid integrados no pacote configurável; por exemplo:

```
<objectgrid:container id="container"
    objectgridxml="/META-INF/objectGrid.xml"
    deploymentxml="/META-INF/objectGridDeployment.xml"
    server="xsServer" />
```

4. Armazene o arquivo XML do Blueprint no pacote configurável do contêiner. O XML do Blueprint deve ser armazenado no diretório `OSGI-INF/blueprint` para que o contêiner do Blueprint seja localizado.

   Para armazenar o XML do Blueprint em um diretório diferente, você deve especificar o cabeçalho de manifesto Bundle-Blueprint; por exemplo:

```
Bundle-Blueprint: OSGI-INF/blueprint.xml
```

5. Empacote os arquivos em um arquivo JAR do pacote configurável único. Consulte o exemplo a seguir de uma hierarquia do diretório do pacote configurável:

```
MyBundle.jar
    /META-INF/manifest.mf
    /META-INF/objectGrid.xml
    /META-INF/objectGridDeployment.xml
    /OSGI-INF/blueprint/blueprint.xml
```

Resultados

Um pacote configurável do contêiner do eXtreme Scale agora está criado e pode ser instalado no Eclipse Equinox. Quando o pacote configurável do contêiner é iniciado, o ambiente de tempo de execução do servidor eXtreme Scale no pacote configurável do servidor eXtreme Scale irá iniciar automaticamente servidor do eXtreme Scale de singleton usando os parâmetros definidos no pacote configurável e um servidor de contêiner é iniciado. O pacote configurável pode ser interrompido e iniciado, o que resulta no contêiner parando e iniciando. O servidor é um singleton e não para quando o pacote configurável é iniciado pela primeira vez.

Cenário: Usando JCA para Conectar Aplicativos Transacionais aos Clientes do eXtreme Scale

O cenário a seguir trata da conexão de clientes com os aplicativos que participam das transações.

Antes de Iniciar

Leia o tópico Processamento de Transações na Visão Geral de Aplicativos Java EE para aprender mais sobre o suporte à transação.

Sobre Esta Tarefa

O Java EE Connector Architecture (JCA) fornece suporte para clientes que estão usando a Java Transaction API (JTA). Por meio do JTA, o gerenciamento do cliente é simplificado e realizado com o uso do Java Platform, Enterprise Edition (Java EE). A especificação JCA também suporta os adaptadores de recursos que podem ser usados para conectar os aplicativos aos clientes do eXtreme Scale. Um adaptador de recursos é um driver de software de nível do sistema que um aplicativo Java usa para conectar-se a um Enterprise Information System (EIS). Um adaptador de recurso se conecta em um servidor de aplicativos e fornece conectividade entre o EIS, o servidor de aplicativos e o aplicativo corporativo. O WebSphere eXtreme Scale fornece seu próprio adaptador de recursos, que pode ser instalado sem nenhuma configuração necessária.

Assim como em versões anteriores do produto, é possível usar as transações para processar uma unidade única de trabalho para a grade de dados. Com o suporte do JCA, ao confirmar essas transações, é possível reunir recursos para essa transação no one-phase commit, que tem os benefícios a seguir:

- Desenvolvimento de aplicativo eXtreme Scale simplificado. Anteriormente, os desenvolvedores coordenavam as transações do eXtreme Scale com recursos, como enterprise beans, servlets e contêineres de web. Como não existia nenhum mecanismo de retrocesso, os desenvolvedores não tinham nenhuma maneira simples de recuperarem-se das falhas.
- Há uma integração mais fechada com o WebSphere Application Server, o que inclui o último suporte participante a ser relacionado nas transações globais, se necessário.

Objetivos do Cenário

Depois de concluir esse cenário, você saberá como concluir os objetivos a seguir:

- Usar o suporte de Java Transaction API (JTA) para desenvolver os componentes de aplicativo que usam as transações.
- Conectar seus aplicativos aos clientes do eXtreme Scale.

Processamento de Transações nos Aplicativos Java EE

O WebSphere eXtreme Scale fornece seu próprio adaptador de recursos que pode ser usado para conectar os aplicativos à grade de dados e processar as transações locais.

Por meio do suporte do adaptador de recursos do eXtreme Scale, os aplicativos Java Platform, Enterprise Edition (Java EE) podem consultar as conexões do cliente do eXtreme Scale e demarcar as transações locais usando as transações locais do

Java EE ou as APIs do eXtreme Scale. Quando o adaptador de recursos estiver configurado, será possível concluir as ações a seguir com seus aplicativos Java EE:

- Consulte ou introduza os connection factories do adaptador de recursos eXtreme Scale em um componente de aplicativo Java EE.
- Obtenha as manipulações de conexões padrão para o cliente eXtreme Scale e as compartilhe entre aos componentes de aplicativo usando as convenções do Java EE.
- Demarque as transações do eXtreme Scale usando a API javax.resource.cci.LocalTransaction ou a interface do com.ibm.websphere.objectgrid.Session.
- Use a API inteira do cliente eXtreme Scale, como a API ObjectMap e a API EntityManager.

Os recursos adicionais a seguir estão disponíveis com o WebSphere Application Server:

- Relacione as conexões do eXtreme Scale com uma transação global como um último participante com outros recursos de two-phase commit. O adaptador de recursos do eXtreme Scale fornece suporte de transação local com um recurso de single-phase commit. Com o WebSphere Application Server, seus aplicativos podem alistar um recurso single-phase commit em uma transação global por meio do último suporte participante.
- Instalação automática do adaptador de recursos quando o perfil é aumentado.
- Propagação da entidade de segurança automática.

Responsabilidades de Administrador

O adaptador de recursos do eXtreme Scale é instalado no servidor de aplicativo Java EE ou integrado no aplicativo. Depois de instalar o adaptador de recursos, o administrador criará um ou mais connection factories do adaptador de recursos para cada domínio de serviço de catálogo e opcionalmente cada instância da grade de dados. O connection factory identifica as propriedades que são necessárias para a comunicação com a grade de dados.

Os aplicativos se referem ao connection factory, o que estabelece a conexão com a grade de dados remotos. Cada connection factory hospeda uma única conexão do cliente do eXtreme Scale que é reutilizada para todos os componentes de aplicativo.

Importante: Como a conexão do cliente eXtreme Scale pode incluir um cache próximo, os aplicativos não devem compartilhar uma conexão. Um connection factory deve existir para uma instância única do aplicativo para evitar problemas ao compartilhar objetos entre os aplicativos.

O connection factory hospeda uma conexão do cliente eXtreme Scale, que é compartilhada entre todos os componentes do aplicativo de referência. Você pode usar o bean gerenciado (MBean) para acessar informações sobre a conexão do cliente ou para reconfigurar a conexão quando ela não for mais necessária.

Responsabilidades do Desenvolvedor de Aplicativos

Um desenvolvedor de aplicativos cria referências de recurso para connection factories gerenciados no descritor de implementação do aplicativo ou com anotações. Cada referência de recurso inclui uma referência local para o connection factory do eXtreme Scale, bem como o escopo de compartilhamento de recursos.

Importante: Ativar o compartilhamento de recurso é importante porque permite que a transação local seja compartilhada entre os componentes de aplicativo.

Os aplicativos podem introduzir o connection factory no componente de aplicativo Java EE ou podem consultar o connection factory usando o Java Naming Directory Interface (JNDI). O connection factory é usado para obter manipulações de conexão com a conexão do cliente do eXtreme Scale. A conexão do cliente eXtreme Scale é gerenciada de forma independente a partir da conexão do adaptador de recursos e é estabelecida no primeiro uso e reutilizada para todas as conexões subsequentes.

Após localizar a conexão, o aplicativo recupera uma referência de sessão do eXtreme Scale. Com a referência de sessão eXtreme Scale, o aplicativo pode usar os recursos e as APIs do cliente eXtreme Scale inteiro.

É possível demarcar as transações de uma das maneiras a seguir:

- Use os métodos de demarcação de transação com.ibm.websphere.objectgrid.Session.
- Use a transação local javax.resource.cci.LocalTransaction.
- Use uma transação global, ao usar o WebSphere Application Server com o último suporte ao participante ativado. Ao selecionar essa abordagem para demarcação, você deve:
  - Usar uma transação global gerenciada por aplicativo com o javax.transaction.UserTransaction.
  - Usar uma transação gerenciada por contêiner.

Responsabilidades do Implementador de Aplicativos

O implementador de aplicativos liga a referência local ao connection factory do adaptador de recursos que o desenvolvedor de aplicativos define para os connection factories do adaptador de recursos que o administrador define. O implementador de aplicativos deve designar o tipo de connection factory correto e o escopo para o aplicativo e garantir que o connection factory não seja compartilhado entre os aplicativos para evitar o compartilhamento do objeto Java. O implementador de aplicativo também é responsável por configurar e mapear outras informações de configuração apropriadas que são comuns a todos os connection factories.

Informações relacionadas:

- Conexões Não Compartilháveis e Compartilháveis
- Tratamento de Conexões
- Tipo de Transação e Comportamento da Conexão
- Suporte de Transação no WebSphere Application Server
- Transações Globais
- Local transaction containment
- Transações Local e Global

Instalando um Adaptador de Recursos do eXtreme Scale

O adaptador de recursos WebSphere eXtreme Scale é compatível com Java Connector Architecture (JCA) 1.5 e pode ser instalado em um Java 2 Platform, Enterprise Edition (J2EE) 1.5 1.6 ou posterior ou em um servidor de aplicativos como o WebSphere Application Server.

Antes de Iniciar

O adaptador de recursos está no arquivo `wxsra.rar` Resource Adapter Archive (RAR), que está disponível em todas as instalações do eXtreme Scale. O arquivo RAR está nos diretórios a seguir:

- Para instalações do WebSphere Application Server: *wxs_install_root*/`optionalLibraries/ObjectGrid`
- Para instalações independentes: diretório *wxs_install_root*/`ObjectGrid/lib`

O adaptador de recursos é acoplado ao ambiente de tempo de execução eXtreme Scale. Ele requer os arquivos JAR de tempo de execução eXtreme Scale no caminho de classe correto. Em geral, é possível atualizar o ambiente de tempo de execução eXtreme Scale sem atualizar o adaptador de recursos. Atualizar o ambiente de tempo de execução eXtreme Scale também atualiza o ambiente de tempo de execução do adaptador de recursos. O adaptador de recursos suporta a versão 8.5 e até duas versões posteriores do ambiente de tempo de execução eXtreme Scale. As versões mais recentes do adaptador de recursos podem precisar das versões mais recentes do ambiente de tempo de execução eXtreme Scale conforme ficam disponíveis.

O arquivo `wxsra.rar` requer que um dos arquivos JAR de tempo de execução do cliente eXtreme Scale opere. Para obter detalhes sobre qual arquivo JAR de tempo de execução do cliente é apropriado, consulte Arquivos de Tempo de Execução para Instalação Independente do WebSphere eXtreme Scale e Arquivos de Tempo de Execução para o WebSphere eXtreme Scale Integrado ao WebSphere Application Server, que inclui detalhes sobre os arquivos JAR de tempo de execução disponíveis.

Sobre Esta Tarefa

É possível instalar o adaptador de recursos do eXtreme Scale usando várias opções que permitem cenários de implementação flexíveis. O adaptador de recursos pode ser integrado ao aplicativo Java Platform, Enterprise Edition (Java EE) ou pode ser instalado como um arquivo RAR independente que é compartilhado entre os aplicativos.

A integração do adaptador de recursos com o aplicativo simplifica a implementação, porque os connection factories só são criados com o escopo do aplicativo e não podem ser compartilhados entre os aplicativos. Com o adaptador de recursos integrado no aplicativo, você também pode integrar os objetos de cache e as classes de plug-in do cliente ObjectGrid no aplicativo. A integração do adaptador de recursos também protege o aplicativo contra compartilhamento de objetos de cache de forma inadvertida entre aplicativos, o que pode resultar em exceções java.lang.ClassCastException.

Ao instalar o arquivo `wxsra.rar` como um adaptador de recursos independente, é possível criar connection factories do gerenciador de recursos no escopo do nó. Essa opção é útil nas situações a seguir:

- Quando não for prático integrar o arquivo `wxsra.rar` no aplicativo
- Quando a versão do eXtreme Scale não for conhecida no tempo da construção
- Quando você desejar compartilhar uma conexão do cliente eXtreme Scale com diversos aplicativos

Importante: Em diversas versões do WebSphere Application Server, até a Versão 8.0.2, não é possível instalar o adaptador de recursos eXtreme Scale em um arquivo

EAR do aplicativo e o servidor independente simultaneamente. O resultado, quando você usa o arquivo archive corporativo (EAR) que também tem o arquivo RAR instalado, é que o aplicativo presencia uma exceção, como `ClassCastException: com.ibm.websphere.xs.ra.XSConnectionFactory incompatível com com.ibm.websphere.xs.ra.XSConnectionFactory`. A mensagem de exemplo WebSphere Application Server a seguir e a pilha de chamada para esse erro são exibidas quando um servlet encontra esta exceção:

```
SRVE0068E: An exception was thrown by one of the service methods of the servlet [ClientServlet]
in application [JTASampleClientEAR]. Exception created : [java.lang.ClassCastException:
com.ibm.websphere.xs.ra.XSConnectionFactory incompatible with com.ibm.websphere.xs.ra.XSConnectionFactory
at com.ibm.websphere.xs.sample.jtasample.WXSClientServlet.connectClient(WXSClientServlet.java:484)
at com.ibm.websphere.xs.sample.jtasample.WXSClientServlet.doGet(WXSClientServlet.java:200)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:575)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:668)
at com.ibm.ws.webcontainer.servlet.ServletWrapper.service(ServletWrapper.java:1214)
at com.ibm.ws.webcontainer.servlet.ServletWrapper.handleRequest(ServletWrapper.java:774)
at com.ibm.ws.webcontainer.servlet.ServletWrapper.handleRequest(ServletWrapper.java:456)
```

Procedimento

- **Instale um adaptador de recursos do eXtreme Scale integrado.** Quando o arquivo `wxsra.rar` é integrado no arquivo EAR do aplicativo, o adaptador de recursos deve ter acesso às bibliotecas de tempo de execução do eXtreme Scale.

  Para os aplicativos que são executados no WebSphere Application Server, as opções a seguir e as ações subsequentes ficam disponíveis:

Opção	Descrição
Se o eXtreme Scale for integrado com o nó do WebSphere Application Server	Os arquivos de biblioteca de tempo de execução já estão disponíveis no caminho de classe e nenhuma outra ação é requerida.
Se o eXtreme Scale não for integrado com o nó do WebSphere Application Server	Você deve incluir o arquivo `wsogclient.jar` no caminho de classe `wxsra.rar`.

  Para os aplicativos que não são executados no WebSphere Application Server, o arquivo da biblioteca de tempo de execução do cliente, `ogclient.jar`, ou o arquivo da biblioteca do tempo de execução do servidor, `objectgrid.jar`, deve estar no caminho de classe do arquivo RAR.

- **Instale um adaptador de recursos do eXtreme Scale independente.** Ao instalar o arquivo `wxsra.rar` como um adaptador de recursos independente, ele deve ter acesso às bibliotecas de tempo de execução do eXtreme Scale.

  Para os aplicativos que são executados no WebSphere Application Server, as opções a seguir e as ações subsequentes ficam disponíveis:

Opção	Descrição
Se o eXtreme Scale for integrado com o nó do WebSphere Application Server	Os arquivos de biblioteca de tempo de execução já estão disponíveis no caminho de classe e nenhuma outra ação é requerida.
Se o eXtreme Scale não for integrado com o nó do WebSphere Application Server	Você deve incluir o arquivo `wsogclient.jar` no caminho de classe `wxsra.rar`.

  Para os aplicativos que não são executados no WebSphere Application Server, o arquivo da biblioteca de tempo de execução do cliente, `ogclient.jar`, ou o arquivo da biblioteca do tempo de execução do servidor, `objectgrid.jar`, deve estar no caminho de classe do arquivo RAR.

  1. Conceda o acesso ao adaptador de recursos a qualquer classe compartilhada. Todas as classes de plug-in do ObjectGrid e os aplicativos que as usam devem compartilhar um carregador de classes. Uma vez que o adaptador de recursos é compartilhado por diversos aplicativos, todas as classes devem ser acessíveis pelo mesmo carregador de classes. É possível criar esse acesso

usando uma biblioteca compartilhada entre todos os aplicativos que interagem com o adaptador de recursos.

O que Fazer Depois

Agora que você instalou o adaptador de recursos eXtreme Scale, é possível configurar os connection factories para que os seus aplicativos Java EE possam se conectar a uma grade de dados eXtreme Scale remota.

Informações relacionadas:

Instalando um Resource Adapter Archive

Instalando Adaptadores de Recursos Integrados em Aplicativos

Coleção do Adaptador de Recursos

Configurando os Connection Factories do eXtreme Scale

Java

Um connection factory do eXtreme Scale permite que os aplicativos Java EE se conectem com uma grade de dados remotos do WebSphere eXtreme Scale. Use as propriedades customizadas para configurar os adaptadores de recursos.

Antes de Iniciar

Antes de criar os connection factories, você deve instalar o adaptador de recursos.

Sobre Esta Tarefa

Depois de instalar o adaptador de recursos, é possível criar um ou mais connection factories do adaptador de recursos que representam as conexões do cliente do eXtreme Scale para grades de dados remotos. Conclua as etapas a seguir para configurar um connection factory do adaptador de recursos e usá-lo em um aplicativo.

É possível criar um connection factory do eXtreme Scale no escopo do nó para os adaptadores de recursos independentes ou no aplicativo para adaptadores de recursos integrados. Consulte os tópicos relacionados para obter informações sobre como criar connection factories no WebSphere Application Server.

Procedimento

1. Usando o console administrativo WebSphere Application Server para criar um connection factory eXtreme Scale que representa uma conexão do cliente do eXtreme Scale. Consulte Configurando os Connection Factories do Java EE Connector no console administrativo. Depois de especificar as propriedades para o connection factory no painel Propriedades Gerais, você deve clicar em **Aplicar** para que o link de propriedades Customizadas se torne ativo.
2. Clique em **Propriedades Customizadas** no console administrativo. Defina as propriedades customizadas a seguir para configurar a conexão do cliente para a grade de dados remotos.

Tabela 2. Propriedades Customizadas para Configurar os Connection Factories

Nome da Propriedade	Tipo	Descrição
ConnectionName	Sequência	(Opcional) O nome da conexão do cliente eXtreme Scale. O ConnectionName ajuda a identificar a conexão quando exposta como um bean gerenciado. Essa propriedade é opcional. Se não for especificada, o ConnectionName ficará indefinido.
CatalogServiceEndpoints	Sequência	(Opcional) Os terminais de domínio de serviço de catálogo no formato: `<host>:<port>[,<host><port>]`. Para obter informações adicionais, consulte Configurações do Domínio de Serviço de Catálogo. Essa propriedade será necessária se o domínio de serviço de catálogo não estiver configurado.
CatalogServiceDomain	Sequência	(Opcional) O nome do domínio de serviço de catálogo que está definido no WebSphere Application Server. Para obter informações adicionais, consulte Configurando os Servidores de Catálogos e os Domínios de Serviço de Catálogo. Essa propriedade será necessária se a propriedade CatalogServiceEndpoints não estiver configurada.
ObjectGridName	Sequência	(Opcional) Nome da grade de dados à qual esse connection factory se conecta. Se não estiver especificado, o aplicativo deverá fornecer o nome ao obter a conexão a partir do connection factory.
ObjectGridURL	Sequência	(Opcional) URL da grade de dados de cliente, substitui o arquivo XML. Essa propriedade não será válida se ObjectGridResource também for especificado. Para obter informações adicionais, consulte Configurando Clientes.
ObjectGridResource	Sequência	Caminho de recurso da grade de dados de cliente, substitui o arquivo XML. Essa propriedade será opcional e inválida se ObjectGridURL também for especificado. Para obter informações adicionais, consulte Configurando Clientes.
ClientPropertiesURL	Sequência	(Opcional) URL do arquivo de propriedades do cliente. Essa propriedade não será válida se ClientPropertiesResource também for especificado. Para obter informações adicionais, consulte Arquivo de Propriedades do Cliente.
ClientPropertiesResource	Sequência	(Opcional) Caminho de recurso do arquivo de propriedades do cliente. Essa propriedade não será válida se ClientPropertiesURL também for especificado. Para obter informações adicionais, consulte Arquivo de Propriedades do Cliente.

O WebSphere Application Server também permite outras opções de configuração para ajustar os conjuntos de conexões e gerenciar a segurança. Consulte as informações relacionadas para obter links para os tópicos do Centro de Informações do WebSphere Application Server.

O que Fazer Depois

Crie uma referência do connection factory do eXtreme Scale no aplicativo. Consulte “Configurando os Aplicativos para a Conexão com o eXtreme Scale” na página 197 para obter mais informações.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Informações relacionadas:

Configurações do Domínio de Serviço de Catálogo
Use esta página para gerenciar as configurações para um domínio de serviço de catálogo específico. Os domínios de serviço de catálogo definem um grupo de servidores de catálogos que gerenciam o posicionamento dos shards e monitora o funcionamento dos servidores de contêiner na grade de dados. É possível definir um domínio de serviço de catálogo que esteja na mesma célula que o seu gerenciador de implementação. Também é possível definir domínios de serviço de catálogo remoto se a configuração do WebSphere eXtreme Scale estiver em uma célula diferente ou se sua grade de dados for composta de processos Java SE.

Configurando Connection Factories de adaptadores de recursos dentro de aplicativos

Configurando Connection Factories do Java EE Connector no Console Administrativo

Configurando Novas Connection Factories J2C Utilizando Script wsadmin

Coleção de Connection Factories J2C

Práticas de Nomes JNDI da Connection Factory

Configurando os Ambientes do Eclipse para Usar os Connection Factories do eXtreme Scale

Java

O adaptador de recursos do eXtreme Scale inclui os connection factories customizados. Para usar essas interfaces em seus aplicativos eXtreme Scale Java Platform, Enterprise Edition (Java EE), você deve importar o arquivo `wxsra.rar` em sua área de trabalho e vinculá-lo ao seu projeto do aplicativo.

Antes de Iniciar

- Você deve instalar o Rational Application Developer Versão 7 ou posterior ou o Eclipse Java EE IDE para Desenvolvedores da Web Versão 1.4 ou posterior.
- Um ambiente de tempo de execução do servidor deve estar configurado.

Procedimento

1. Importe o arquivo `wxsra.rar` para o seu projeto selecionando **Arquivo** > **Importar**. A janela Importar é exibida.
2. Selecione **Java EE** > **Arquivo RAR**. A janela Importação do Conector é exibida.
3. Para especificar o arquivo do conector, clique em **Procurar** para localizar o arquivo `wxsra.rar`. O arquivo `wxsra.rar` é instalado quando você instala um adaptador de recursos. É possível localizar o arquivo Resource Adapter Archive (RAR) no local a seguir:
   - Para as instalações do WebSphere Application Server: *wxs_install_root*/optionalLibraries/ObjectGrid
   - Para instalações independentes: diretório *wxs_install_root*/ObjectGrid/lib
4. Crie um nome para o novo projeto de conector no campo **Projeto de conector**. É possível usar `wxsra`, que é o nome padrão.

5. Escolha um tempo de execução de Destino, o que faz referência a um ambiente de tempo de execução do servidor Java EE.
6. Opcionalmente, selecione **Incluir projeto ao EAR** para integrar o RAR a um projeto EAR existente.

Resultados

O arquivo RAR é agora importado para a área de trabalho do Eclipse.

O que Fazer Depois

É possível referenciar o projeto RAR a partir de seus outros projetos Java EE usando as etapas a seguir:

1. Clique com o botão direito no projeto e clique em **Propriedades**.
2. Selecione **Caminho de Construção Java**.
3. Selecione a guia Projetos.
4. Clique em **Incluir**.
5. Selecione o projeto de conector **wxsra** e clique em **OK**.
6. Clique em **OK** novamente para fechar a janela Propriedades.

As classes do adaptador de recursos do eXtreme Scale agora estão no caminho de classe. Para instalar o produto Arquivos JAR de Tempo de Execução usando o console Eclipse, consulte "Configurando um Ambiente de Desenvolvimento Independente no Eclipse" na página 339 para obter informações adicionais.

Configurando os Aplicativos para a Conexão com o eXtreme Scale

Os aplicativos usam um connection factory do eXtreme Scale para criar manipulações de conexão para uma conexão do cliente eXtreme Scale. É possível configurar as referências do connection factory do adaptador de recursos usando essa tarefa.

Antes de Iniciar

Crie um componente de aplicativo Java Platform, Enterprise Edition (Java EE), como um contêiner ou servlet do Enterprise JavaBeans (EJB).

Procedimento

Crie uma referência de recurso do javax.resource.cci.ConnectionFactory no componente de aplicativo. As referências de recurso são declaradas no descritor de implementação pelo provedor de aplicativos. O connection factory representa uma conexão do cliente eXtreme Scale que pode ser usada para a comunicação com uma ou mais grades de dados nomeadas que estão disponíveis no domínio de serviço de catálogo.

Informações relacionadas:

Conexões Não Compartilháveis e Compartilháveis

Benefícios de Referência de Recurso

Criando ou Alterando uma Referência de Recurso

Protegendo as Conexões do Cliente J2C

Use a arquitetura Java 2 Connector (J2C) para proteger as conexões entre clientes WebSphere eXtreme Scale e seus aplicativos.

Sobre Esta Tarefa

Os aplicativos se referem ao connection factory, o que estabelece a conexão com a grade de dados remotos. Cada connection factory hospeda uma única conexão do cliente do eXtreme Scale que é reutilizada para todos os componentes de aplicativo.

Importante: Uma vez que a conexão do cliente do eXtreme Scale pode incluir um cache próximo, é importante que os aplicativos não compartilhem uma conexão. Um connection factory deve existir para uma instância única do aplicativo para evitar problemas ao compartilhar objetos entre os aplicativos.

É possível configurar o gerador de credenciais com a API ou no arquivo de propriedades do cliente. No arquivo de propriedades do cliente, as propriedades securityEnabled e credentialGenerator são usadas. O exemplo de código a seguir é exibido em diversas linhas para propósitos de publicação:

```
securityEnabled=true
credentialGeneratorClass=com.ibm.websphere.objectgrid.security.plugins.builtins.
     UserPasswordCredentialGenerator
credentialGeneratorProps=operator XXXXXX
```

O gerador de credenciais e a credencial no arquivo de propriedades do cliente são usados para a operação de conexão eXtreme Scale e as credenciais J2C padrão. Portanto, as credenciais que são especificadas com a API são usadas no tempo de conexão J2C para a conexão J2C. No entanto, se nenhuma credencial estiver especificada no tempo de conexão J2C, o gerenciador de credencial no arquivo de propriedades do cliente será usado.

Procedimento

1. Configure o acesso seguro em que a conexão J2C representa o cliente eXtreme Scale. Use a propriedade do connection factory ClientPropertiesResource ou a propriedade do connection factory ClientPropertiesURL para configurar a autenticação de cliente.

   Se estiver usando o WebSphere eXtreme Scale com o WebSphere Application Server, especifique as propriedades do cliente na configuração do domínio de serviço de catálogo. Quando a connection factory referencia o domínio, ela usa automaticamente esta configuração.
2. Configure as propriedades de segurança do cliente para usar o connection factory que faz referência ao objeto gerador de credencial apropriado para eXtreme Scale. Essas propriedades também são compatíveis com a segurança do servidor eXtreme Scale. Por exemplo, use o gerador de credencial WSTokenCredentialGenerator para as credenciais WebSphere quando o eXtreme Scale estiver instalado com o WebSphere Application Server. Como alternativa, use o gerador de credencial UserPasswordCredentialGenerator quando executar o eXtreme Scale em um ambiente independente. No exemplo a seguir, as

credenciais são passadas programaticamente usando a chamada de API em vez de usar a configuração nas propriedades do cliente:

```
XSConnectionSpec spec = new XSConnectionSpec();
spec.setCredentialGenerator(new UserPasswordCredentialGenerator("operator", "xxxxxx"));
Connection conn = connectionFactory.getConnection(spec);
```

3. (Opcional) Desative o cache próximo, se necessário.

   Todas as conexões J2C de um único connection factory compartilham um único cache próximo. As permissões da entrada de grade e as permissões de mapa são validadas no servidor, mas não no cache próximo. Quando um aplicativo usa diversas credenciais para criar conexões J2C e a configuração usa permissões específicas para entradas de grade e mapas para essas credenciais, desative o cache próximo. Desative o cache próximo usando a propriedade do connection factory, ObjectGridResource ou ObjectGridURL. Para obter mais informações sobre como desativar o cache local, consulte Configurando o Cache Local.

4. (Opcional) Configure as configurações de política de segurança, se necessário.

   Se o aplicativo J2EE contém a configuração de arquivo Resource Adapter Archive (RAR) do eXtreme Scale integrado, pode ser necessário configurar as configurações de política de segurança adicionais no arquivo da política de segurança para o aplicativo. Por exemplo, essas políticas são necessárias:

   ```
   permission com.ibm.websphere.security.WebSphereRuntimePermission "accessRuntimeClasses";
   permission java.lang.RuntimePermission "accessDeclaredMembers";
   permission javax.management.MBeanTrustPermission "register";
   permission java.lang.RuntimePermission "getClassLoader";
   ```

   Além disso, quaisquer arquivos de propriedade ou recurso usados pelos connection factories precisarão do arquivo ou de outras permissões, como `permission java.io.FilePermission "filePath";`. Para WebSphere Application Server, o arquivo de políticas é `META-INF/was.policy`, e está localizado no arquivo EAR J2EE.

Resultados

As propriedades de segurança do cliente configuradas no domínio de serviço de catálogo são usadas como valores padrão. Os valores que você especifica substituem quaisquer propriedades definidas nos arquivos `client.properties`.

O que Fazer Depois

Use as APIs de acesso a dados eXtreme Scale para desenvolver os componentes do cliente que você deseja para usar as transações.

Desenvolvendo Componentes do Cliente eXtreme Scale para Usar Transações

Java

O adaptador de recursos WebSphere eXtreme Scale fornece suporte à transação local e gerenciamento de conexão do cliente. Com esse suporte, os aplicativos Java Platform, Enterprise Edition (Java EE) podem consultar as conexões do cliente eXtreme Scale e demarcar as transações locais com transações Java EE ou APIs eXtreme Scale.

Antes de Iniciar

Crie uma referência de recurso do connection factory do eXtreme Scale.

Sobre Esta Tarefa

Há várias opções para trabalhar com as APIs de acesso a dados do eXtreme Scale. Em todos os casos, o connection factory eXtreme Scale deve ser injetado no componente de aplicativo ou consultado no Java Naming Directory Interface (JNDI). Depois que o connection factory for consultado, você poderá demarcar as transações e criar conexões para acessar as APIs do eXtreme Scale.

Opcionalmente, você pode executar cast da instância javax.resource.cci.ConnectionFactory para um com.ibm.websphere.xs.ra.XSConnectionFactory que forneça opções adicionais para recuperar as manipulações de conexões. As manipulações de conexão resultante devem ser lançadas na interface com.ibm.websphere.xs.ra.XSConnection, que fornece o método getSession. O método getSession retorna uma manipulação de objeto com.ibm.websphere.objectgrid.Session que permite que os aplicativos usem algumas das APIs de acesso a dados eXtreme Scale, como a API ObjectMap e a API EntityManager.

A manipulação de Sessão e quaisquer objetos derivados são válidos pela duração da manipulação XSConnection.

Os procedimentos a seguir podem ser usados para demarcar as transações do eXtreme Scale. Não é possível combinar cada um dos procedimentos. Por exemplo, não é possível combinar demarcação de transação global e demarcação de transação local no mesmo contexto do componente de aplicativo.

Procedimento

- Use confirmação automática, transações locais. Use as etapas a seguir para confirmar automaticamente as operações de acesso a dados ou operações que não suportam uma transação ativa:
  1. Recupere uma conexão com.ibm.websphere.xs.ra.XSConnection fora do contexto de uma transação global.
  2. Recupere e use a sessão com.ibm.websphere.objectgrid.Session para interagir com a grade de dados.
  3. Chame qualquer operação de acesso a dados que suporte as transação de confirmação automática.
  4. Feche a conexão.
- Use uma sessão ObjectGrid para demarcar uma transação local. Use as etapas a seguir para demarcar uma transação ObjectGrid usando o objeto de Sessão:
  1. Recupere uma conexão com.ibm.websphere.xs.ra.XSConnection.
  2. Recupere a sessão com.ibm.websphere.objectgrid.Session.
  3. Use o método Session.begin() para iniciar a transação.
  4. Use a sessão para interagir com a grade de dados.
  5. Use os métodos Session.commit() ou rollback() para terminar a transação.
  6. Feche a conexão.
- Use uma transação javax.resource.cci.LocalTransction para demarcar uma transação local. Use as etapas a seguir para demarcar uma transação ObjectGrid usando a interface javax.resource.cci.LocalTransaction:
  1. Recupere uma conexão com.ibm.websphere.xs.ra.XSConnection.
  2. Recupere a transação javax.resource.cci.LocalTransaction usando o método XSConnection.getLocalTransaction().
  3. Use o método LocalTransaction.begin() para iniciar a transação.

4. Recupere e use a sessão com.ibm.websphere.objectgrid.Session para interagir com a grade de dados.
5. Use os métodos LocalTransaction.commit() ou rollback() para terminar a transação.
6. Feche a conexão.

- Relacione a conexão em uma transação global. Esse procedimento também se aplica a transações gerenciadas por contêiner:
  1. Inicie a transação global por meio da interface javax.transaction.UserTransaction ou com uma transação gerenciada por contêiner.
  2. Recupere uma conexão com.ibm.websphere.xs.ra.XSConnection.
  3. Recupere e use a sessão com.ibm.websphere.objectgrid.Session.
  4. Feche a conexão.
  5. Confirme ou retroceda a transação global.
- **8.6+** Configure uma conexão para compor diversas partições em uma transação. Use as etapas a seguir para demarcar uma transação ObjectGrid usando o objeto de Sessão:
  1. Crie um novo objeto com.ibm.websphere.xs.ra.XSConnectionSpec.
  2. Chame o método XSConnectionSpec e o método setMultiPartitionSupportEnabled com um argumento igual a `true`.
  3. Recupere a conexão com.ibm.websphere.xs.ra.XSConnection para transmitir a XSConnectionSpec ao método ConnectionFactory.getConnection.
  4. Recupere e use a sessão com.ibm.websphere.objectgrid.Session.

Exemplo

Consulte o exemplo de código a seguir, que demonstra as etapas anteriores para demarcar as transações eXtreme Scale.

```
// (C) Copyright IBM Corp. 2001, 2012.
// All Rights Reserved. Licensed Materials - Property of IBM.
package com.ibm.ws.xs.ra.test.ee;

import javax.naming.InitialContext;
import javax.resource.cci.Connection;
import javax.resource.cci.ConnectionFactory;
import javax.resource.cci.LocalTransaction;
import javax.transaction.Status;
import javax.transaction.UserTransaction;

import junit.framework.TestCase;

import com.ibm.websphere.objectgrid.ObjectMap;
import com.ibm.websphere.objectgrid.Session;
import com.ibm.websphere.xs.ra.XSConnection;

/**
* This sample requires that it runs in a J2EE context in your
* application server. For example, using the JUnitEE framework servlet.
*
* The code in these test methods would typically reside in your own servlet,
* EJB, or other web component.
*
* The sample depends on a configured WebSphere eXtreme Scale connection
* factory registered at of JNDI Name of "eis/embedded/wxscf" that defines
* a connection to a grid containing a Map with the name "Map1".
*
* The sample does a direct lookup of the JNDI name and does not require
* resource injection.
*/
public class DocSampleTests extends TestCase {
    public final static String CF_JNDI_NAME = "eis/embedded/wxscf";
    public final static String MAP_NAME = "Map1";
```

```
Long                key = null;
Long                value = null;
InitialContext      ctx = null;
ConnectionFactory cf = null;

public DocSampleTests() {
}
public DocSampleTests(String name) {
    super(name);
}
protected void setUp() throws Exception {
    ctx = new InitialContext();
    cf = (ConnectionFactory)ctx.lookup(CF_JNDI_NAME);
    key = System.nanoTime();
    value = System.nanoTime();
}
/**
 * This example runs when not in the context of a global transaction
 * and uses autocommit.
 */
public void testLocalAutocommit() throws Exception {
    Connection conn = cf.getConnection();
    try {
        Session    session = ((XSConnection)conn).getSession();
        ObjectMap  map = session.getMap(MAP_NAME);
        map.insert(key, value); // Or various data access operations
    }
    finally {
        conn.close();
    }
}

/**
 * This example runs when not in the context of a global transaction
 * and demarcates the transaction using session.begin()/session.commit()
 */
public void testLocalSessionTransaction() throws Exception {
    Session session = null;
    Connection conn = cf.getConnection();
    try {
        session = ((XSConnection)conn).getSession();
        session.begin();
        ObjectMap  map = session.getMap(MAP_NAME);
        map.insert(key, value); // Or various data access operations
        session.commit();
    }
    finally {
        if (session != null && session.isTransactionActive()) {
            try { session.rollback(); }
            catch (Exception e) { e.printStackTrace(); }
        }
        conn.close();
    }
}

/**
 * This example uses the LocalTransaction interface to demarcate
 * transações.
 */
public void testLocalTranTransaction() throws Exception {
    LocalTransaction tx = null;
    Connection conn = cf.getConnection();
    try {
        tx = conn.getLocalTransaction();
        tx.begin();
        Session    session = ((XSConnection)conn).getSession();
        ObjectMap  map = session.getMap(MAP_NAME);
        map.insert(key, value); // Or various data access operations
        tx.commit(); tx = null;
    }
    finally {
        if (tx != null) {
            try { tx.rollback(); }
            catch (Exception e) { e.printStackTrace(); }
        }
        conn.close();
    }
}
```

```
        /**
         * This example depends on an externally managed transaction,
         * the externally managed transaction might typically be present in
         * an EJB with its transaction attributes set to REQUIRED or REQUIRES_NEW.
         * NOTE: If there is NO global transaction active, this example runs in auto-commit
         *       mode because it doesn't verify a transaction exists.
         */
        public void testGlobalTransactionContainerManaged() throws Exception {
            Connection      conn = cf.getConnection();
            try {
                Session    session = ((XSConnection)conn).getSession();
                ObjectMap  map = session.getMap(MAP_NAME);
                map.insert(key, value); // Or various data access operations
            }
            catch (Throwable t) {
                t.printStackTrace();
                UserTransaction tx = (UserTransaction)ctx.lookup("java:comp/UserTransaction");
                if (tx.getStatus() != Status.STATUS_NO_TRANSACTION) {
                    tx.setRollbackOnly();
                }
            }
            finally {
                conn.close();
            }
        }

        /**
         * This example demonstrates starting a new global transaction using the
         * UserTransaction interface. Typically the container starts the global
         * transaction (for example in an EJB with a transaction attribute of
         * REQUIRES_NEW), but this sample will also start the global transaction
         * using the UserTransaction API if it is not currently active.
         */
        public void testGlobalTransactionTestManaged() throws Exception {
            boolean         started = false;
            UserTransaction tx = (UserTransaction)ctx.lookup("java:comp/UserTransaction");
            if (tx.getStatus() == Status.STATUS_NO_TRANSACTION) {
                tx.begin();
                started = true;
            }
            // else { called with an externally/container managed transaction }
            Connection conn  = null;
            try {
                conn = cf.getConnection(); // Get connection after the global tran starts
                Session    session = ((XSConnection)conn).getSession();
                ObjectMap  map = session.getMap(MAP_NAME);
                map.insert(key, value); // Or various data access operations
                if (started) {
                    tx.commit(); started = false; tx = null;
                }
            }
            finally {
                if (started) {
                    try { tx.rollback(); }
                    catch (Exception e) { e.printStackTrace(); }
                }
                if (conn != null) { conn.close(); }
            }
        }
/**
         /**
         * This example demonstrates a multi-partition transaction.
         */

    public void testGlobalTransactionTestManagedMultiPartition() throws Exception {
      boolean         started = false;
      XSConnectionSpec connSpec = new XSConnectionSpec();
      connSpec.setWriteToMultiplePartitions(true);
      UserTransaction tx = (UserTransaction)ctx.lookup("java:comp/UserTransaction");
      if (tx.getStatus() == Status.STATUS_NO_TRANSACTION) {
        tx.begin();
      started = true;
     }
    // else { called with an externally/container managed transaction }
      Connection conn  = null;
         try {
      conn = cf.getConnection(connSpec); // Get connection after the global tran starts
      Session    session = ((XSConnection)conn).getSession();
```

```
 ObjectMap  map = session.getMap(MAP_NAME);
 map.insert(key, value); // Or various data access operations
 if (started) {
   tx.commit(); started = false; tx = null;
   }
 }
 finally {
  if (started) {
    try { tx.rollback(); }
    catch (Exception e) { e.printStackTrace(); }
  }
  if (conn != null) { conn.close(); }
 }
}
```

Informações relacionadas:

- Benefícios de Referência de Recurso
- Desenvolvendo Componentes para Usar Transações

Administrando as Conexões do Cliente J2C

Java

O connection factory do WebSphere eXtreme Scale inclui uma conexão do cliente eXtreme Scale que pode ser compartilhada entre os aplicativos e persistida com a reinicialização do aplicativo.

Sobre Esta Tarefa

A conexão do cliente inclui um bean de gerenciamento que fornece informações do status de conexão e operações de gerenciamento do ciclo de vida.

Procedimento

Manter as conexões do cliente. Quando a primeira conexão é obtida a partir do objeto do connection factory XSConnectionFactory, uma conexão do cliente eXtreme Scale é estabelecida para a grade de dados remotos e o ObjectGridJ2CConnection MBean é criado. A conexão do cliente é mantida durante a vida útil do processo. Para terminar uma conexão do cliente, chame um dos eventos a seguir:

- Pare o adaptador de recursos. Um adaptador de recursos pode ser interrompido, por exemplo, quando ele é integrado em um aplicativo e o aplicativo é interrompido.
- Chame a operação resetConnection MBean no ObjectGridJ2CConnection MBean. Quando a conexão é reconfigurada, todas as conexões são invalidadas, as transações são concluídas e a conexão do cliente ObjectGrid é destruída. As chamadas subsequentes para os métodos getConnection no connection factory resultam em uma nova conexão do cliente.

O WebSphere Application Server também fornece beans de gerenciamento adicionais para gerenciar as conexões J2C, monitorar os conjuntos de conexões e o desempenho.

Informações relacionadas:

Gerenciamento do Ciclo de Vida do JCA

Documentação da API do MBean de Conexão J2C da Grade de Objeto

Cenário: Configurando o Failover da Sessão HTTP no Perfil do Liberty

É possível configurar um servidor de aplicativos da web para que, quando o servidor da web receber uma solicitação de HTTP para a replicação da sessão, a solicitação seja encaminhada para um ou mais servidores que são executados no perfil do Liberty.

Antes de Iniciar

Para concluir esta tarefa, você deve instalar o Perfil do Liberty. Para obter informações adicionais, consulte Instalando o Perfil do Liberty.

Sobre Esta Tarefa

O perfil do Liberty não inclui replicação de sessão. No entanto, se você usar o WebSphere eXtreme Scale com o perfil do Liberty, poderá replicar sessões. Portanto, se um servidor falhar, os usuários do aplicativo não perderão dados da sessão.

Ao incluir o recurso webApp na definição do servidor e configurar o gerenciador de sessões, é possível usar a replicação de sessão em seus aplicativos eXtreme Scale executados no perfil do Liberty.

Ativando o Recurso da Web do eXtreme Scale no Perfil do Liberty

Java

É possível ativar o recurso da web para utilizar o failover de sessão HTTP no perfil do Liberty.

Sobre Esta Tarefa

O recurso da web foi descontinuado. Use o recurso webApp em seu lugar. Ao incluir o recurso webApp na definição do servidor e configurar o gerenciador de sessões, é possível usar a replicação de sessão em seus aplicativos WebSphere eXtreme Scale executados no Perfil do Liberty.

Ao instalar o WebSphere Application Server Perfil do Liberty, ele não inclui a replicação da sessão. No entanto, se você utilizar o WebSphere eXtreme Scale com o perfil do Liberty, poderá replicar as sessões de forma que, se um servidor ficar inativo, os usuários do aplicativo não percam os dados da sessão.

Quando você inclui o recurso da web na definição de servidor e configura o gerenciador de sessões, é possível usar a replicação de sessão em seus aplicativos eXtreme Scale que são executados no perfil do Liberty.

Procedimento

Definir um aplicativo da web para execução no perfil do Liberty.

O que Fazer Depois

Em seguida, configure um plug-in de servidor da web para encaminhar solicitações de HTTP para vários servidores no perfil do Liberty.

Referências relacionadas:

Propriedades do Recurso da Web do Perfil do Liberty
Especifique o recurso da web para sua definição de servidor para identificar aplicativos baseados na web e incluir funções, como replicação da sessão.

Propriedades do Recurso webGrid do Perfil do Liberty
Especifique o recurso webGrid para iniciar automaticamente um contêiner que hospeda clientes para replicação de sessão HTTP.

Propriedades do Recurso webApp do Perfil do Liberty
Especifique o recurso webApp para estander o aplicativo da web do perfil do Liberty. Inclua o recurso webApp quando desejar replicar os dados da sessão HTTP para tolerância a falhas.

Ativando o Recurso webGrid do eXtreme Scale no Perfil do Liberty

Use o recurso webGrid para iniciar automaticamente um contêiner para hospedar os clientes para replicação de sessão HTTP no Perfil do Liberty.

Sobre Esta Tarefa

Ao instalar o WebSphere Application Server Perfil do Liberty, ele não inclui a replicação da sessão. No entanto, se você utilizar o WebSphere eXtreme Scale com o perfil do Liberty, poderá replicar as sessões de forma que, se um servidor ficar inativo, os usuários do aplicativo não percam os dados da sessão.

Quando você inclui o recurso webGrid na definição de servidor e configura o gerenciador de sessões, é possível usar a replicação de sessão em seus aplicativos eXtreme Scale que são executados no perfil do Liberty.

Procedimento

Inclua o recurso webGrid a seguir no arquivo `server.xml` do Perfil do Liberty. O recurso webGrid inclui o recurso cliente e o recurso servidor. Você provavelmente deseja separar seus aplicativos da web a partir das grades de dados. Por exemplo, você tem um servidor Perfil do Liberty para seus aplicativos da web e um servidor Perfil do Liberty diferente para hospedar a grade de dados.

```
<featureManager>
<feature>eXtremeScale_webGrid-1.1</feature>
</featureManager>
```

Resultados

Seus aplicativos da web agora podem persistir seus dados de sessão em uma grade do WebSphere eXtreme Scale.

Exemplo

O recurso webGrid possui propriedades de metatipo que você pode configurar no elemento xsWebGrid do arquivo `server.xml`. Consulte o exemplo a seguir de um arquivo `server.xml`, que contém o recurso webGrid usado ao se conectar à grade de dados remotamente.

```
<server description="Airport Entry eXtremeScale Getting Started Client Web Server">
<!--
This sample program is provided AS IS and may be used, executed, copied and modified
without royalty payment by customer
(a) for its own instruction and study,
(b) in order to develop applications designed to run with an IBM WebSphere product,
either for customer's own internal use or for redistribution by customer, as part of such an
application, in customer's own products.
Licensed Materials - Property of IBM
5724-X67, 5655-V66 (C) COPYRIGHT International Business Machines Corp. 2012
-->
<!-- Enable features -->
<featureManager>
<feature>eXtremeScale.webGrid-1.1</feature>
</featureManager>

<xsServer catalogServer="true"/>

<xsWebGrid objectGridName="session" catalogHostPort="remoteHost:2809" securityEnabled="false" />

</server>
```

Referências relacionadas:

Propriedades do Recurso webGrid do Perfil do Liberty
Especifique o recurso webGrid para iniciar automaticamente um contêiner que hospeda clientes para replicação de sessão HTTP.

Ativando o Recurso webApp do eXtreme Scale no Perfil do Liberty

Um servidor de perfis Liberty pode hospedar uma grade de dados que armazena dados em cache para aplicativos para replicar dados de sessão HTTP para tolerância a falhas.

Sobre Esta Tarefa

Ao instalar o WebSphere Application Server Perfil do Liberty, ele não inclui a replicação da sessão. No entanto, se você utilizar o WebSphere eXtreme Scale com o perfil do Liberty, poderá replicar as sessões de forma que, se um servidor ficar inativo, os usuários do aplicativo não percam os dados da sessão.

Quando você inclui o recurso webApp na definição de servidor e configura o gerenciador de sessões, é possível usar a replicação de sessão em seus aplicativos eXtreme Scale que são executados no perfil do Liberty.

Procedimento

Inclua o recurso webApp a seguir no arquivo `server.xml` do Perfil do Liberty. O recurso webApp inclui o recurso cliente; entretanto, ele não inclui o recurso do servidor. Você provavelmente deseja separar seus aplicativos da web a partir das grades de dados. Por exemplo, você tem um servidor Perfil do Liberty para seus aplicativos da web e um servidor Perfil do Liberty diferente para hospedar a grade de dados.

```
<featureManager>
<feature>eXtremeScale_webapp-1.1</feature>
</featureManager>
```

Resultados

Seus aplicativos da web agora podem persistir seus dados de sessão em uma grade do WebSphere eXtreme Scale.

Exemplo

Consulte o exemplo a seguir de um arquivo `server.xml`, que contém o recurso webApp usado ao se conectar à grade de dados remotamente.

```
<server description="Airport Entry eXtremeScale Getting Started Client Web Server">
<!--
This sample program is provided AS IS and may be used, executed, copied and modified
without royalty payment by customer
(a) for its own instruction and study,
(b) in order to develop applications designed to run with an IBM WebSphere product,
either for customer's own internal use or for redistribution by customer, as part of such an
application, in customer's own products.
Licensed Materials - Property of IBM
5724-X67, 5655-V66 (C) COPYRIGHT International Business Machines Corp. 2012
-->
<!-- Enable features -->
<featureManager>
<feature>eXtremeScale.webapp-1.1</feature>
</featureManager>

<httpEndpoint id="defaultHttpEndpoint"
host="*"
httpPort="${default.http.port}"
httpsPort="${default.https.port}" />

<xsWebApp objectGridName="session" catalogHostPort="remoteHost:2809" securityEnabled="false" />

</server>
```

O que Fazer Depois

O recurso webApp possui propriedades de metatipo que você pode configurar no elemento xsWebApp do arquivo `server.xml`. Para obter informações adicionais, consulte Propriedades do Recurso webApp do Perfil do Liberty.

Referências relacionadas:

Propriedades do Recurso webApp do Perfil do Liberty
Especifique o recurso webApp para estander o aplicativo da web do perfil do Liberty. Inclua o recurso webApp quando desejar replicar os dados da sessão HTTP para tolerância a falhas.

Configurando um Plug-in de Servidor da Web para Encaminhar Solicitações para Diversos Servidores no Perfil do Liberty

Java

Utilize esta tarefa para configurar o plug-in de servidor da Web para distribuir solicitações do servidor HTTP entre múltiplos servidores no perfil do Liberty.

Antes de Iniciar

Antes de configurar o plug-in de servidor da web para rotear solicitações de HTTP para vários servidores, conclua a seguinte tarefa:

- "Ativando o Recurso webApp do eXtreme Scale no Perfil do Liberty" na página 207

Sobre Esta Tarefa

Configure o plug-in de servidor da web para que o servidor da web receba uma solicitação de HTTP para recursos dinâmicos, a solicitação é encaminhada para vários servidores que são executados no perfil do Liberty.

Procedimento

Consulte Configurando o Perfil do Liberty com um Plug-in de Servidor da Web no Centro de Informações do WebSphere Application Server para concluir esta tarefa.

O que Fazer Depois

Em seguida, mescle os arquivos `plugin-cfg.xml` de diversas células do servidor de aplicativos. Você também deve assegurar que IDs de clone exclusivos existam para cada servidor de aplicativos que é executado no perfil do Liberty.

Mesclando os Arquivos de Configuração do Plug-in para Implementação no Plug-in do Servidor de Aplicativos

Java

Gere os arquivos de configuração de plug-in após configurar um ID de clone exclusivo no arquivo de configuração server.xml do Liberty.

Antes de Iniciar

Se você estiver gerando e mesclando arquivos de configuração do plug-in para configurar o failover da sessão HTTP em um perfil do Liberty, deverá concluir as seguintes tarefas:

- "Ativando o Recurso da Web do eXtreme Scale no Perfil do Liberty" na página 205
- "Configurando um Plug-in de Servidor da Web para Encaminhar Solicitações para Diversos Servidores no Perfil do Liberty" na página 208

Sobre Esta Tarefa

Utilize o console administrativo do WebSphere Application Server para concluir esta tarefa.

Procedimento

1. Mescle os arquivos `plugin-cfg.xml` a partir de diversas células do servidor de aplicativos. É possível mesclar manualmente os arquivos `plugin-cfg.xml` ou usar a ferramenta pluginCfgMerge para mesclar automaticamente o arquivo `plugin-cfg.xml` a partir de diversos perfis do servidor de aplicativos em um único arquivo de saída. Os arquivos pluginCfgMerge.bat e pluginCfgMerge.sh estão no diretório *install_root*`/bin`.

   Para obter informações adicionais sobre como mesclar manualmente os arquivos `plugin-cfg.xml`, consulte a nota técnica sobre como mesclar arquivos `plugin-cfg.xml` de diversos perfis de servidor de aplicativos.
2. Assegure que o valor de cloneID para cada servidor de aplicativos seja exclusivo. Examine o valor de cloneID para cada servidor de aplicativos no arquivo mesclado para assegurar que esse valor seja exclusivo para cada servidor de aplicativos. Se os valores de cloneID no arquivo mesclado não forem todos exclusivos, ou se você estiver executando com replicação de sessão de memória para memória no modo peer to peer, utilize o console administrativo para configurar cloneIDs de sessão HTTP exclusivos.

   Para configurar um ID de clone da sessão HTTP exclusivo com o console administrativo do WebSphere Application Server, conclua as seguintes etapas:

a. Clique em **Servidores** > **Tipos de Servidor** > **WebSphere Application Servers** > *server_name*.
b. Em Configurações do Contêiner, clique em **Configurações do Contêiner da Web** > **Contêiner da Web**.
c. Em Propriedades Adicionais, clique em **Propriedades Customizadas** > **Novo**.
d. Insira `HttpSessionCloneId` no campo **Nome** e insira um valor exclusivo para o servidor no campo **Valor**. O valor exclusivo deve ser de oito a nove caracteres alfanuméricos de comprimento. Por exemplo, `test1234` é um valor de cloneID válido.
e. Clique em **Aplicar** ou em **OK**.
f. Clique em **Salvar** para salvar as mudanças na configuração principal.

3. Copie o arquivo `plugin-cfg.xml` mesclado no diretório *plugin_installation_root*`/config/web_server_name` no host do servidor da web.
4. Assegure que você definiu as permissões de acesso ao arquivo do sistema operacional corretas para o arquivo `plugin-cfg.xml` mesclado. Essas permissões de acesso de arquivo permite que o processo do plug-in do servidor HTTP leia o arquivo.

Resultados

Ao concluir essa tarefa, você terá um arquivo de configuração de plug-in para diversas células do servidor de aplicativos e seus aplicativos eXtreme Scale que são executados no perfil do Liberty e são ativados para replicação de sessão.

Cenário: Executando Servidores de Grade no Perfil do Liberty Usando Ferramentas Eclipse

É possível usar ferramentas Eclipse para executar servidores WebSphere eXtreme Scale no perfil do Liberty do WebSphere Application Server. As ferramentas Eclipse oferecem uma maneira conveniente de executar seus servidores no mesmo ambiente Eclipse no qual você desenvolve, configura e implementa seus aplicativos eXtreme Scale.

Sobre Esta Tarefa

Com as ferramentas Eclipse, é possível configurar servidores eXtreme Scale para execução no Perfil do Liberty. Se você concluir esta tarefa manualmente, inclua os recursos do Liberty suportados no arquivo `server.xml`. No entanto, ao usar as ferramentas Eclipse, é possível concluir esta tarefa e outras tarefas de desenvolvimento usando Eclipse Java EE IDE for Web Developers, Versão: Indigo Service Release 1.

Instalando as Ferramentas do Desenvolvedor do Perfil do Liberty para WebSphere eXtreme Scale

O Eclipse fornece uma interface gráfica com o usuário (GUI) que você pode usar para executar servidores WebSphere eXtreme Scale no Perfil do Liberty. Para utilizar essa GUI, você deve instalar as ferramentas de perfil do Liberty do WebSphere eXtreme Scale Versão 8.5.

Sobre Esta Tarefa

As ferramentas podem ser instaladas usando um dos seguintes métodos:

- Instalar a partir do Eclipse Marketplace. Clique em **Ajuda** > **Eclipse Marketplace**.
- Instale arrastando um ícone **Instalar** para um ambiente de trabalho em execução. Essa opção está disponível somente para instalar as ferramentas do desenvolvedor no Eclipse IDE para Java EE Developers 3.7 ou posterior.

Você deve instalar o IBM WebSphere Application Server V8.5 Liberty Profile Developer Tools para usar o IBM WebSphere eXtreme Scale V8.5 Liberty Profile Developer Tools. Portanto, as etapas nesta tarefa incluem a instalação de ambas as ferramentas do desenvolvedor.

Procedimento

- Instalar a partir do Eclipse Marketplace.
  1. Inicie o seu ambiente de trabalho Eclipse.
  2. Clique em Ajuda > Eclipse Marketplace.
  3. No campo Localizar, digite WebSphere.
  4. Na lista de resultados, localize **IBM WebSphere Application Server V8.5 Liberty Profile Developer Tools** e clique em **Instalar**.
  5. A página Confirmar Recursos Selecionados é aberta. Continue com o procedimento de instalação na etapa "Concluir o Procedimento de Instalação".
  6. Conclua cada uma das etapas anteriores para instalar o **IBM WebSphere eXtreme Scale V8.5 Liberty Profile Developer Tools**.
- Conclua o procedimento de instalação.
  1. Expanda o nó para o conjunto de ferramentas que você instalou.
  2. Selecione **IBM WebSphere Application Server V8.5 Liberty Profile Developer Tools** ou **IBM WebSphere eXtreme Scale V8.5 Liberty Profile Developer Tools**.
  3. Selecione qualquer um dos recursos opcionais que você deseja instalar. Quando concluir, clique em **Avançar**.

     Lembre-se: Se você desejar instalar qualquer um dos recursos de instalação adicionais opcionais, como os recursos de ferramentas do WebSphere Application Server para a Versão 8.5, 8.0 ou 7.0, um conjunto separado de instruções de instalação está disponível no tópico Visão Geral do IBM WebSphere Application Server Developer Tools para Eclipse Versão 8.5 no Centro de Informações do WebSphere Application Server.
  4. Na página Revisar Licenças, revise o texto da licença.
  5. Se concordar com os termos, clique em **Eu aceito os termos do contrato de licença** e clique em **Concluir**. O processo de instalação é iniciado.
  6. Quando o processo de instalação for concluído, reinicie o ambiente de trabalho.

Configurando seu Ambiente de Desenvolvimento no Eclipse

Após instalar o conjunto de ferramentas Perfil do Liberty Eclipse para WebSphere eXtreme Scale, você deve configurar seus servidores eXtreme Scale no Perfil do Liberty e gerar um projeto Eclipse no qual você pode iniciar tarefas de desenvolvimento.

Configurando o eXtreme Scale no Perfil do Liberty Usando Ferramentas Eclipse

Você deve configurar seus servidores WebSphere eXtreme Scale para execução no WebSphere Application Server Perfil do Liberty. Conclua esta tarefa para configurar servidores do eXtreme Scale com ferramentas do Eclipse.

Antes de Iniciar

Você deve definir um servidor Perfil do Liberty no Eclipse. Para concluir esta tarefa, consulte Criando um Servidor de Perfil do Liberty Utilizando Ferramentas do Desenvolvedor.

Sobre Esta Tarefa

A configuração o servidor eXtreme Scale envolve especificar as propriedades do servidor e incluir essas propriedades no arquivo `server.xml` do Perfil do Liberty no diretório *`wlp_home`*`/usr/servers/`*`your_server_name`*. Esta definição de servidor é necessária para executar o eXtreme Scale no Perfil do Liberty.

Este procedimento também engloba incluir a configuração do arquivo de propriedade de servidor do eXtreme Scale, `xsServerConfig.xml`, no arquivo `server.xml`.

Procedimento

1. Gere o arquivo de propriedades do servidor eXtreme Scale.
   a. Clique em **Arquivo** > **Novo** > **Outro**.
   b. Expanda **WebSphere eXtreme Scale** e selecione **Arquivo de Configuração do Servidor de Contêiner**. Clique em **Avançar**. A janela Arquivo de Configuração do Servidor do eXtreme Scale é exibida.
   c. Clique em **Procurar** para especificar onde o Perfil do Liberty é instalado. Em seguida, selecione a definição do servidor Perfil do Liberty a qual você deseja configurar para seus servidores eXtreme Scale. Clique em **Avançar**. A janela Configuração do Servidor Geral é exibida.
   d. Conclua a configuração do servidor. Clique em **Avançar**. A janela Configuração do Servidor de Contêiner é exibida.
   e. Conclua a configuração do servidor de contêiner. Clique em **Avançar**.
   f. Se você incluiu a configuração do servidor de catálogo, outra janela será exibida, na qual você especifica as configurações do servidor de catálogo. Clique em **Avançar**. A janela Configuração de Criação do Log do Servidor é exibida.
   g. Preencha as páginas de informações de criação de log e clique em **Avançar** até a janela Configuração de Segurança ser exibida.
   h. Opcional: Especifique o local do arquivo `objectGridSecurity.xml`, que descreve as propriedades de segurança que são comuns a todos os servidores, incluindo servidores de catálogo e servidores de contêiner. Um exemplo das propriedades de segurança definidas é a configuração do autenticador, que representa o registro do usuário e o mecanismo de autenticação. O nome do arquivo especificado para esta propriedade deve estar em um formato de URL, tal como `file:///tmp/og/objectGridSecurity.xml`.
   i. Clique em **Concluir**.

   Um arquivo de configuração é gerado no perfil do Liberty.

2. Inclua a configuração do arquivo de propriedades do servidor eXtreme Scale no arquivo `server.xml`.
   a. Abra a visualização Servidores no Eclipse.
   b. Expanda o Servidor Liberty para localizar o arquivo XML de configuração do servidor.
   c. Dê um clique duplo na entrada para a configuração do servidor para abrir o arquivo.
   d. Clique em **Incluir** e selecione **Incluir** para incluir uma instrução include no arquivo `server.xml`. Clique em **OK**.
   e. Em Detalhes da Inclusão, clique em **Procurar**. A janela Procurar Arquivo Include é exibida.
   f. Selecione **xsServerConfig.xml**, para incluir as definições de configuração do servidor que você criou na etapa 1. Clique em **OK**.

O que Fazer Depois

O arquivo de configuração do servidor eXtreme Scale, `xsServerConfig.xml`, agora está incluído no arquivo `server.xml` do Perfil do Liberty. Agora, você está pronto para iniciar o servidor Perfil do Liberty, no qual seus servidores eXtreme Scale serão executados.

Criando um Projeto de Pacote Configurável OSGi para Desenvolvimento de Grade do eXtreme Scale

Para utilizar o Eclipse como o ambiente de desenvolvimento para seus servidores WebSphere eXtreme Scale no Perfil do Liberty, você deve criar um projeto Eclipse na estrutura Open Services Gateway initiative (OSGi) suportada.

Procedimento

1. Crie o projeto de pacote configurável OSGi no Eclipse.
   a. Clique em **Arquivo** > **Novo** > **Project**. A janela "Selecionar um Assistente" é exibida.
   b. Expanda a pasta WebSphere eXtreme Scale e selecione o projeto **Grade de Objeto**. A janela "Projeto da Grade de Objeto" é exibida.
   c. Clique em **Incluir** e insira um nome de mapa de apoio para incluir o mapa da grade do objeto para a qual você deseja concluir atividades de desenvolvimento. É possível inserir diversos mapas nesta página. Clique em **Avançar**.
   d. Especifique parâmetros da grade do objeto para cada mapa que você inseriu. Clique em **Avançar**.
   e. Especifique os parâmetros de implementação e clique em **Concluir**.

   O projeto de pacote configurável OSGi é criado e você poderá acessar as APIs do eXtreme Scale para concluir as atividades de desenvolvimento no Perfil do Liberty. O pacote configurável inclui o arquivo `gridBlueprint.xml`. Esse arquivo inclui o local dos arquivos de configuração do eXtreme Scale, `objectGrid.xml` e `gridDeployment.xml`. Esses arquivos de configuração incluem o mapa ou mapas que você criou na etapa c.
2. Exporte o projeto de pacote configurável e coloque o pacote configurável na pasta da grade. Você deve exportar o projeto para implementar aplicativos eXtreme Scale no Perfil do Liberty. Ao exportar o projeto, ele é exportado como um arquivo Java archive (JAR) do pacote configurável para a pasta *Liberty_profile_Server_Definition*/grids.

a. Clique com o botão direito do mouse no projeto que você acabou de criar e selecione **Exportar** > **Pacote Configurável OSGi ou Fragmento**. A janela Exportação do Aplicativo OSGi é exibida.
b. Especifique onde você deseja exportar o arquivo JAR do pacote configurável. Clique em **Concluir**.

Migrando uma Replicação de Memória para Memória ou uma Sessão de Banco de Dados do WebSphere Application Server para Usar Gerenciamento de Sessões do WebSphere eXtreme Scale

Java

É possível migrar qualquer sessão de replicação memória-a-memória ou sessão de banco de dados anteriormente configurada para usar gerenciamento de sessões do WebSphere eXtreme Scale.

Antes de Iniciar

- Para obter suporte de sessão para aplicativos clientes em execução no WebSphere Application Server no cluster, o WebSphere eXtreme Scale deve ser instalado sobre as implementações de nós do WebSphere Application Server, incluindo o nó do gerenciador de implementação. Consulte Instalando o WebSphere eXtreme Scale ou o WebSphere eXtreme Scale Client com WebSphere Application Server.
- Um ambiente de grade do WebSphere eXtreme Scale que consiste em um ou mais servidores de catálogos e contêineres deve ser iniciado. Para obter informações adicionais, consulte Iniciando e Parando Servidores Independentes.

  Nota: Se você não vir o WebSphere eXtreme Scale, então seu perfil do WebSphere Application Server não foi aumentado para o WebSphere eXtreme Scale. Para obter informações adicionais, consulte Criando e Alterando Perfis para o WebSphere eXtreme Scale.
- Se os servidores de catálogos em seu domínio de serviço de catálogo tiverem Secure Sockets Layer (SSL) ativado ou se desejar usar SSL para um domínio de serviço de catálogo com SSL suportado, então, a segurança global deve estar ativada no console administrativo do WebSphere Application Server. Você requer SSL para um servidor de catálogos configurando o atributo transportType para SSL-Required no Arquivo de Propriedades do Servidor. Para obter informações adicionais, consulte Definições de Configurações Globais.

Sobre Esta Tarefa

As etapas nesse cenário são para a Versão 8.5 do console administrativo do WebSphere Application Server. Estas informações podem variar ligeiramente dependendo da versão do WebSphere Application Server que está sendo usada.

Nota: O WebSphere eXtreme Scale Versão 8.6 não é suportado nas versões do WebSphere Application Server anteriores à Versão 7.0.

Tomando Nota de Definições de Configuração Anterior no Console Administrativo do WebSphere Application Server

Java

Como arte da migração para uma sessão do WebSphere eXtreme Scale, você deve tomar nota de suas definições de configuração anterior no console administrativo do WebSphere Application Server. Ao migrar para uma sessão do WebSphere eXtreme Scale, as definições de configuração precisam refletir o que já havia configurado para sua sessão de banco de dados ou de memória para memória.

Sobre Esta Tarefa

Há configurações específicas no console administrativo do WebSphere Application Server das quais deve tomar nota. Você precisará desses valores ao atualizar o arquivo `splicer.properties`. As etapas nesse procedimento são para a Versão 8.5 do console administrativo do WebSphere Application Server. Estas informações podem variar ligeiramente dependendo da versão do WebSphere Application Server que está sendo usada.

Nota: O WebSphere eXtreme Scale Versão 8.6 não é suportado nas versões do WebSphere Application Server anteriores à Versão 7.0.

Procedimento

1. Inicie o console administrativo do WebSphere Application Server.
   - Se tiver configurado anteriormente as definições no nível do servidor, então, acesse:
     a. **Servidores>Tipos de Servidores>WebSphere Application Servers**
     b. Na área **Servidores de Aplicativos**, selecione **seu nome do servidor**
     c. Na área **Configurações do Contêiner**, clique em **Gerenciamento de Sessões**
   - Se tiver configurado anteriormente as definições no nível do aplicativo, então, acesse:
     a. **Aplicativos > Todos os Aplicativos**.
     b. Na área **Servidores de Aplicativos**, selecione **seu nome do aplicativo**.
     c. Na área **Propriedades do Módulo da Web**, clique em **Gerenciamento de Sessões**
2. Em **Propriedades Gerais**, selecione a caixa de seleção **Permitir Estouro**.
3. Na área **Propriedades Gerais**, tome nota as configurações do WebSphere Application Server. Esse valores serão necessários para atualizar as propriedades no arquivo `splicer.properties`.

Tabela 3. Definições de Configuração para Atualizar o Arquivo splicer.properties

Configurações no console de administração do WebSphere Application Server	Propriedades para atualizar no arquivo splicer.properties
Ativar cookies	useCookies
Ativar regravação da URL	useURLEncoding
Contagem Máxima de Sessões na Memória	sessionTableSize

4. Na área **Propriedades Gerais**, se a caixa de seleção **Ativar Cookies** estiver selecionada, então, clique-a e tome nota das configurações do WebSphere Application Server. Esse valores serão necessários para atualizar as propriedades no arquivo `splicer.properties`.

Tabela 4. Definições de Configuração para as Propriedades no Arquivo splicer.properties

Configurações no console de administração do WebSphere Application Server	Propriedades para atualizar no arquivo splicer.properties
Domínio de Cookies	cookieDomain
Caminho de Cookies	cookiePath

5. Clique em **Gerenciamento de Sessões** e na área **Propriedades Adicionais**, clique em **Configurações de Ambiente Distribuído**.
6. Na área **Sessões Distribuídas**, altere sua configuração de banco de dados ou de replicação memória-a-memória para **Nenhuma**.
7. Clique em **Propriedades de Ajuste Customizadas** e tome nota das configurações do WebSphere Application Server. Esse valores serão necessários para atualizar as propriedades no arquivo `splicer.properties`

Tabela 5. Definições de Configuração para as Propriedades no Arquivo splicer.properties

Configurações no console de administração do WebSphere Application Server	Propriedades para atualizar no arquivo splicer.properties
Freqüência de Gravação	replicationInterval
Gravar Conteúdo	fragmentedSession

O que Fazer Depois

Em seguida, crie o domínio de serviço de catálogo para uma sessão do WebSphere eXtreme Scale.

Criando o Domínio de Serviço de Catálogo para Gerenciamento de Sessões do WebSphere eXtreme Scale

Java

Como parte da migração para uma sessão do WebSphere eXtreme Scale, você deve criar um domínio de serviço de catálogo no console administrativo do WebSphere Application Server.

Sobre Esta Tarefa

As etapas nesse procedimento são para a Versão 8.5 do console administrativo do WebSphere Application Server. Estas informações podem variar ligeiramente dependendo da versão do WebSphere Application Server que está sendo usada.

Nota: O WebSphere eXtreme Scale Versão 8.6 não é suportado nas versões do WebSphere Application Server anteriores à Versão 7.0.
Crie o domínio de serviço de catálogo para o WebSphere eXtreme Scale no console administrativo do WebSphere Application Server. Para obter informações adicionais, consulte Criando Domínios do Serviço de Catálogo no WebSphere Application Server.

Procedimento

1. Inicie o console administrativo do WebSphere Application Server.
2. No menu na parte superior, clique em **Administração do Sistema > WebSphere eXtreme Scale > Domínios de Serviços de Catálogo**

Nota: Se você não vir o WebSphere eXtreme Scale, então seu perfil do WebSphere Application Server não foi aumentado para o WebSphere eXtreme Scale. Para obter informações adicionais, consulte Criando e Alterando Perfis para o WebSphere eXtreme Scale.

3. Clique em **Novo**.
4. Especifique um nome para o serviço de catálogo na caixa **Nome**.
5. Na área **Servidores de Catálogos**, escolha **Servidor Remoto** e especifique o local ou o nome do servidor remoto na caixa.
6. Especifique um número de porta na caixa **Porta do Listener**.
7. Clique em **Aplicar** ou em **OK** e salve a configuração.

O que Fazer Depois

Em seguida, use as definições de configuração anteriores anotadas no console de administração do WebSphere Application Server para associar um aplicativo ou um servidor de aplicativos ao gerenciamento de sessões do WebSphere eXtreme Scale.

Configurando o WebSphere eXtreme Scale para Usar suas Definições de Configuração Anteriores

Java

Usando suas definições de configuração anteriores anotadas no console de administração do WebSphere Application Server, você deve usar essas configurações para associar um aplicativo ou um servidor de aplicativos ao gerenciamento de sessões do WebSphere eXtreme Scale.

Sobre Esta Tarefa

As etapas nesse procedimento são para a Versão 8.5 do console administrativo do WebSphere Application Server. Estas informações podem variar ligeiramente dependendo da versão do WebSphere Application Server que está sendo usada.

Nota: O WebSphere eXtreme Scale Versão 8.6 não é suportado nas versões do WebSphere Application Server anteriores à Versão 7.0.

Procedimento

- Se desejar configurar um aplicativo para que seja associado ao gerenciamento de sessões do WebSphere eXtreme Scale, siga estas etapas:
  1. Inicie o console administrativo do WebSphere Application Server.
  2. No menu na parte superior, clique em **Aplicativos > Todos os Aplicativos**.
  3. Na área **Servidores de Aplicativos**, selecione **nome do aplicativo**.
  4. Na área de propriedades **Módulo da Web**, clique em **Gerenciamento de Sessões**
  5. Clique em **Configurações de gerenciamento de sessões do eXtreme Scale**.
  6. Se você não vir o WebSphere eXtreme Scale, então seu perfil do WebSphere Application Server não foi aumentado para o WebSphere eXtreme Scale. Para obter informações adicionais, consulte Criando e Alterando Perfis para o WebSphere eXtreme Scale.
  7. Para configurar um aplicativo para o WebSphere eXtreme Scale em um ambiente independente, siga estas etapas:

a. Na lista **Gerenciar persistência de sessão por**, selecione **Grade de dados do eXtreme Scale remoto**
b. Selecione o domínio de serviço de catálogo criado na lista.
c. Clique em **Procurar** para selecionar a grade.

8. Clique em **Aplicar** ou em **OK** e salve a configuração.
9. Um novo arquivo splicer.properties é criado para esse aplicativo. O local do arquivo `splicer.properties` é o valor da nova propriedade `{application name},com.ibm.websphere.xs.sessionFilterProps`. Para localizar a propriedade customizada, acesse **Administração do Sistema> Célula** e clique em **Propriedades Customizadas**.
10. Atualize o arquivo `splicer.properties` com os valores obtidos em "Tomando Nota de Definições de Configuração Anterior no Console Administrativo do WebSphere Application Server" na página 214.
11. Reinicie os processos do servidor de aplicativos.

Nota: Altere `splicer.properties` no nível do Deployment Manager para que as propriedades sejam sincronizadas para o agente do nó. Se você atualizar `splicer.properties` no nível do nó, então, o Deployment Manager irá sobrescrever o arquivo `splicer.properties` na próxima sincronização.

Nota: Se você voltar ao gerenciamento de sessões do banco de dados e, em seguida, retornar ao gerenciamento de sessões do WebSphere eXtreme Scale, o arquivo `splicer.properties` será recriado para que quaisquer mudanças feitas sejam substituídas. Para uma discussão sobre o processo de sincronização de arquivo do Deployment Manager para o Notes e sobre o que é alterado, consulte Sincronização de Arquivos no Gerenciamento de Sistemas.

- Se desejar configurar um servidor de aplicativos para que seja associado ao gerenciamento de sessões do WebSphere eXtreme Scale, siga estas etapas:
  1. Inicie o console administrativo do WebSphere Application Server.
  2. No menu na parte superior, clique em **Servidores > Tipos de Servidores > WebSphere Application Servers**.
  3. Na área **Servidores de Aplicativos**, selecione **seu nome do servidor**.
  4. Na área **Configurações do Contêiner**, clique em **Gerenciamento de Sessões**
  5. Clique em **Configurações de gerenciamento de sessões do eXtreme Scale**

     Nota: Se você não vir o WebSphere eXtreme Scale, então seu perfil do WebSphere Application Server não foi aumentado para o WebSphere eXtreme Scale. Para obter informações adicionais, consulte Criando e Alterando Perfis para o WebSphere eXtreme Scale.
  6. Para configurar um servidor de aplicativos para o WebSphere eXtreme Scale em um ambiente independente, siga estas etapas:
     a. Na lista **Gerenciar persistência de sessão por**, selecione **Grade de dados do eXtreme Scale remoto**
     b. Selecione o domínio de serviço de catálogo criado na lista.
     c. Clique em **Procurar** para selecionar a grade.
  7. Clique em **Aplicar** ou em **OK** e salve a configuração.
  8. Um novo arquivo splicer.properties é criado para esse aplicativo. O local do arquivo splicer.properties é o valor da nova propriedade `com.ibm.websphere.xs.sessionFilterProps`. Para localizar a propriedade customizada, acesse **Servidores > Tipos de Servidores > WebSphere Application Servers**.

9. Na área **Servidores de Aplicativos**, selecione **seu nome do servidor**.
10. Na área **Infraestrutura do Servidor**, selecione **Propriedades Customizadas**.
11. Atualize o arquivo `splicer.properties` com os valores obtidos em "Tomando Nota de Definições de Configuração Anterior no Console Administrativo do WebSphere Application Server" na página 214.
12. Reinicie os processos do servidor de aplicativos.

Nota: Altere `splicer.properties` no nível do Deployment Manager para que as propriedades sejam sincronizadas para o agente do nó. Se você atualizar `splicer.properties` no nível do nó, então, o Deployment Manager irá sobrescrever o arquivo `splicer.properties` na próxima sincronização.

Nota: Se você voltar ao gerenciamento de sessões do banco de dados e, em seguida, retornar ao gerenciamento de sessões do WebSphere eXtreme Scale, o arquivo `splicer.properties` será recriado para que quaisquer mudanças feitas sejam substituídas. Para uma discussão sobre o processo de sincronização de arquivo do Deployment Manager para o Notes e sobre o que é alterado, consulte Sincronização de Arquivos no Gerenciamento de Sistemas.

Resultados

Agora, você alterou suas definições de configuração anteriores para um gerenciamento de sessões de memória para memória ou de banco de dados com gerenciamento de sessões do WebSphere eXtreme Scale.

Cenário: Usando o WebSphere eXtreme Scale como um Provedor de Cache Dinâmico

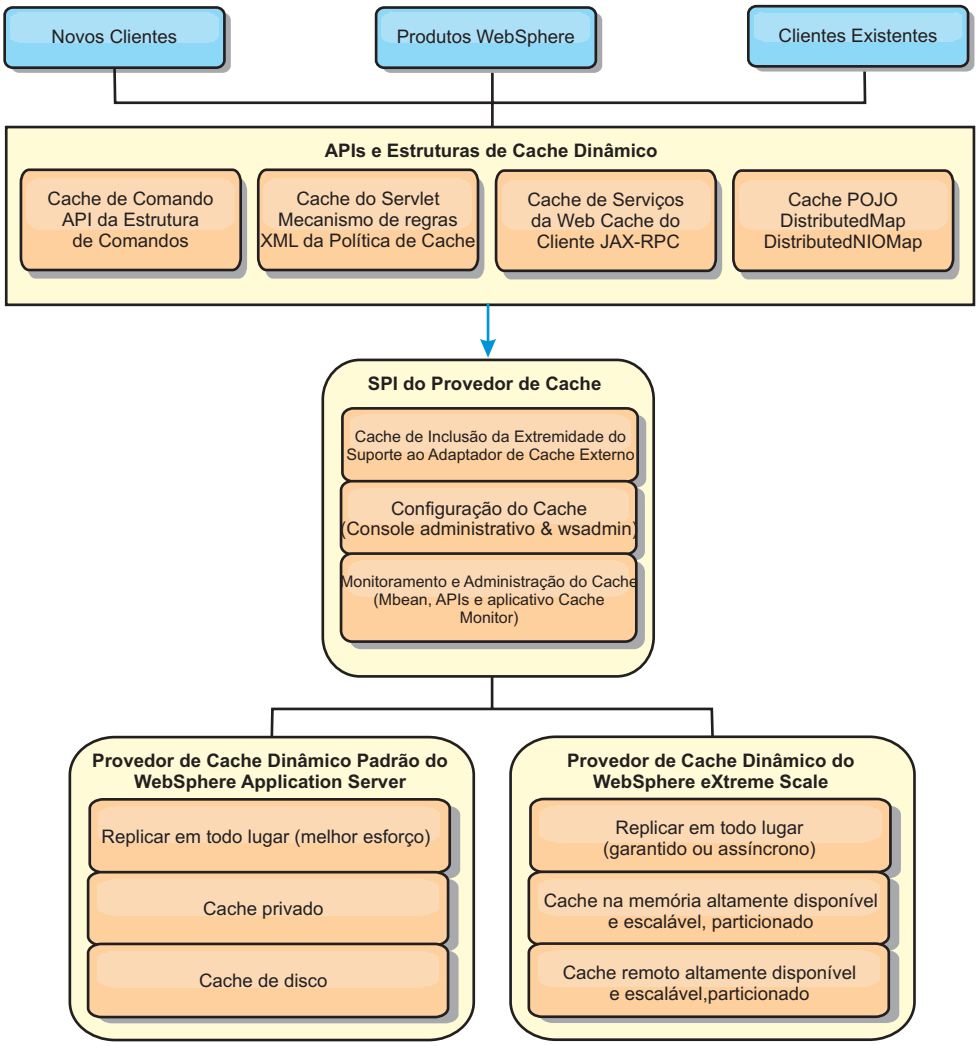
O WebSphere Application Server fornece um serviço de Cache Dinâmico disponível para os aplicativos Java EE implementados. Esse serviço é usado para armazenar dados de negócios, HTML gerado, saída de comando, etc., em cache. Inicialmente, o único provedor para o serviço de Cache Dinâmico era o provedor de cache dinâmico padrão integrado ao WebSphere Application Server. Hoje os clientes também podem especificar o WebSphere eXtreme Scale para ser o provedor de cache para qualquer instância de cache fornecida. Isso permite que os aplicativos que usam o serviço de Cache Dinâmico, usem os recursos e capacidades de desempenho do WebSphere eXtreme Scale.

Sobre Esta Tarefa

Visão Geral do Provedor de Cache Dinâmico

O WebSphere Application Server fornece um serviço de Cache Dinâmico que está disponível para aplicativos implementados do Java EE. Esse serviço é usado para armazenar dados em cache, como saída de servlet, JSP ou comandos, assim como dados de objetos especificados de forma programática em um aplicativo corporativo usando APIs de DistributedMap.

Inicialmente, o único provedor de serviços para o serviço de Cache Dinâmico era o mecanismo de cache dinâmico padrão integrado ao WebSphere Application Server. Hoje, clientes também podem especificar o WebSphere eXtreme Scale para ser o provedor de cache para qualquer instância de cache fornecida. Ao configurar esse recurso, é possível ativar aplicativos que usam o serviço de Cache Dinâmico para usar os recursos e as capacidades de desempenho do WebSphere eXtreme Scale.



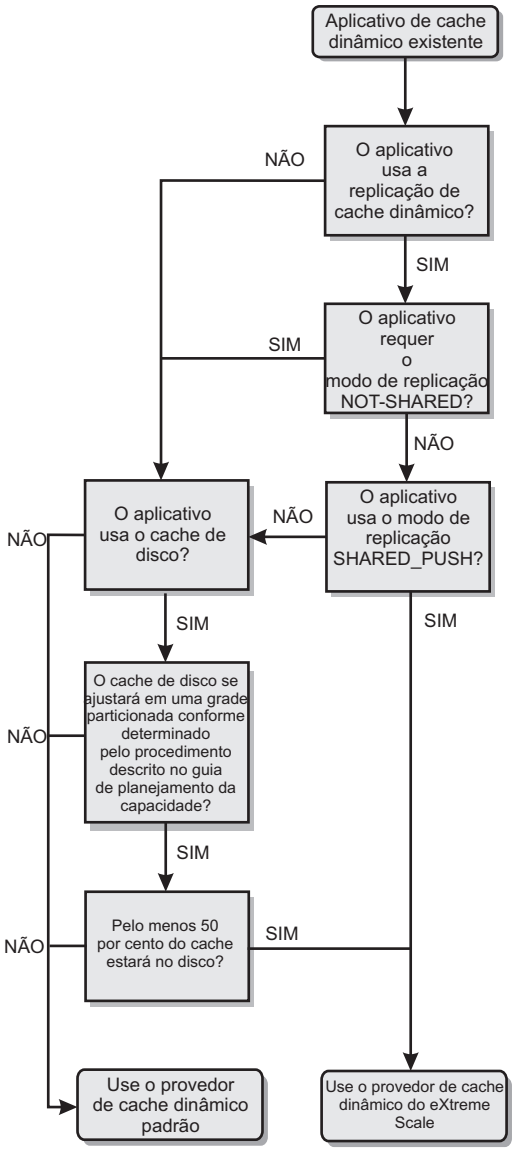
É possível instalar e configurar o provedor de cache dinâmico conforme descrito em Configurando a Instância de Cache Dinâmico Padrão (baseCache).

Decidindo como Usar o WebSphere eXtreme Scale

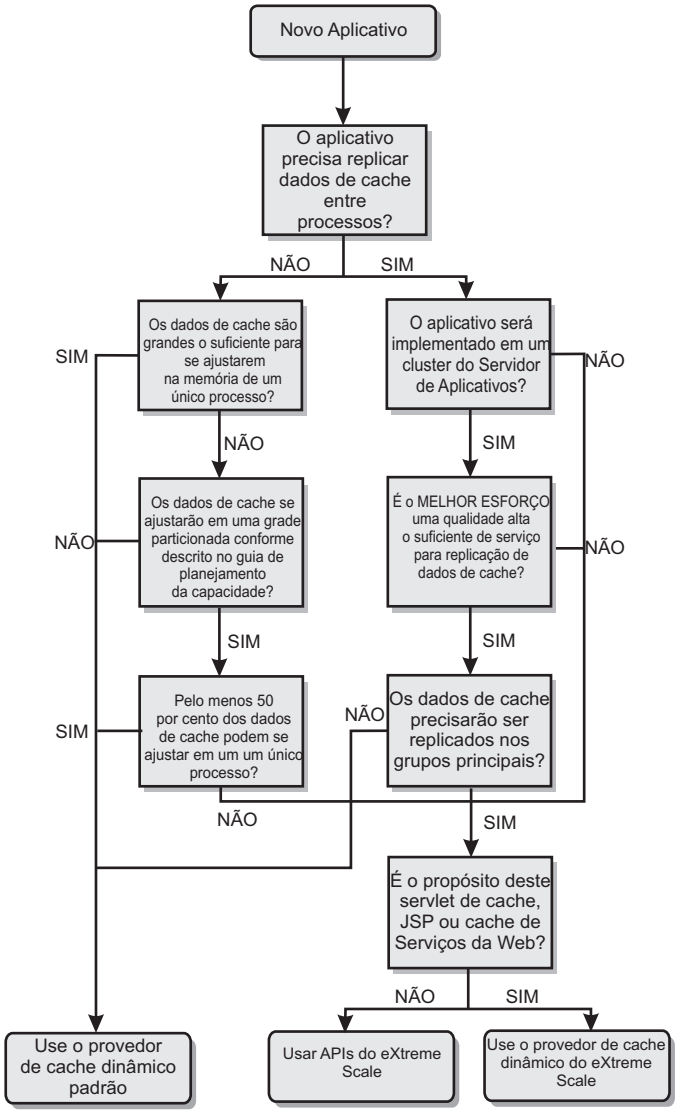
Os recursos disponíveis no WebSphere eXtreme Scale aumentam de forma significativa os recursos distribuídos do serviço de Cache Dinâmico além do que é oferecido pelo provedor de cache dinâmico padrão e o serviço de replicação de dados. Com o eXtreme Scale, é possível criar caches que são verdadeiramente distribuídos entre múltiplos servidores, em em de simplesmente replicados e sincronizados entre os servidores. Também, os caches do eXtreme Scale são transacionais e altamente disponíveis, garantindo que cada servidor veja o mesmo conteúdo para o serviço de cache dinâmico. O WebSphere eXtreme Scale oferece uma qualidade de serviço mais alta para a replicação de cache via DRS.

Porém, essas vantagens não significam que o provedor de cache dinâmico doeXtreme Scale seja a escolha certa para cada aplicativo. Use as árvores de decisão e matriz e comparação de recursos abaixo para determinar qual tecnologia se encaixa melhor no seu aplicativo.

Árvore de Decisão para Migrar Aplicativos de Cache Dinâmico Existente



Árvore de Decisão para Escolher um Provedor de Cache para Novos Aplicativos



Comparação de Recursos

Tabela 6. Comparação de Recursos

Recursos do cache	Provedor padrão	Provedor do eXtreme Scale	eXtreme Scale API
Cache na memória, local	Sim	via capacidade de Cache Local	via capacidade de Cache Local
Armazenamento em cache distribuído	via DRS	Sim	Sim
Linearmente escalável	Não	Sim	Sim
Replicação confiável (síncrona)	Não	Sim	Sim
Estouro de disco	Sim	N/D	N/D

Tabela 6. Comparação de Recursos (continuação)

Recursos do cache	Provedor padrão	Provedor do eXtreme Scale	eXtreme Scale API
Despejo	LRU/TTL/baseado em heap	LRU/TTL (por partição)	LRU/TTL (por partição)
Invalidação	Sim	Sim	Sim
Relacionamentos	Relacionamentos de dependência / ID do modelo	Sim	No (outros relacionamentos são possíveis)
Consultas sem chave	Não	Não	via Consulta e índice
Integração de backend	Não	Não	via Carregadores
Transacional	Não	Sim	Sim
Armazenamento baseado em chave	Sim	Sim	Sim
Eventos e listeners	Sim	Não	Sim
Integração do WebSphere Application Server	Somente célula única	Célula múltipla	Célula independente
Suporte à Java Standard Edition	Não	Sim	Sim
Monitoramento e estatística	Sim	Sim	Sim
Segurança	Sim	Sim	Sim

Para obter uma descrição mais detalhada sobre como os caches distribuídos do eXtreme Scale funcionam, consulte o “Planejando a Topologia” na página 258.

Nota: Um cache distribuído do eXtreme Scale somente pode armazenar entradas nas quais ambos, a chave e o valor, implementam a interface java.io.Serializable.

Tipos de topologia

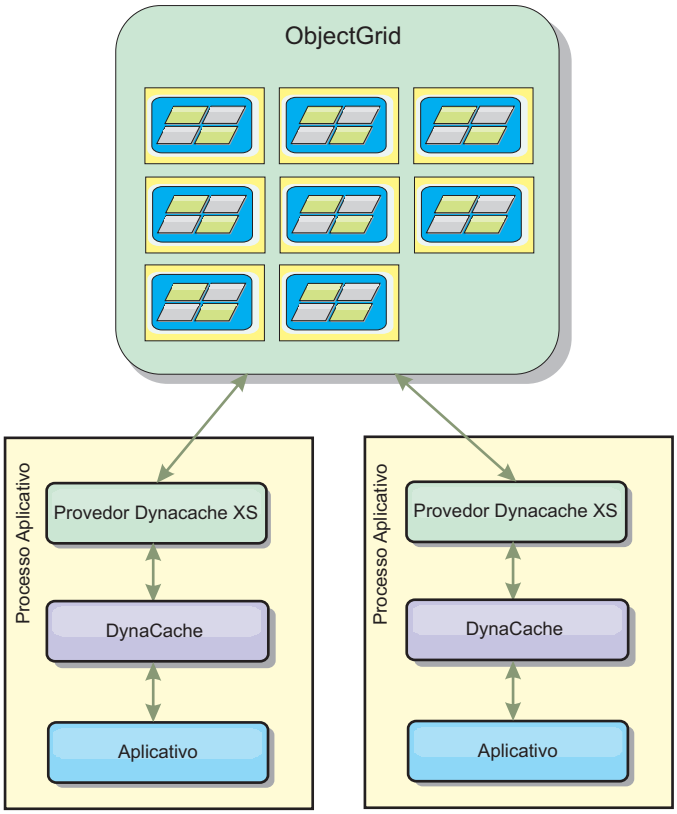
Reprovado: 8.6+ Os tipos de topologia local, integrado e integrado particionado foram descontinuados.

Um serviço de cache dinâmico criado com o eXtreme Scale como o provedor pode ser implementado em uma topologia remota.

Topologia Remota

A topologia remota elimina a necessidade de um cache de disco. Todos os dados em cache são armazenados fora dos processos do WebSphere Application Server. O WebSphere eXtreme Scale suporta processos de contêiner independentes para dados do cache. Esses processos de contêiner têm um gasto adicional mais baixo do que um processo do WebSphere Application Server e também não são limitados ao uso de uma Java Virtual Machine (JVM) particular. Por exemplo, os dados para um serviço de cache dinâmico que está sendo acessado por um processo do WebSphere Application Server de 32 bits poderiam ser alocados em um processo de contêiner do eXtreme Scale que estivesse executando em uma JVM de 64 bits. Isso permite aos usuários usar a capacidade de memória aumentada dos processos

de 64 bits para armazenamento em cache, sem incorrer um gasto adicional de 64 bits para os processos do servidor de aplicativos. A topologia remota é mostrada na seguinte imagem:



Mecanismo de Cache Dinâmico e Diferenças Funcionais do eXtreme Scale

Os usuários não devem observar uma diferença funcional entre os dois caches, exceto que os caches retornados pelo WebSphere eXtreme Scale não suportam a transferência de disco ou estatísticas e operações relacionadas ao tamanho do cache em memória.

Não haverá nenhuma diferença apreciável nos resultados retornados pela maioria das chamadas de API de Cache Dinâmico, independentemente de se o cliente está usando o provedor de cache dinâmico padrão ou o provedor de cache do eXtreme Scale. Para algumas operações não é possível emular o comportamento do mecanismo de cache dinâmico usando o eXtreme Scale.

Estatísticas do Cache Dinâmico

Dados estatísticos para um cache dinâmico do WebSphere eXtreme Scale podem ser recuperados usando o conjunto de ferramentas de monitoramento do eXtreme Scale. Consulte Monitoramento para obter mais informações.

Chamadas de MBean

O provedor de cache dinâmico do WebSphere eXtreme Scale não suporta o armazenamento em disco. Quaisquer chamadas de MBean relacionadas ao armazenamento em disco não funcionarão.

Mapeamento da Política de Replicação de Cache Dinâmico

A topologia remota do provedor de cache dinâmico do eXtreme Scale suporta uma política de replicação que corresponde mais proximamente à política SHARED_PULL e SHARED_PUSH_PULL (usando a terminologia usada pelo provedor de cache dinâmico padrão do WebSphere Application Server). Em um cache dinâmico do eXtreme Scale, o estado distribuído do cache é completamente consistente entre todos os servidores.

8.6+ Invalidação do Índice Global

É possível usar um índice global para melhorar a eficiência em grandes ambientes particionados; por exemplo, mais de 40 partições. Sem o recurso de índice global, o modelo de cache dinâmico e o processamento de invalidação de dependência devem enviar solicitações de agentes remotos a todas as partições, o que resulta em desempenho mais lento. Ao configurar um índice global, os agentes de invalidação são enviados somente a partições aplicáveis que contêm entradas de cache relacionadas ao ID de Modelo ou de Dependência. A melhoria de desempenho em potencial será maior em ambientes com um grande número de partições configuradas. É possível configurar um índice global usando os índices de ID de Dependência e de ID de Modelo, que estão disponíveis nos arquivos XML do descritor de objectGrid de cache dinâmico de exemplo, consulte “Configurando uma Grade de Dados Corporativos em um Ambiente Independente para Armazenamento em Cache Dinâmico” na página 226.

Segurança

Quando um cache está em execução em uma topologia remota, é possível que um cliente independente do eXtreme Scale conecte ao cache e afete o conteúdo da instância de cache dinâmica. É, portanto, importante que os servidores do WebSphere eXtreme Scale que contêm as instâncias de cache dinâmico residam em uma rede interna, atrás do que é tipicamente conhecido como a DMZ da rede.

Consulte a documentação do eXtreme Scale no “Visão Geral de Segurança” na página 304 se autenticação SSL ou do cliente for necessária.

Cache Local

Uma instância de cache dinâmico pode ser configurada para criar e manter um cache local, que irá residir localmente dentro da JVM do servidor de aplicativos e irá conter um subconjunto das entradas contidas na instância de cache dinâmico remota. É possível configurar uma instância de cache local usando um arquivo dynacache-nearCache-ObjectGrid.xml. Para obter informações adicionais, consulte “Configurando uma Grade de Dados Corporativos em um Ambiente Independente para Armazenamento em Cache Dinâmico” na página 226. Há também propriedades customizadas para ajustar o cache local, consulte Propriedades customizadas do cache dinâmico para obter informações adicionais.

Informações adicionais

- Redbook do Cache Dinâmico
- Documentação do Cache Dinâmico
  - WebSphere Application Server 7.0
- Documentação do DRS
  - WebSphere Application Server 7.0

Capacidade do Ambiente de Planejamento

Se você tiver um tamanho de conjunto de dados inicial e um tamanho de conjunto de dados projetado, é possível planejar a capacidade necessária para executar o WebSphere eXtreme Scale. Usando esses exercícios de planejamento, é possível implementar o WebSphere eXtreme Scale eficientemente para futuras mudanças e maximizar a elasticidade da grade de dados, o que não haveria com um cenário diferente, como um banco em memória ou outro tipo de banco de dados.

Configurando uma Grade de Dados Corporativos em um Ambiente Independente para Armazenamento em Cache Dinâmico

Copie e modifique estes arquivos de implementação e do descritor objectGrid para configurar uma grade corporativa para armazenamento em cache dinâmico. Esses arquivos são usados para iniciar a grade de dados corporativos.

Sobre Esta Tarefa

Quando o WebSphere eXtreme Scale é especificado como o provedor para uma instância de cache dinâmico do WebSphere Application Server, os servidores do WebSphere eXtreme Scale são iniciados em um ambiente independente ou em um ambiente do WebSphere Application Server, consulte Iniciando e Parando Servidores Independentes para obter informações adicionais. Esse processo requer o uso de arquivos de implementação e do descritor objectGrid que são usados para configurar a grade de dados corporativos. O armazenamento em cache dinâmico requer uma configuração específica. Portanto, diversos arquivos XML são entregues com o WebSphere eXtreme Scale que devem ser copiados, alterados (conforme necessário) e usados para iniciar a grade de dados corporativos. Esses arquivos podem ser usados no estado em que se encontram, mas estão sujeitos a mudança e, portanto, devem ser copiados para um local separado antes de serem alterados ou usados.

Nota: Dependendo de como o WebSphere eXtreme Scale foi instalado, esses arquivos estão localizados no diretório `was_root/optionalLibraries/ObjectGrid/dynacache/etc` para instalações com o WebSphere Application Server; ou, para uma instalação em um ambiente independente, esses arquivos estão localizados no diretório `wxs_install_root/ObjectGrid/dynacache/etc`.

Importante: É altamente recomendável que esses arquivos sejam copiados para algum outro local antes de serem ediados ou usados.

Arquivo descritor de cache dinâmico (dynacache-remote-deployment.xml)

Esse arquivo é o arquivo descritor de implementação para iniciar um servidor de contêiner para armazenamento em cache dinâmico, consulte Arquivo Descritor XML de Política de Implementação para obter informações adicionais. Apesar de esse arquivo poder ser usado no estado em que se encontra, os elementos ou atributos a seguir são ocasionalmente alterados ou têm importância significativa:

- **mapSet name e map ref**

  O atributo **`name`** em mapSet e o valor definido para map ref não correspondem diretamente ao nome da instância de cache dinâmico configurado para o WebSphere Application Server e geralmente não são alterados. Se, no entanto, esses valores forem alterados, então, propriedades customizadas correspondentes devem ser incluídas na

configuração da instância de cache dinâmico. Para obter informações adicionais, consulte Customizando uma Instância de Cache Dinâmico com Propriedades Customizadas.

- **numberOfPartitions**

  Esse atributo pode ser alterado para representar o número apropriado de partições para sua configuração. Para obter informações adicionais, consulte "Capacidade do Ambiente de Planejamento" na página 226.

- **maxAsyncReplicas**

  Esse atributo deve ser alterado. Um cache dinâmico é geralmente usado em um modelo de cache lateral com um banco de dados ou alguma outra origem como o sistema de registro para os dados. Como resultado, configurar essa opção para OPTIMISTIC ou NONE acionará processamento de cache local, quando o tipo de transporte do eXtreme I/O (XIO) for usado e o espaço e as compensações de desempenho necessários para tornar os dados altamente disponíveis desincentivam o uso de replicação. No entanto, em alguns casos, alta disponibilidade é importante.

- **numInitialContainers**

  Esse atributo deve ser configurado para o número de contêineres que serão incluídos na inicialização inicial da grade de dados corporativos. Ter isso configurado corretamente auxiliará na localização e distribuição de partições pela grade de dados.

Arquivo XML descritor de ObjectGrid de cache dinâmico (dynacache-remote-objectgrid.xml)

Esse arquivo é o arquivo descritor de ObjectGrid recomendado para iniciar um servidor de contêiner para armazenamento em cache dinâmico, consulte Arquivo XML descritor do ObjectGrid para obter informações adicionais. Ele está configurado para executar com o tipo de transporte eXtreme I/O (XIO) usando eXtreme Data Formatting (XDF). Além disso, os índices do ID de Dependência e do ID do Modelo são configurados para usarem um Índice Global, o que melhora o desempenho de invalidação. Apesar de esse arquivo poder ser usado no estado em que se encontra, os elementos ou atributos a seguir são ocasionalmente alterados ou têm importância significativa.

- **objectGrid name e backingMap name**

  Os atributos **name** nos elementos objectGrid e backingMap não correspondem diretamente ao nome da instância de cache dinâmico configurado para a instância de cache do WebSphere Application Server e geralmente não precisam ser alterados. Se, no entanto, esses atributos forem alterados, então, as propriedades customizadas correspondentes devem ser incluídas na configuração da instância de cache dinâmico. Para obter informações adicionais, consulte Customizando uma Instância de Cache Dinâmico com Propriedades Customizadas.

- **copyMode**

  Configure esse atributo para COPY_TO_BYTES. Esse valor ativa eXtreme Data Format (XDF) quando o tipo de transporte eXtreme I/O (XIO) é usado. Alterar para algum outro copyMode irá desativar XDF e irá requerer a remoção do comentário do bean do plug-in ObjectTransformer.

- **lockStrategy**

Configure esse atributo para PESSIMISTIC. Configurar para OPTIMISTIC ou NONE acionará o processamento de cache local e deve ser acompanhado com propriedades do dynamic-nearcache-objectgrid.xml.

- **backingMapPluginCollections**

  Esse elemento é necessário. Os elementos filhos plug-in Evictor e plug-in MapIndex são ambos requeridos para armazenamento em cache dinâmico e não devem ser removidos.

- **GlobalIndexEnabled**

  DEPENDENCY_ID_INDEX e TEMPLATE_INDEX contêm uma propriedade GlobalIndexEnabled configurada para true. Configurar esse valor para false irá desativar o recurso de índice global para esses índices. É recomendável deixar esses índices globais ativados, a menos que esteja executando com um pequeno número de partições totais, por exemplo, menos de 40.

- **objectTransformer**

  Como esse arquivo descritor e objectGrid é destinado a ser executado no eXtreme Data Format (XDF), ele teve a linha comentada. Se desejar desativar XDF (alterando o valor de copyMode), então, você deve remover comentário desse plug-in.

Arquivo descritor de ObjectGrid de cache local dinâmico (dynacache-nearCache-ObjectGrid.xml)

Esse arquivo é o arquivo descritor de ObjectGrid recomendado para iniciar servidores de contêineres de grade para armazenamento em cache dinâmico quando um cache local é desejado. Ele está configurado para executar com o tipo de transporte eXtreme I/O (XIO) usando eXtreme Data Formatting (XDF). Além disso, os índices do ID de Dependência e do Modelo são configurados para usarem um Índice Global, o que melhora o desempenho de invalidação. O recurso de cache local de armazenamento em cache requer o uso do tipo de transporte eXtreme I/O (XIO).

Apesar de esse arquivo poder ser usado no estado em que se encontra, os elementos ou atributos a seguir são ocasionalmente alterados ou têm importância significativa:

- **objectGrid name e backingMap name**

  Esses valores nesse arquivo não correspondem diretamente ao nome da instância de cache dinâmico configurado para a instância de cache do WebSphere Application Server e geralmente não precisam ser alterados. Se, no entanto, esses valores forem alterados, então, propriedades customizadas correspondentes devem ser incluídas na configuração da instância de cache dinâmico.

- **lockStrategy**

  Essa propriedade deve ser configurada para OPTIMISTIC ou NONE para ativar um cace local. Nenhum outro lockingStrategy suporta um cache local.

- **nearCacheInvalidationEnabled**

  Essa propriedade deve ser configurada para true para ativar um cache local de armazenamento em cache dinâmico. Esse recurso usa pub-sub para fluir invalidações de instâncias de cache remoto para o cache local, mantendo-as em sincronização.

- **nearCacheLastAccessTTLSyncEnabled**

Essa propriedade deve ser configurada para true para ativar um cache local de armazenamento em cache dinâmico. Esse recurso usa pub-sub para fluir despejos de TTL das instâncias de cache remoto para o cache local, mantendo-as em sincronização.

- **copyMode**

  Essa propriedade backingMap é configurada para COPY_TO_BYTES. Esse valor ativa eXtreme Data Format (XDF) quando o tipo de transporte eXtreme I/O (XIO) é usado. Alterar para algum outro copyMode irá desativar XDF e irá requerer a remoção do comentário do bean do plug-in ObjectTransformer.

- **backingMapPluginCollections**

  MapIndexPlugins e Evictor são itens obrigatórios para armazenamento em cache dinâmico e não devem ser removidos.

- **GlobalIndexEnabled**

  DEPENDENCY_ID_INDEX e TEMPLATE_INDEX contêm uma propriedade GlobalIndexEnabled configurada para true. Configurar esse valor para false irá desativar o recurso de índice global para esses índices. É recomendável deixar esses índices globais ativados, a menos que esteja executando com um pequeno número de partições totais (< 40).

- **ObjectTransformer**

  Como esse arquivo é destinado a ser executado no eXtreme Data Format (XDF), esse plug-in teve a linha comentada. Se XDF for ser desativado (via mudança de copyMode), então, esse plug-in deve ter comentário removido.

Arquivo descrito de ObjectGrid de legado dinâmico (dynacache-legacy85-ObjectGrid.xml)

Esse arquivo é o arquivo descritor de ObjectGrid recomendado para iniciar um servidor de contêiner para armazenamento em cache dinâmico quando você escolheu um cache local. Apesar de esse arquivo poder ser usado no estado em que se encontra, os elementos ou atributos a seguir são ocasionalmente alterados ou têm importância significativa:

- **objectGrid name e backingMap name**

  Esses valores nesse arquivo não correspondem diretamente ao nome da instância de cache dinâmico configurado para a instância de cache do WebSphere Application Server e geralmente não precisam ser alterados. Se, no entanto, esses valores forem alterados, então, propriedades customizadas correspondentes devem ser incluídas na configuração da instância de cache dinâmico.

- **copyMode**

  Essa propriedade backingMap é configurada para COPY_ON_READ_AND_COMMIT. Esse valor não dever ser alterado.

- **lockStrategy**

  Essa propriedade backingMap é configurada para PESSIMISTIC. Esse valor não dever ser alterado.

- **backingMapPluginCollections**

  MapIndexPlugins, Evictor e Object Transformer são itens obrigatórios para armazenamento em cache dinâmico e não devem ser removidos.

Configurando uma Grade de Dados Corporativos para Armazenamento em Cache Dinâmico Usando um Perfil Liberty

Um servidor Perfil do Liberty pode hospedar uma grade de dados que armazena dados em cache para aplicativos que têm o cache dinâmico ativado.

Antes de Iniciar

- Instale o Perfil do Liberty. Para obter informações adicionais, consulte Instalando o Perfil do Liberty.
- Crie um aplicativo que utiliza o cache dinâmico. Para obter informações adicionais, consulte Configurando a Instância de Cache Dinâmico Padrão (baseCache).

Sobre Esta Tarefa

O Perfil do Liberty hospeda a grade de dados que suporta aplicativos ativados por cache dinâmico. Isso significa que o aplicativo é executado em uma instalação tradicional do WebSphere Application Server. Para os aplicativos a serem armazenados em cache pelo ambiente de tempo de execução do eXtreme Scale, você deve configurar o WebSphere Application Server para utilizar o serviço do domínio de catálogo e as propriedades do servidor que você especifica no Perfil do Liberty.

Procedimento

1. Ative o recurso de cache dinâmico do WebSphere eXtreme Scale.
   a. Inclua o recurso de cache dinâmico no arquivo `server.xml` do Perfil do Liberty. Por exemplo, o arquivo `server.xml` é semelhante à sub-rotina a seguir de código:

```
<featureManager>
<feature>eXtremeScale.server-1.1</feature>
<feature>eXtremeScale.dynacacheGrid-1.1</feature>
</featureManager>
```

2. Opcional: Configure propriedades no elemento `xsDynacacheGrid` no arquivo `server.xml`. É possível alterar qualquer uma das propriedades a seguir; no entanto, é recomendado que você aceite os valores padrão.

   `globalIndexDisabled`
   A invalidação de índice global melhora a eficiência da invalidação em um ambiente particionado grande; por exemplo, mais de 40 partições. Para obter informações adicionais, consulte "Invalidação de Dados" na página 278. Valor Padrão: `false`

   `objectGridName`
   Uma sequência que especifica o nome da grade de dados. Valor padrão: `DYNACACHE_REMOTE`

   `ojectGridTxTimeout`
   Especifica a quantidade de tempo em segundos permitida para que uma transação seja concluída. Se uma transação não for concluída nesse período de tempo, ela será marcada para rollback, resultando em uma exceção `TransactionTimeoutException`. Valor padrão: `30` (em segundos)

   `backingMapLockStrategy`
   Especifica se o gerenciador de bloqueio interno é utilizado sempre que uma entrada de mapa é acessada por uma transação. Configure esse atributo com um dos três valores: `OPTIMISTIC`, `PESSIMISTIC` ou `NONE`. Valor padrão: `PESSIMISTIC`

backingMapCopyMode

Especifica se uma operação get de uma entrada na instância BackingMap retorna o valor real, uma cópia do valor ou um proxy para o valor. Se você usar o eXtreme data format (XDF) para que Java e .NET possam acessar a mesma grade de dados, então, o modo de cópia padrão e obrigatório é COPY_TO_BYTES. Caso contrário, o modo de cópia COPY_ON_READ_AND_COMMIT será usado. Configure o atributo CopyMode para um dos cinco valores:

COPY_ON_READ_AND_COMMIT

O valor padrão é `COPY_ON_READ_AND_COMMIT`. Configure o valor como `COPY_ON_READ_AND_COMMIT` para garantir que um aplicativo nunca faça uma referência ao objeto de valor que está na instância BackingMap. Em vez disso, o aplicativo trabalha sempre com uma cópia do valor que está na instância de BackingMap. (Opcional)

COPY_ON_READ

Configure o valor como `COPY_ON_READ` para melhorar o desempenho sobre o valor `COPY_ON_READ_AND_COMMIT` eliminando a cópia que ocorre quando uma transação é confirmada. Para preservar a integridade dos dados do BackingMap, o aplicativo é confirmado para excluir cada referência para uma entrada após a transação ser confirmada. A configuração deste valor resulta em um método ObjectMap.get retornando uma cópia do valor ao invés de uma referência ao valor, o que garante que as alterações que são feitas pelo aplicativo no valor não afetem o elemento BackingMap até que a transação seja confirmada.

COPY_ON_WRITE

Configure o valor como `COPY_ON_WRITE` para melhorar o desempenho sobre o valor `COPY_ON_READ_AND_COMMIT` eliminando a cópia que ocorre quando o método ObjectMap.get é chamado pela primeira vez por uma transação para uma determinada chave. Em vez disso, o método ObjectMap.get retorna um proxy para o valor em vez de uma referência direta ao objeto de valor. O proxy assegura que não seja feita uma cópia do valor, a menos que o aplicativo chame um método set na interface do valor.

NO_COPY

Configure o valor como `NO_COPY` para permitir que um aplicativo nunca modifique um objeto de valor que é obtido utilizando um método ObjectMap.get na troca de aprimoramentos de desempenho. Configure o valor como `NO_COPY` para mapas associados com as entidades da API do EntityManager.

COPY_TO_BYTES

Configure o valor para `COPY_TO_BYTES` para melhorar a área de cobertura da memória para tipos complexos do Object e para melhorar o desempenho quando a cópia de um Object depender da serialização para ser feita. Se um Object não for Clonável ou um ObjectTransformer com um método copyValue eficiente não for fornecido, o mecanismo de cópia padrão deverá serializar e aumentar o objeto para fazer uma cópia. Com a configuração `COPY_TO_BYTES`, o aumento é executado apenas durante a leitura e a serialização é executada apenas durante a confirmação.

Valor padrão: `COPY_ON_READ_AND_COMMIT`

backingMapNearCacheEnabled
Configure o valor como `true` para ativar o cache local do cliente. Para usar um cache local, o atributo **lockStrategy** deve ser configurado como `NONE` ou `OPTIMISTIC`. Valor Padrão: `false`

mapSetNumberOfPartitions
Especifica o número de partições para o elemento mapSet. Valor padrão: `47`

mapSetMinSyncReplicas
Especifica o número mínimo de réplicas assíncronas para cada partição no mapSet. Os shards não são posicionados até que o domínio possa suportar o número mínimo de réplicas síncronas. Para suporte do valor minSyncReplicas, é necessário mais um servidor de contêiner do que o valor **minSyncReplicas**. Se o número de réplicas síncronas ficar abaixo do valor **minSyncReplicas**, grave as transações que não forem mais permitidas para essa partição. Valor padrão: `0`

mapSetMaxSyncReplicas
Especifica o número máximo de réplicas síncrona para cada partição no mapSet. Nenhuma outra réplica síncrona é colocada para um partição depois que o domínio atinge esse número de réplicas síncronas para essa partição específica. Incluir servidores de contêineres que podem suportar esse ObjectGrid pode resultar em um aumento no número de réplicas síncronas se o valor **maxSyncReplicas** ainda não tiver sido atingido. Valor padrão: `0`

mapSetNumInitialContainers
Especifica o número de servidores de contêiner que são necessárias antes de o posicionamento inicial ocorrer para os shards neste elemento mapSet. Este atributo pode ajudar a economizar a largura da banda da rede e do processo ao colocar uma grade de dados online a partir de uma inicialização a frio. Valor padrão: `1`

mapSetDevelopmentMode
Com este atributo, é possível influenciar onde um shard é posicionado em relação a seus shards peer. Quando o atributo developmentMode estiver configurado como `false`, nenhum dos dois shards da mesma partição será posicionado no mesmo computador. Quando o atributo developmentMode é configurado para `true`, os shards da mesma partição podem ser colocados na mesma máquina. Nos dois casos, nenhum dos dois shards da mesma partição chegam a ser posicionados no mesmo servidor de contêiner. Valor Padrão: `false`

mapSetReplicaReadEnabled
Se este atributo é configurado como `true`, pedidos de leitura são distribuídos entre uma partição primária e suas réplicas. Se o atributo replicaReadEnabled for `false`, os pedidos de leitura são roteados para o primário apenas. Valor Padrão: `false`

.

3. Configure WebSphere Application Server para apontar para o Perfil do Liberty.
   É possível conectar contêineres do WebSphere eXtreme Scale e aplicativos da web ativados para cache dinâmico a um domínio de serviço de catálogo que está em execução em uma outra célula do WebSphere Application Server ou como processos independentes. Como servidores de catálogos configurados remotamente não iniciam automaticamente na célula, você deve iniciar manualmente qualquer servidor de catálogos configurado remotamente.

Ao configurar um domínio do serviço de catálogo remoto, o nome de domínio deve corresponder ao nome de domínio que você especificou ao iniciar os servidores de catálogos remotos. O nome de domínio do serviço de catálogo padrão para servidores de catálogos independentes é `DefaultDomain`. Especifique um nome de domínio de serviço de catálogo com o parâmetro **`-domain`** do comando **`startOgServer`** ou **`startXsServer`**, um arquivo de propriedades de servidor ou com a API do servidor integrado. É necessário iniciar cada processo do servidor de catálogos remoto no domínio remoto com o mesmo nome de domínio. Para obter mais informações sobre como iniciar servidores de catálogos, consulte Iniciando um Serviço de Catálogo Independente que Utiliza o Transporte ORB.

Configurando as Instâncias de Cache Dinâmico

O Serviço de Cache Dinâmico do WebSphere suporta a criação de uma instância de cache padrão (baseCache) assim como de instâncias adicionais de servlet e de cache de objeto.

Sobre Esta Tarefa

A instância de cache padrão (baseCache) era inicialmente somente a instância de cache dinâmico suportada pelo WebSphere Application Server e é atualmente a instância de cache dinâmico pronta usada pelo WebSphere Commerce Suite. As instâncias de servlet e de cache de objeto adicionais foram incluídas em liberações posteriores do WebSphere Application Server e são configuradas em uma seção "instância de cache" separada do WebSphere Administrative Console.

Capítulo 3. Introdução

Depois de instalar o produto, será possível usar a introdução de amostra para testar a instalação e usar o produto pela primeira vez.

Tutorial: Introdução ao WebSphere eXtreme Scale

Após instalar o WebSphere eXtreme Scale em um ambiente independente, é possível usar o aplicativo de amostra de introdução para verificar sua instalação. O aplicativo de amostra de introdução é uma introdução para grades de dados na memória e corporativos. O aplicativo de amostra introduzido só é incluído em instalações integrais (cliente e servidor) do WebSphere eXtreme Scale.

Objetivos do aprendizado

- Aprenda sobre o arquivo XML descritor do ObjectGrid e os arquivos XML descritores da política de implementação que são usados para configurar seu ambiente.
- Inicie os servidores de catálogos e de contêineres com os arquivos de configuração.
- Aprenda sobre como desenvolver um aplicativo cliente nas linguagens de programação Java ou .NET. Aprenda como interoperar entre as linguagens de programação, criando uma grade de dados corporativos.
- Execute o aplicativo cliente para inserir dados na grade de dados.
- Monitore as grades de dados com o console da web.

Tempo Necessário

60 minutos

Tutorial de Introdução - Lição 1.1: Definindo Grades de Dados com Arquivos de Configuração

Os arquivos `objectgrid.xml` e `deployment.xml` são necessários para iniciar os servidores de contêiner.

A amostra usa os arquivos `objectgrid.xml` e `deployment.xml` que estão no diretório *wxs_install_root*`/ObjectGrid/gettingstarted/server/config`. Estes arquivos são transmitidos para os comandos iniciais para iniciar servidores de contêiner e um servidor de catálogos. O arquivo `objectgrid.xml` é o arquivo descritor XML do ObjectGrid. O arquivo `objectgrid.xml` é o arquivo descritor XML da política de implementação do ObjectGrid. Esses arquivos definem uma topologia distribuída.

Referências relacionadas:

Arquivo XML descritor do ObjectGrid
Para configurar o WebSphere eXtreme Scale, utilize um arquivo XML descritor do ObjectGrid e a API do ObjectGrid.

Arquivo Descritor XML de Política de Implementação
Para configurar uma política de implementação, utilize um arquivo XML do descritor da política de implementação.

Arquivo XML descritor do ObjectGrid

Um arquivo XML descritor de ObjectGrid é usado para definir a estrutura do ObjectGrid que será usada pelo aplicativo. Ele inclui uma lista de configurações de mapa de apoio. Esses mapas de apoio armazenam os dados de cache. O exemplo a seguir é um arquivo `objectgrid.xml` de amostra. As primeiras linhas do arquivo incluem o cabeçalho obrigatório de cada arquivo XML do ObjectGrid. O arquivo de exemplo a seguir define `Grid` ObjectGrid com os mapas de apoio `Map1` e `Map2`.

```
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
xmlns="http://ibm.com/ws/objectgrid/config">
 <objectGrids>
  <objectGrid name="Grid" txTimeout="30">
   <backingMap name="Map1" copyMode="COPY_TO_BYTES"  lockStrategy="PESSIMISTIC"
    nullValuesSupported="false"/>
   <backingMap name="Map2" copyMode="COPY_TO_BYTES"  lockStrategy="PESSIMISTIC"
    nullValuesSupported="false"/>
  </objectGrid>
 </objectGrids>
</objectGridConfig>
```

8.6+

- O valor de **`txtTmeout`** igual a `30` segundos é um bom valor de tempo limite para a maioria das grades de dados.
- O valor de **`copyMode`** igual a `COPY_TO_BYTES` é necessário quando você não fornece uma classe de objeto para serialização.
- O valor de **`lockStrategy`** igual a `PESSIMISTIC` é uma boa estratégia de bloqueio quando você estiver desenvolvendo inicialmente seu aplicativo de grade de dados. Com essa estratégia, você não está usando um cache local nem um plug-in de carregador. O aplicativo não manipula problemas de bloqueio.
- O valor de **`nullValuesSupported`** igual a `false` elimina o problema que pode ocorrer ao recuperar um valor de uma chave que é um valor nulo. Nessa situação, você não sabe se a chave existia. É possível eliminar esse problema não permitindo vaores nulos no mapa de apoio.

Arquivo Descritor XML de Política de Implementação

O arquivo XML descritor de política de implementação deve igualar-se com o arquivo XML ObjectGrid correspondente, o arquivo `objectgrid.xml`. No seguinte exemplo, as primeiras linhas do arquivo `deployment.xml` incluem o cabeçalho obrigatório de cada arquivo XML de política de implementação. O arquivo define o elemento **`objectgridDeployment`** para o ObjectGrid `Grid` definido no arquivo `objectgrid.xml`. Os BackingMaps `Map1` e `Map2` definidos no ObjectGrid `Grid` são incluídos no mapSet `mapSet`.

```
<deploymentPolicy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/deploymentPolicy
 ../deploymentPolicy.xsd"
 xmlns="http://ibm.com/ws/objectgrid/deploymentPolicy">
```

```
    <objectgridDeployment objectgridName="Grid">
        <mapSet name="mapSet" numberOfPartitions="13" minSyncReplicas="0"
maxSyncReplicas="1" >"1" >
            <map ref="Map1"/>
            <map ref="Map2"/>
        </mapSet>
    </objectgridDeployment>

</deploymentPolicy>
```

O atributo **numberOfPartitions** do elemento **mapSet** especifica o número de partições para o conjunto de mapas. Esse atributo é opcional; o valor padrão é 1. O valor do atributo deve ser apropriado para a capacidade previsat da grade de dados.

O atributo **minSyncReplicas** do elemento **mapSet** especifica o número mínimo de réplicas síncronas para cada partição no conjunto de mapas. Esse atributo é opcional; o padrão é 0. Shards primários e de réplica não são localizados até o domínio de serviço de catálogo poder suportar o número mínimo de réplicas síncronas. Para suportar o valor de **minSyncReplicas**, mais um servidor de contêiner do que o valor do atributo **minSyncReplicas** é necessário. Se o número de réplicas síncronas ficar abaixo do valor do atributo **minSyncReplicas**, as transações de gravação não serão mais permitidas para essa partição.

O atributo **maxSyncReplicas** do elemento **mapSet** é para especificar o número máximo de réplicas síncronas para cada partição no conjunto de mapas. Esse atributo é opcional; o padrão é 0. Nenhuma outra réplica síncrona é localizada para um partição após um domínio de serviço de catálogo atingir esse número de réplicas síncronas para essa partição específica. Incluir servidores de contêineres que podem suportar esse ObjectGrid pode resultar em um aumento no número de réplicas síncronas se o valor de **maxSyncReplicas** ainda não tiver sido atingido. A amostra configurou **maxSyncReplicas** para 1, o que significa que o domínio de serviço de catálogo localiza uma réplica síncrona no máximo. Se você iniciar mais de um servidor de contêiner, somente uma réplica síncrona será localizada nas instâncias do servidor de contêiner.

Ponto de verificação de lições

Nesta lição, você aprendeu:

- Como definir os mapas que armazenam os dados no arquivo descritor XML do ObjectGrid.
- Como usar o arquivo descritor XML de implementação para definir o número de partições e réplicas para a grade de dados.

Tutorial de Introdução - Módulo 2: Criar um Aplicativo Cliente

Grave aplicativos clientes para inserir, atualizar, excluir e recuperar dados de sua grade de dados. É possível usar o aplicativo de amostra para saber sobre como criar um aplicativo para seu ambiente.

Objetivos do aprendizado

Após concluir as lições neste módulo você saberá como fazer o seguinte:

- Java Desenvolver um aplicativo de cliente Java
- .NET 8.6+ Desenvolver um aplicativo cliente .NET

Tutorial de Introdução - Lição 2.1: Criando um Aplicativo de Cliente Java

Java

Para inserir, excluir, atualizar e recuperar dados de sua grade de dados, você deverá gravar um aplicativo cliente. A amostra de introdução inclui um aplicativo de cliente Java que pode ser usado para aprender sobre como criar seu próprio aplicativo cliente.

O arquivo `Client.java` no diretório *wxs_install_root*`/ObjectGrid/gettingstarted/client/src/` é o programa cliente que demonstra como se conectar a um servidor de catálogos, obter a instância do ObjectGrid e usar a API ObjectMap. A API ObjectMap armazena dados como pares de valores de chave e é ideal para armazenar em cache os objetos que não possuírem nenhum relacionamento envolvido. As etapas a seguir discutem o conteúdo do arquivo `Client.java`.

Se você precisar armazenar em cache objetos que possuem relacionamentos, use a API EntityManager .

1. Conexão com o serviço de catálogo por meio da obtenção de uma instância de ClientClusterContext

   Para se conectar a um servidor de catálogos, use o método connect da API ObjectGridManager. O método connect que é usado requer apenas o terminal do servidor de catálogos no formato de *`hostname:port`*. É possível indicar diversos terminais do servidor de catálogos separando a lista de valores de *`hostname:port`* com vírgulas. O fragmento de código a seguir demonstra como se conectar a um servidor de catálogos e obter uma instância de ClientClusterContext: **8.6+**

   ```
   ClientClusterContext ccc = ObjectGridManagerFactory.getObjectGridManager().connect(cep, null, null);
   ```

   Se as conexões com os servidores de catálogos forem bem-sucedidas, o método connect retorna uma instância de ClientClusterContext. A instância do ClientClusterContext é necessária para a obtenção do ObjectGrid da API do ObjectGridManager.

2. Obter uma instância do ObjectGrid.

   Para obter uma instância do ObjectGrid, use o método getObjectGrid da API do ObjectGridManager. O método getObjectGrid requer a instância de ClientClusterContext e o nome da instância da grade de dados. A instância do ClientClusterContext é obtida durante a conexão com o servidor de catálogos. O nome da instância de ObjectGrid é `Grid` que é especificado no arquivo `objectgrid.xml`. O fragmento de código a seguir demonstra como obter a grade de dados chamando o método getObjectGrid da API ObjectGridManager.

   ```
   ObjectGrid grid = ObjectGridManagerFactory.getObjectGridManager().getObjectGrid(ccc, "Grid");
   ```

3. Obter uma instância de Sessão.

   É possível obter uma Sessão da instância do ObjectGrid obtida. Uma instância da Sessão é necessária para obter a instância do ObjectMap e executar a demarcação da transação. O fragmento de código a seguir demonstra como obter uma instância da Sessão chamando o método getSession da API ObjectGrid.

   ```
   Session sess = grid.getSession();
   ```

4. Obter uma instância do ObjectGrid.

   Após obter uma Sessão, é possível obter uma instância do ObjectMap a partir de uma instância da Sessão chamando o método getMap da API de Sessão. Você deve transmitir o nome do mapa como parâmetro para o método getMap

para obter a instância de ObjectMap. O fragmento de código a seguir demonstra como obter o ObjectMap chamando o método getMap da API de Sessão.

8.6+

```
ObjectMap map1 = sess.getMap(mapName);
```

5. Use os métodos ObjectMap.

   Depois que uma instância ObjectMap for obtida, será possível usar a API ObjectMap. Lembre-se de que a interface ObjectMap é um mapa transacional e requer demarcação de transação usando os métodos begin e commit da API Session. Se não houver demarcação de transação explícita no aplicativo, as operações do ObjectMap serão executadas com transações de confirmação automática.

   - O fragmento de código a seguir demonstra como usar a API ObjectMap com uma transação de confirmação automática.

     8.6+

     ```
     map1.insert(key1, value1);
     ```

   - **8.6+** É possível executar uma transação em uma partição por vez ou em diversas partições. Para executar uma transação em uma única partição, use uma transação one-phase commit:

     ```
     sess.setTxCommitProtocol(TxCommitProtocol.ONEPHASE);
     sess.begin();
     map1.insert(k, v);
     sess.commit();
     ```

     Para executar uma transação em diversas partições, use uma transação two-phase commit:

     ```
     sess.setTxCommitProtocol(TxCommitProtocol.TWOPHASE);
     sess.begin();
     map1.insert(k, v);
     sess.commit();
     ```

6. Opcional: Feche a sessão. Após todas as operações de Sessão e ObjectMap serem concluídas, feche a sessão com o método Session.close(). A execução desse método retorna os recursos que estavam sendo usados pela sessão.

   ```
   sess.close();
   ```

   Como resultado, as chamadas de método getSession() subsequentes são retornadas mais rapidamente e menos objetos de Sessão ficam no heap.

Conceitos relacionados:

"Objetos de Armazenamento em Cache sem Relacionamentos Envolvidos (API ObjectMap)" na página 372
Os ObjectMaps são como Mapas Java que permitem que os dados sejam armazenados como pares chave-valor. Os ObjectMaps apresentam uma abordagem simples e intuitiva para o aplicativo que armazenará os dados. Um ObjectMap é ideal para o armazenamento em cache de objetos que não tenham nenhum relacionamento envolvido. Se os relacionamentos de objetos estiverem envolvidos, então você deve usar a API EntityManager.

Tarefas relacionadas:

"Introdução ao Desenvolvimento de Aplicativos" na página 254
Para iniciar o desenvolvimento de aplicativos WebSphere eXtreme Scale, você deve configurar seu ambiente de desenvolvimento, aprender sobre APIs que podem ser usadas e, em seguida, desenvolver e testar seu aplicativo.

"Tutorial: Armazenando Informações de Pedido nas Entidades" na página 9
Este tutorial do gerenciador de entidade mostra como utilizar o WebSphere eXtreme Scale para armazenar informações de pedido em um Web site. É possível criar um aplicativo Java Platform, Standard Edition 5 simples que utiliza um eXtreme Scale local e de memória. As entidades utilizam anotações e genéricos do Java SE 5.

Informações relacionadas:

Documentação da API

Ponto de verificação de lições:

Nesta lição, você aprendeu como criar um aplicativo cliente simples para executar operações da grade de dados.

Tutorial de Introdução - Lição 2.2: Criando um Aplicativo Cliente .NET

.NET

Para inserir, excluir, atualizar e recuperar dados de sua grade de dados, você deverá gravar um aplicativo cliente. A introdução de amostra inclui um aplicativo cliente .NET que pode ser usado para saber mais sobre a criação de seu próprio aplicativo cliente.

- Você deve ter o WebSphere eXtreme Scale Client para .NET instalado. Para obter informações adicionais, consulte Instalando o WebSphere eXtreme Scale Client para .NET.
- O arquivo de projeto para a amostra funciona com o Microsoft Visual Studio 2010 ou posterior. Se estiver usando uma versão anterior do Microsoft Visual Studio, deve criar seu próprio arquivo de projeto.

É possível usar o aplicativo de amostra de introdução do .NET para os propósito a seguir:

- Para verificar se você instalou o WebSphere eXtreme Scale Client para .NET corretamente.
- Para aprender como escrever aplicativos para o cliente .NET que se comunica com a grade de dados, de forma que seja possível criar aplicativos customizados. A amostra demonstra como se conectar a uma grade de dados em um servidor de catálogos remoto. O modo interativo demonstra como executar

transações manuais usando o mapa GridMapPessimisticTx. O modo da linha de comandos demonstra transações de confirmação automática com o mapa GridMapPessimisticAutoTx.

- Para aprender como interoperar com a amostra de introdução de Java. Ambos os aplicativos de amostra armazenam itens na grade de dados com pares TestKey/TestValue. A amostra de .NET tem os atributos ClassAlias e FieldAlias para criar identificadores exclusivos para serialização e desserialização. Se uma operação de inserção de chave for executada a partir do aplicativo de cliente Java, o cliente .NET pode obter o valor executando uma operação get na chave que foi inserida.

O aplicativo de amostra de introdução de .NET tem as limitações a seguir:

- Somente bloqueio pessimista é suportado.
- Operações two-phase commit não são suportadas. É possível confirmar operações somente para uma partição. Se você executar uma confirmação que envolva diversas partições, uma exceção MultiplePartitionWriteException resulta.
- A amostra não suporta valores nulos. A API .NET não permite valores nulos, mas você deve usar tipos anuláveis.

O arquivo de projeto `SimpleClient.csproj` está no diretório *net_client_home*/`sample/SimpleClient`. Esse arquivo de projeto é o programa cliente que demonstra como se conectar a um servidor de catálogos, obter a instância do ObjectGrid e usar a API ObjectMap. A API ObjectMap armazena dados como pares de valores de chave e é ideal para armazenar em cache os objetos que não possuírem nenhum relacionamento envolvido. As etapas a seguir contêm informações sobre o conteúdo de chave do arquivo `SimpleClient.csproj`. Também é possível verificar o arquivo de projeto em mais detalhes no Microsoft Visual Studio.

O tutorial demonstra o uso de IGridMapPessimisticTx, que é o mapa de transações manuais que é usado quando o aplicativo é executado em modo interativo. Se você usar o aplicativo o modo de linha de comando, o mapa IGridMapPessimisticAutoTx é usado.

1. Conecte-se ao serviço de catálogo obtendo uma instância IClientConnectionContext.

   Para conectar ao servidor de catálogos, use o método Connect da API IGridManager.

   ```
   IGridManager gm = GridManagerFactory.GetGridManager( );
   ICatalogDomainInfo cdi = gm.CatalogDomainManager.CreateCatalogDomainInfo( endpoint );
   ccc = gm.Connect( cdi, "SimpleClient.properties" );
   ```

   Se a conexão com o servidor de catálogos for bem-sucedida, o método Connect retorna uma instância IClientConnectionContext. A instância IClientConnectionContext é necessária para obter a grade de dados da API IGridManager.

2. Obter uma instância do ObjectGrid.

   Para obter uma instância ObjectGrid, use o método GetGrid da API IGridManager. O método GetGrid requer a instância IClientConnectionContext e o nome da instância da grade de dados. A instância IClientConnectionContext é obtida durante a conexão com o servidor de catálogos. O nome da instância da grade de dados é a grade especificada no arquivo `objectgrid.xml`.

   ```
   grid = gm.GetGrid( ccc, gridName );
   ```

3. Obtenha uma instância de mapa.

É possível obter uma instância de mapa chamando o método GetGridMapPessimisticTx da API IGrid. Passe o nome do mapa como parâmetro para o método GetGridMapPessimisticTx para obter a instância de mapa.

```
pessMap = grid.GetGridMapPessimisticTx<Object, Object>( mapName );
```

4. Use os métodos IGridMapPessimisticTx.

   Após uma instância de mapa ser obtida, é possível usar a API IGridMapPessimisticTx.

   O fragmento de código a seguir demonstra como usar a API IGridMapPessimisticTx.

   - Para iniciar uma transação com a API IGridMapPessimisticTx, você deve chamar o método map.Transaction.Begin(). Esse método começa com uma nova transação na qual é possível executar operações.

     ```
     case "begin":
        map.Transaction.Begin( );
        return 0;
     ```

   - O método add insere um novo par chave/valor. Se a chave existir atualmente, então, uma exceção é lançada.

     ```
      case "a":
        if( key == null ) throw new MissingParameterException( "key" );
        if( value == null ) throw new MissingParameterException( "value" );
        map.Add( key, value );
        Console.WriteLine( "SUCCESS: Added key '{0}' with value '{1}',
        partitionId={2}", key, value, partitionId );
        return 0;
     ```

   - O método put insere ou atualiza um par chave/valor.

     ```
     case "p":
       if( key == null ) throw new MissingParameterException( "key" );
       if( value == null ) throw new MissingParameterException( "value" );
       map.Put( key, value );
       Console.WriteLine( "SUCCESS: Put key '{0}' with value '{1}',
       partitionId={2}", key, value, partitionId );
       return 0;
     ```

   - O método replace substitui um par chave/valor existente. Se o item não estiver presente, então, uma exceção é emitida.

     ```
     case "r":
       if( key == null ) throw new MissingParameterException( "key" );
       if( value == null ) throw new MissingParameterException( "value" );
       map.Replace( key, value );
       Console.WriteLine( "SUCCESS: Replaced key '{0}' with value '{1}',
       partitionId={2}", key, value, partitionId );
       return 0;
     ```

   - O método remove exclui um par chave/valor.

     ```
     case "d":
       if( key == null ) throw new MissingParameterException( "key" );
       map.Remove( key );
       Console.WriteLine( "SUCCESS: Deleted value with key '{0}',
       partitionId={1}", key, partitionId );
        return 0;
     ```

   - O método get recupera o valor para a chave fornecida.

     ```
      case "g":
       if( key == null ) throw new MissingParameterException( "key" );
       value = ( TestValue )map.Get( key );
       if ( value != null )
       {
         Console.WriteLine( "SUCCESS: Value is '{0}',
       partitionId={1}", value, partitionId );
       }
     ```

```
else
{
  Console.WriteLine( "FAILED: Key not found" );
}
return 0;
```

- Se desejar cancelar as operações executadas na operação antes da confirmação, use o método rollback.

```
case "rollback":
  map.Transaction.Rollback( );
  return 0;
```

- O método commit confirma as operações concluídas na transação.

```
case "commit":
  map.Transaction.Commit( );
  return 0;
```

Tarefas relacionadas:

.NET 8.6+ “Configurando o Ambiente de Desenvolvimento .NET” na página 696
Para usar o WebSphere eXtreme Scale Client para .NET no Microsoft Visual Studio, você deve instalar o ambiente de desenvolvimento e configurar seu projeto para usar a montagem do WebSphere eXtreme Scale Client para .NET.

.NET 8.6+ “Acessando o WebSphere eXtreme Scale Client para Documentação da API .NET” na página 697
É possível acessar a documentação do WebSphere eXtreme Scale Client para a API .NET em um arquivo `.chm` ou visualizando a documentação da API no centro de informações.

Ponto de verificação de lições:

Nesta lição, você aprendeu como criar um aplicativo cliente simples .NET para executar operações da grade de dados.

Lição 2.3: Criando um Aplicativo de Grade de Dados Corporativos

Para criar um aplicativo de grade de dados corporativos no qual clientes Java e .NET podem atualizar a mesma grade de dados, você deve tornar suas classes compatíveis. Nos aplicativos de amostra de introdução, o aplicativo de amostra .NET tem aliases para corresponderem aos padrões Java.

Inclua atributos de alias de classe e de alias de campo em seu aplicativo .NET. É possível incluir o alias de classe no aplicativo .NET, no aplicativo Java ou em ambos. A amostra .NET tem aliases que correspondem aos padrões Java, portanto, o aplicativo Java não precisa de um alias. Os arquivos `TestKey.cs` e `TestValue.cs` estão no diretório *net_client_home*`/sample/SimpleClient`.

```
[ClassAlias( "com.ibm.websphere.xs.sample.gettingstarted.model.TestKey" )]
```

Figura 12. Atributo de Alias de Classe no Arquivo TestKey.cs

```
[ClassAlias( "com.ibm.websphere.xs.sample.gettingstarted.model.TestValue" )]
```

Figura 13. Atributo de Alias de Classe no Arquivo TestValue.cs

Conceitos relacionados:

8.6+ "Anotações ClassAlias e FieldAlias" na página 125
Use as anotações ClassAlias e FieldAlias para ativar o compartilhamento de dados da grade de dados entre classes. É possível compartilhar dados entre duas classes Java ou entre uma classe Java e uma .NET.

Tarefas relacionadas:

8.6+ "Definindo Anotações ClassAlias e FieldAlias para Correlacionar Classes Java e .NET" na página 124
Use as anotações ClassAlias e FieldAlias para ativar o compartilhamento de dados da grade de dados entre suas classes Java e .NET.

Ponto de verificação de lições:

Você incluiu atributos de classe no aplicativo de introdução .NET. Como resultado, é possível interoperar com o aplicativo de introdução Java, criando uma grade de dados corporativa.

Módulo 3: Executando o Aplicativo de Amostra na Grade de Dados

Para executar o aplicativo de amostra, primeiro você deve iniciar os servidores de catálogos e os servidores de contêineres. Em seguida, é possível executar seu aplicativo de amostra.

O processo para iniciar os servidores de catálogos e de contêineres é o mesmo se estiver executando o aplicativo .NET ou Java.

Objetivos do aprendizado

Após concluir as lições neste módulo você saberá como fazer o seguinte:

- Iniciar servidores de catálogos e contêineres
- Java Executar o aplicativo cliente de amostra de introdução Java
- .NET 8.6+ Executar o aplicativo cliente de amostra .NET

8.6+ Além de executar os aplicativos de amostra Java e .NET separadamente, é possível executá-los simultaneamente na mesma grade de dados. Por exemplo, é possível inserir um valor na grade de dados com o aplicativo .NET e, em seguida, obter o valor com o aplicativo Java. Nesse cenário, você está executando uma grade de dados corporativos.

Lição 3.1 do Tutorial de Introdução: Iniciando Servidores de Catálogos e de Contêineres

Para executar o aplicativo cliente de amostra, você deve iniciar um servidor de catálogos e um servidor de contêiner.

O script `env.sh|bat` é chamado pelos outros scripts para configurar as variáveis necessárias do ambiente. Normalmente não é necessário alterar esse script.

- UNIX Linux `./env.sh`
- Windows `env.bat`

Para executar o aplicativo, primeiro você deve iniciar o processo do serviço de catálogo. O serviço de catálogo é o centro de controle da grade de dados. O serviço de catálogo controla os locais dos servidores de contêiner e controla o

posicionamento de dados para hospedar os servidores de contêiner. Após o serviço de catálogo ser iniciado, é possível iniciar os servidores de contêiner, que armazenam os dados do aplicativo para a grade de dados. Para armazenar diversas cópias dos dados, diversos servidores de contêiner podem ser iniciados. Quando todos os servidores forem iniciados, será possível executar o aplicativo cliente para inserir, atualizar, remover e obter dados da grade de dados.

1. Abra uma sessão de terminal ou janela de linha de comandos.
2. Em uma sessão de terminal ou janela da linha de comandos, navegue até o diretório *wxs_install_root*/ObjectGrid/gettingstarted de sua instalação de servidor.
3. Execute o script a seguir para iniciar um processo de serviço de catálogo no host local: 8.6+
   - UNIX Linux `./startcat.sh`
   - Windows `startcat.bat`

   O processo do serviço de catálogo executa na janela do terminal atual.

   Também é possível iniciar o serviço de catálogo com o comando **startXsServer**. Execute o **startXsServer** a partir do diretório *wxs_install_root*/ObjectGrid/bin:

   - UNIX Linux 8.6+
     ```
     ./startXsServer.sh cs0
     -catalogServiceEndPoints cs0:localhost:6600:6601 -listenerPort 2809
     ```
   - Windows 8.6+
     ```
     startXsServer.bat cs0 -catalogServiceEndPoints
     cs0:localhost:6600:6601 -listenerPort 2809
     ```
4. Abra outra sessão de terminal ou janela de linha de comandos e execute o comando a seguir para iniciar uma instância do servidor de contêiner: 8.6+
   - UNIX Linux `./startcontainer.sh server0`
   - Windows `startcontainer.bat server0`

   O servidor de contêiner será executado na janela do terminal atual. Se desejar iniciar mais instâncias do servidor de contêiner para suportar a replicação, será possível repetir esta etapa com um nome de servidor diferente.

   Também é possível iniciar servidores de contêiner com o comando **startXsServer**. Execute o comando **startXsServer** a partir do diretório *wxs_install_root*/ObjectGrid/bin:

   - UNIX Linux 8.6+
     ```
     ./startXsServer.sh c0
     -catalogServiceEndPoints localhost:2809  -objectgridFile
     gettingstarted/server/config/objectgrid.xml -deploymentPolicyFile
     gettingstarted/server/config/deployment.xml
     ```
   - Windows 8.6+
     ```
     startXsServer.bat c0 -catalogServiceEndPoints
     localhost:2809  -objectgridFile gettingstarted\server\config\
     objectgrid.xml -deploymentPolicyFile gettingstarted\server\config\
     deployment.xml
     ```
5. Java 8.6+ Opcional: Em vez de iniciar os servidores de catálogos e de contêineres separadamente, é possível usar o script **runall** para iniciar um servidor de catálogos, um servidor de contêiner e um aplicativo cliente de amostra Java na mesma Java virtual machine. 8.6+
   - UNIX Linux `./runall.sh`
   - Windows `runall.bat`

Restrição: Como o script **runall** é executado integrado a servidores de contêineres, não é possível usar o console de monitoramento para monitorar seu ambiente. Estatísticas não são coletadas para os servidores de contêineres.

Tarefas relacionadas:

Iniciando e Parando Servidores Independentes
É possível iniciar e parar os servidores de catálogos e contêineres independentes com scripts ou a API do servidor integrado.

Referências relacionadas:

8.6+ Script **startXsServer** (XIO)
O script **startXsServer** inicia o contêiner e os servidores de catálogos que usam o mecanismo de transporte IBM eXtremeIO (XIO). Você deve usar o **startXsServer** quando desejar uma grade de dados corporativos. É possível utilizar uma variedade de parâmetros quando você inicia seu servidores para ativar o rastreio, especificar números de porta e assim por diante.

Ponto de verificação de lições:

Nesta lição, você aprendeu:

- Como iniciar os servidores de catálogos e servidores de contêiner

Lição 3.2 do Tutorial de Introdução: Executando o Aplicativo Cliente de Amostra de Introdução Java

Java

Use as etapas a seguir para executar um cliente Java para interagir com a grade de dados. O servidor de catálogos, o servidor de contêiner e o cliente são todos executados em um único servidor neste exemplo.

- 8.6+ Execute o cliente em modo interativo. A partir da janela de linha de comandos, execute um dos comandos a seguir:
  - UNIX Linux `./runclient.sh`
  - Windows `runclient.bat`

1. Inicie uma transação. É possível usar uma operação one-phase commit ou uma two-phase commit para sua transação. Com um one-phase commit, a transação deve gravar em uma única partição. Se durante a transação diversas chaves forem inseridas que são colocadas em diferentes partições, a transação falha na confirmação. É possível usar uma two-phase commit para gravar em diversas partições em uma única transação.
   - : Inicie uma transação one-phase commit.

     ```
     begin
     ```

   - Inicie uma transação two-phase commit.

     ```
     begin2pc
     ```

2. Insira um valor.

   ```
   > i key1 helloWorld
   SUCCESS: Inserted TestValue [value=helloWorld] with key TestKey [key=key1], part
   itionId=6
   ```

3. Recupere um valor inserido.

```
> g key1
Value is TestValue [value=helloWorld], partitionId=6
```

4. Atualize um valor.

```
> u key1 goodbyeWorld
SUCCESS: Updated key TestKey [key=key1] with value TestValue [value=goodbyeWorld
], partitionId=6
```

5. Retroceda a transação. Ao retroceder a transação, todas as operações associadas a essa transação são canceladas.

```
>rollback
```

6. Para testar a opção de retrocesso, tente obter a chave novamente. Como você reverteu a transação, a chave não existe:

```
> g key1
```

7. Insira um valor.

```
> i key1 helloWorld
SUCCESS: Inserted TestValue [value=helloWorld] with key TestKey [key=key1], part
itionId=6
```

8. Confirme o valor. Após confirmar a transação, não será possível reverter mudanças.

```
> commit
```

9. Exclua um valor inserido.

```
> d key1
SUCCESS: Deleted value with key TestKey [key=key1], partitionId=6
```

10. Insira um número de entradas de teste. Por exemplo, para inserir 1000 chaves e valores numerados de 0 a 999, use o comando a seguir:

```
> n 1000
```

- **8.6+** Execute o cliente no modo de linha de comando. Usar o modo de linha de comando pode ser útil se deseja gravar um script para executar o aplicativo cliente. É possível executar os mesmos comandos executados no modo interativo. Segue um exemplo da sintaxe para o modo de linha de comando:
  - UNIX Linux

```
./runclient.sh i "key1" "helloWorld"
```

  - Windows

```
runclient.bat i "key1" "helloWorld"
```

Ponto de verificação de lições:

Lições Aprendidas

Nesta lição, você aprendeu:

- Como executar o aplicativo cliente de amostra Java para inserir, obter, atualizar e excluir dados da grade de dados.

Lição 3.3 do Tutorial de Introdução: Executando o Aplicativo Cliente de Amostra .NET

.NET

Use as etapas a seguir para executar um aplicativo cliente .NET para interagir com a grade de dados. O servidor de catálogos, o servidor de contêiner e o cliente são todos executados em um único servidor neste exemplo.

O cliente .NET suporta somente one-phase commits. Portanto, se você tentar inserir diversos valores na mesma transação, uma exceção resulta, pois os valores irão para diferentes partições. Para evitar que essas exceções ocorram ao executar a amostra, é possível alterar seu arquivo XML descritor de política de implementação para usar uma partição. Para obter informações adicionais sobre como atualizar o número de partições, consulte "Tutorial de Introdução - Lição 1.1: Definindo Grades de Dados com Arquivos de Configuração" na página 235.

É possível executar o aplicativo de amostra no modo interativo ou de linha de comandos. No modo interativo, o aplicativo executa transações manuais de grade de dados com a API IGridMapPessimisticTx. O modo de linha de comando executa transações da grade de dados com a API IGridMapPessimisticAutoTx.

É possível executar a amostra no modo interativo ou no modo de linha de comandos:

- Execute o aplicativo cliente de amostra no modo interativo.
  1. Execute o aplicativo cliente simples. O arquivo está no diretório *net_client_home*`\gettingstarted\bin\`. Para executar a amostra no modo interativo, execute o comando a seguir.

     ```
     SimpleClient.exe -i
     ```

     O aplicativo conecta ao host `localhost:2809` por padrão. Para substituir o padrão, também é possível fornecer um host remoto e uma porta como parâmetro para o aplicativo:

     ```
     SimpleClient.exe -i -h <endpoint>
     ```

     Se executar o aplicativo sem nenhum parâmetro, a ajuda do aplicativo é exibida.
  2. Exiba uma lista de comandos que estão disponíveis.

```
Enter a command: help
This program executes simple CRUD operations on a map.
        a - Adds a value with the specified key. If the key already exists,
        DuplicatKeyException is thrown
        p - Adds a value with the specified key, replacing the entry if it
        already exists
        r - Replaces the value of the specified key. If the key does not exist,
        a CacheKeyNotFound exception is thrown
        g - Retrieve and display the value of the specified key
        d - Deletes the key
        gp - Gets the partition id for the key
        ck - Checks if the map contains the key
        h - Display help
        begin - Begin manual transaction
        commit - Commit transactions
        rollback - Rollback transactions
        exit - Exit program
```

3. Inicie a transação. Você deve iniciar uma transação para executar comandos na grade de dados. Se não iniciar a transação, ocorre uma exceção NoActiveTransacationException.

```
Enter a command: begin
```

4. Inclua os dados na grade de dados.

```
Enter a command: a key1 value1
SUCCESS: Added 'TestKey [key=key1]' with value 'TestValue [value=value1]',
partitionId=6
```

5. Procure e exiba o valor.

```
Enter a command: g key1
SUCCESS: Value is 'TestValue [value=value1]', partitionId=6
```

Neste exemplo, `value1` é retornado.

6. Atualize a chave. Use o comando put, que inclui um valor com a chave especificada, substituindo o valor existente se ele existir.

```
Enter a command: p key1 value2
SUCCESS: Put key 'TestKey [key=key1]' with value 'TestValue [value=value2]',
 partitionId=6
Enter a command: g key1
SUCCESS: Value is 'TestValue [value=value2]', partitionId=6
```

7. Substitua a chave. O comando replace substitui o valor pela chave especificada. Se a chave não existir, uma exceção CacheKeyException resulta.

```
Enter a command: r key1 value3
SUCCESS: Replaced key 'TestKey [key=key1]' with value 'TestValue [value=value3]'
, partitionId=6
```

8. Retroceda a transação e tente exibir a chave de valor novamente. É possível retroceder a transação a qualquer tempo antes da confirmação.

```
Enter a command: rollback
Enter a command: begin
Enter a command: g key1
FAILED: Key not found
```

Ao executar o comando get, você obtém uma exceção de que a chave não foi localizada.

9. Confirme uma chave e um valor na grade de dados.

```
Enter a command: begin
Enter a command: a key2 value2
SUCCESS: Added 'TestKey [key=key2]' with value 'TestValue [value=value2]',
partitionId=7
Enter a command: commit
```

10. Obtenha o ID da partição para uma chave.

```
Enter a command: begin
Enter a command: gp key2
SUCCESS: partitionId=7
```

11. Verifique o mapa para chaves.

```
Enter a command: ck key2
SUCCESS: The map contains key 'TestKey [key=key2]'
Enter a command: ck key3
SUCCESS: The map does NOT contain key 'TestKey [key=key3]'
```

12. Exclua a chave e saia.

```
Enter a command: begin
Enter a command: d key2
SUCCESS: Deleted value with key 'TestKey [key=key2]', partitionId=7
Enter a command: commit
Enter a command: exit
```

- Execute o cliente no modo de linha de comando. O modo de linha de comando executa transações da grade de dados com a API IGridMapPessimisticAutoTx. Para usar esse modo, passe a ação na linha de comandos. Usar o modo de linha de comando pode ser útil se deseja gravar um script para executar o aplicativo cliente. É possível executar os mesmos comandos executados no modo interativo. Segue um exemplo da sintaxe para o modo de linha de comando:

```
SimpleClient [-h <host:port>] <a | p | r | g | d> <key> [<value>]
```

Tarefas relacionadas:

.NET 8.6+ “Desenvolvendo Aplicativos .NET” na página 695
É possível desenvolver aplicativos Microsoft .NET que usam a mesma grade de dados que seus aplicativos Java.

“Acessando o WebSphere eXtreme Scale Client para Documentação da API .NET” na página 697
É possível acessar a documentação do WebSphere eXtreme Scale Client para a API .NET em um arquivo `.chm` ou visualizando a documentação da API no centro de informações.

Ponto de verificação de lições:

Nesta lição, você aprendeu:

- Como executar o aplicativo cliente de amostra .NET para inserir, obter, atualizar e excluir objetos da grade de dados.

Lição 4 do Tutorial de Introdução: Monitore seu Ambiente

É possível usar o utilitário **xscmd** e as ferramentas do console da web para monitorar o ambiente da grade de dados.

Tarefas relacionadas:

Visualizando Estatísticas com o Console da Web
É possível monitorar estatísticas e outras informações de desempenho com o console da web.

Monitorando com o Console da Web
Com o console da Web, é possível registrar no gráfico as estatísticas atuais e de histórico. Este console fornece alguns gráficos pré-configurados para visões gerais de alto nível e tem uma página de relatórios customizada que pode ser usada para construir gráficos a partir das estatísticas disponíveis. É possível usar os recursos gráficos no console de monitoramento do WebSphere eXtreme Scale para visualizar o desempenho geral das grades de dados em seu ambiente.

Iniciando e Efetuando Login no Console da Web
Inicie o servidor de console executando o comando **startConsoleServer** e efetuando login no servidor com o ID de usuário e a senha padrão.

Conectando o Console da Web nos Servidores de Catálogos
Para visualizar as estatísticas no console da Web, primeiro você deve se conectar com os servidores de catálogo que deseja monitorar. Etapas adicionais serão necessárias se a segurança estiver ativada nos seus servidores de catálogos.

Monitorando com o Utilitário **xscmd**
O utilitário **xscmd** substitui o utilitário **xsadmin** de amostra como uma ferramenta de monitoramento e administração totalmente suportada. Com o utilitário **xscmd**, é possível exibir informações textuais sobre sua topologia do WebSphere eXtreme Scale.

Administrando com o Utilitário **xscmd**
Com o utilitário **xscmd**, é possível concluir tarefas administrativas no ambiente, tal como: estabelecer links de replicação multi-master, substituir o quorum e parar os grupos de servidores com o comando teardown.

Referências relacionadas:

Estatísticas do Console da Web
Dependendo da visualização que você está utilizando no console da Web, é possível visualizar estatísticas diferentes sobre sua configuração. Essas estatísticas incluem a memória usada, as principais grades de dados usadas e o número de entradas de cache.

8.6+ Script **startXsServer** (XIO)
O script **startXsServer** inicia o contêiner e os servidores de catálogos que usam o mecanismo de transporte IBM eXtremeIO (XIO). Você deve usar o **startXsServer** quando desejar uma grade de dados corporativos. É possível utilizar uma variedade de parâmetros quando você inicia seu servidores para ativar o rastreio, especificar números de porta e assim por diante.

Monitorando com o Console da Web

Com o console da Web, é possível registrar no gráfico as estatísticas atuais e de histórico. Este console fornece alguns gráficos pré-configurados para visões gerais de alto nível e tem uma página de relatórios customizada que pode ser usada para construir gráficos a partir das estatísticas disponíveis. É possível usar os recursos gráficos no console de monitoramento do WebSphere eXtreme Scale para visualizar o desempenho geral das grades de dados em seu ambiente.

Instale o console da web como um recurso opcional no qual você executa o assistente de instalação.

1. Inicie o servidor do console. O script **startConsoleServer.bat|sh** para iniciar o servidor do console está no diretório *wxs_install_root*/ObjectGrid/bin de sua instalação.
2. Efetue logon no console.
   a. No seu navegador da web, acesse https://your.console.host:7443, substituindo your.console.host pelo nome do host do servidor na qual o console foi instalado.
   b. Efetue logon no console.
      - **ID do usuário:** admin
      - **Senha:** admin

      A página de boas-vindas do console é exibida.
3. Edite a configuração do console. Clique em **Definições** > **Configuração** para revisar a configuração do console. A configuração do console inclui informações como:
   - Cadeia de rastreio para o cliente do WebSphere eXtreme Scale, como *=all=disabled
   - O nome e a senha do Administrador
   - O endereço de e-mail do Administrador
4. Estabeleça e mantenha conexões com servidores de catálogos que você deseja monitorar. Repita as seguintes etapas para incluir cada servidor de catálogos na configuração.
   a. Clique em **Configurações** > **Servidores de Catálogos do eXtreme Scale** .
   b. Inclua um novo servidor de catálogos.

      1) Clique no ícone Incluir () para registrar um servidor de catálogos existente.
      2) Forneça informações, como o nome do host e a porta do listener. Consulte “Planejamento para Portas de Rede” na página 300 para obter mais informações sobre a configuração da porta e os padrões.
      3) Clique em **OK**.
      4) Verifique se o servidor de catálogos foi incluído na árvore de navegação.
5. Agrupe os servidores de catálogos que foram criados em um domínio de serviço de catálogo. Você deve criar um domínio de serviço de catálogo quando a segurança estiver ativada nos seus servidores de catálogos porque as configurações de segurança são definidas no domínio de serviço de catrálogo.
   a. Clique na página **Configurações** > **Domínios do eXtreme Scale** .
   b. Inclua um novo domínio do serviço de catálogo.

      1) Clique no ícone Incluir () para registrar um domínio de serviço de catálogo. Insira um nome para o domínio de serviço de catálogo.
      2) Depois de criar o domínio de serviço de catálogo, as propriedades poderão ser editadas. As propriedades do domínio de serviço de catálogo são:

         Nome Indica o nome do host do domínio, conforme designado pelo administrador.

         Servidores de catálogos
         Lista um ou mais servidores de catálogos que pertencem ao

domínio selecionado. É possível incluir os servidores de catálogos criados na etapa anterior.

Classe de gerador
Exibe o nome da classe que implementa a interface CredentialGenerator. Essa classe é usada para obter credenciais para os clientes.Se você especificar um valor neste campo, o valor substituirá a propriedade **crendentialGeneratorClass** no arquivo `client.properties`.

Propriedades do gerador
Especifica as propriedades para a classe de implementação CredentialGenerator. As propriedades são configuradas para o objeto com o método setProperties(String). O valor credentialGeneratorprops é usado apenas se o valor da propriedade credentialGeneratorClass não for nulo. Se você especificar um valor neste campo, o valor substituirá a propriedade **credentialGeneratorProps** no arquivo `client.properties`.

Caminho de Propriedades do Cliente eXtreme Scale
Especifica o caminho para o arquivo de propriedades do cliente editado para incluir as propriedades de segurança em uma etapa anterior. Por exemplo, você pode indicar o arquivo `c:\ObjectGridProperties\sampleclient.properties`. Se desejar que o console pare de tentar usar conexões seguras, é possível excluir o valor neste campo. Depois de configurar o caminho, o console usará uma conexão não segura.

3) Clique em **OK**.
4) Verifique se o domínio foi incluído na árvore de navegação.

Para visualizar informações sobre um domínio de serviço de catálogo existente, clique no nome do domínio de serviço de catálogo na árvore de navegação na página **Configurações** > **Domínios do eXtreme Scale**.

6. Visualize o status da conexão. O campo **Domínio Atual** indica o nome do domínio do serviço de catálogo que está atualmente sendo usado para exibir informações no console da web. O status da conexão é exibido ao lado do nome do domínio de serviço de catálogo.
7. Visualize as estatísticas para as grades de dados e servidores ou crie um relatório customizado.

Monitorando com o Utilitário xscmd

1. Opcional: Se a autenticação de cliente estiver ativa: Abra uma janela de linha de comandos. Na linha de comandos, configure as variáveis de ambiente apropriadas.
2. Acesse o diretório *wxs_home*/bin.

   ```
   cd wxs_home/bin
   ```
3. Execute vários comandos para exibir informações sobre seu ambiente.
   - Mostre todos os servidores de contêiner on-line para a grade de dados Grid e o conjunto de mapas mapSet:

     ```
     xscmd -c showPlacement -g Grid -ms mapSet
     ```
   - Exiba as informações de roteamento para a grade de dados.

     ```
     xscmd -c routetable -g Grid
     ```
   - Exiba o número de entradas do mapa na grade de dados.

     ```
     xscmd -c showMapSizes -g Grid -ms mapSet
     ```

Parando os Servidores

Depois de usar o aplicativo cliente e o monitorar a amostra do ambiente de introdução, os servidores poderão ser interrompidos.

- Se os arquivos de script forem usados para iniciar os servidores, utilize <ctrl+c> para parar o processo de serviço de catálogo e os servidores de contêiner em suas respectivas janelas.
- Se tiver usado o comando **startXsServer** para iniciar seus servidores, use o comando **stopXsServer** para parar os servidores.

  Pare o servidor de contêiner:

  – UNIX Linux `stopXsServer.sh c0 -catalogServiceEndPoints localhost:2809`

  – Windows `stopXsServer.bat c0 -catalogServiceEndPoints localhost:2809`

  Pare o servidor de catálogos:

  – UNIX Linux `stopXsServer.sh cs1 -catalogServiceEndPoints localhost:2809`

  – Windows `stopXsServer.bat cs1 -catalogServiceEndPoints localhost:2809`

Ponto de verificação de lições

Nesta lição, você aprendeu:

- Como iniciar o console da web e conectá-lo ao servidor de catálogos
- Como monitorar a grade de dados e as estatísticas do servidor
- Como parar os servidores

Introdução ao Desenvolvimento de Aplicativos

Java

Para iniciar o desenvolvimento de aplicativos WebSphere eXtreme Scale, você deve configurar seu ambiente de desenvolvimento, aprender sobre APIs que podem ser usadas e, em seguida, desenvolver e testar seu aplicativo.

Antes de Iniciar

Sobre Esta Tarefa

8.6+ As etapas executadas para iniciar o desenvolvimento de aplicativos são ligeiramente diferentes, dependendo de se estiver usando a linguagem de programação Java ou . NET. Com aplicativos Java, é possível controlar as operações de servidor com as APIs. Essas APIs podem criar e iniciar servidores, instâncias de ObjectGrid e inserir dados na grade de dados. Com um aplicativo .NET, seu aplicativo é conectado a servidores de catálogos e servidores de contêineres em execução. Portanto, se estiver usando um aplicativo .NET, você deve iniciar seus servidores antes de executar seu aplicativo cliente.

Procedimento

1. Configure um ambiente de desenvolvimento e acesse a documentação da API.

É possível iniciar o uso das APIs para desenvolver seus aplicativos. Também é possível utilizar a documentação da API dentro do ambiente de desenvolvimento.

Java **Mais informações:** “Configurando um Ambiente de Desenvolvimento Independente no Eclipse” na página 339

Java **Mais informações:** “Acessando a Documentação da API Java” na página 338

.NET 8.6+ **Mais informações:** “Configurando o Ambiente de Desenvolvimento .NET” na página 696

.NET 8.6+ **Mais informações:** “Acessando o WebSphere eXtreme Scale Client para Documentação da API .NET” na página 697

2. Java Em um ambiente Java, é possível criar um aplicativo simples que inicie servidores, crie uma instância de ObjectGrid e insira dados na grade de dados.
   a. Use a API ServerFactory para iniciar e parar servidores.

      Mais informações: Usando a API do Servidor Integrado para Iniciar e Parar Servidores
   b. Use a API do ObjectGridManager para recuperar a instância do ObjectGrid que foi criada.

      Mais informações: “Interagindo com um ObjectGrid Usando a Interface ObjectGridManager” na página 350
   c. Use a API ObjectMap para inserir dados na grade de dados.

      Mais informações: “Objetos de Armazenamento em Cache sem Relacionamentos Envolvidos (API ObjectMap)” na página 372A API ObjectMap é a forma mais simples de acessar e gravar dados na grade de dados. Se seus objetos possuírem relacionamentos complexos, as seguintes APIs poderão ser usadas para ler, gravar e atualizar os dados:
      - “Acessando Dados com Índices (API de Índice)” na página 359
      - “Objetos de Armazenamento em Cache e seus Relacionamentos (API EntityManager)” na página 388
      - “Recuperando Entidades e Objetos (API de Consulta)” na página 437
      - “Acessando Dados com o Serviço de Dados REST” na página 517

      Para obter mais informações sobre como escolher entre diferentes APIs, consulte Capítulo 5, “Desenvolvendo Aplicativos”, na página 337.

3. .NET 8.6+ Em um ambiente .NET, é possível gravar um aplicativo cliente que conecte ao servidor de catálogos, obtenha uma grade de dados e uma instância de mapa e leia, grave e atualize dados. Para obter informações adicionais sobre como gravar um aplicativo .NET básico, consulte “Tutorial de Introdução - Lição 2.2: Criando um Aplicativo Cliente .NET” na página 240.
4. Execute um teste de unidade de seu aplicativo.

   Também é possível usar o utilitário **xscmd** para exibir informações sobre os servidores em execução, réplicas, e assim por diante. Consulte o Administrando com o Utilitário **xscmd** para obter informações adicionais.
5. Quando estiver satisfeito com seu aplicativo no ambiente de desenvolvimento, crie arquivos de configuração XML e atualize seu aplicativo para usar a configuração. O aplicativo de amostra Introdução fornece exemplos desses arquivos de configuração e um aplicativo simples que usa esses arquivos de configuração.

Mais informações: "Tutorial: Introdução ao WebSphere eXtreme Scale" na página 235

6. Execute seu aplicativo usando os arquivos de configuração XML. O modo com você inicia seus servidores depende do ambiente que estiver sendo usado.

   É possível executar seu aplicativo em um dos seguintes contêineres:

   - Java virtual machine (JVM) independente
   - Tomcat
   - WebSphere Application Server
   - OSGi

Conceitos relacionados:

"Objetos de Armazenamento em Cache sem Relacionamentos Envolvidos (API ObjectMap)" na página 372
Os ObjectMaps são como Mapas Java que permitem que os dados sejam armazenados como pares chave-valor. Os ObjectMaps apresentam uma abordagem simples e intuitiva para o aplicativo que armazenará os dados. Um ObjectMap é ideal para o armazenamento em cache de objetos que não tenham nenhum relacionamento envolvido. Se os relacionamentos de objetos estiverem envolvidos, então você deve usar a API EntityManager.

"Visão Geral da API Java" na página 321
O WebSphere eXtreme Scale fornece diversos recursos que são acessados programaticamente usando a linguagem de programação Java através de interfaces de programação de aplicativos (APIs) e interfaces de programação do sistema.

Java "Visão Geral da API Java" na página 321
O WebSphere eXtreme Scale fornece diversos recursos que são acessados programaticamente usando a linguagem de programação Java através de interfaces de programação de aplicativos (APIs) e interfaces de programação do sistema.

Informações relacionadas:

Documentação da API

"Tutorial de Introdução - Lição 2.1: Criando um Aplicativo de Cliente Java" na página 238
Para inserir, excluir, atualizar e recuperar dados de sua grade de dados, você deverá gravar um aplicativo cliente. A amostra de introdução inclui um aplicativo de cliente Java que pode ser usado para aprender sobre como criar seu próprio aplicativo cliente.

Java Documentação da API

Capítulo 4. Planejamento

Antes de instalar o WebSphere eXtreme Scale e de implementar seus aplicativos de grade de dados, você deve decidir sobre sua topologia de armazenamento em cache, concluir o planejamento da capacidade, revisar os requisitos de hardware e de software, as configurações de rede e ajustes, e assim por diante. Também é possível usar a lista de verificação operacional para garantir que seu ambiente esteja pronto para ter um aplicativo implementado.

Para uma discussão das boas práticas que é possível usar ao projetar seus aplicativos WebSphere eXtreme Scale, leia o seguinte artigo em developerWorks: Princípios e boas práticas para construir aplicativos WebSphere eXtreme Scale de alta execução e alta resiliência.

Visão Geral de Planejamento

Antes de utilizar o WebSphere eXtreme Scale em um ambiente de produção, considere os seguintes problemas para otimizar sua implementação.

Considerações sobre Topologia de Armazenamento em Cache

Cada tipo de topologia de cache tem suas vantagens e desvantagens. A topologia de armazenamento em cache implementada depende dos requisitos do ambiente e do aplicativo. Para obter mais informações sobre as diferentes topologias de armazenamento em cache, consulte o “Planejando a Topologia” na página 258.

Considerações Sobre Capacidade de Dados

A lista a seguir inclui itens a serem considerados:

- **Número de sistemas e processadores**: Quantas máquinas e processadores físicos são necessários no ambiente?
- **Número de servidores**: Quantos servidores do eXtreme Scale são necessários para hospedar mapas do eXtreme Scale?
- **Número de partições**: A quantidade de dados armazenados nos mapas é um fator para determinar o número de partições necessárias.
- **Número de réplicas**: Quantas réplicas são necessárias para cada principal no domínio?
- **Replicação síncrona ou assíncrona**: Os dados são vitais de modo que a replicação síncrona seja necessária? Ou o desempenho é a maior prioridade, tornando a replicação assíncrona a escolha correta?
- **Tamanhos de heap**: Qual é quantidade de dados a ser armazenada em cada servidor?

Para obter uma discussão detalhada de cada uma dessas considerações, consulte “Capacidade do Ambiente de Planejamento” na página 226..

Considerações sobre Instalação

É possível instalar o WebSphere eXtreme Scale em um ambiente independente ou integrar a instalação com o WebSphere Application Server. Para assegurar um upgrade normal de seus servidores no futuro, você deve planejar seu ambiente de acordo. Para obter melhor desempenho, os servidores de catálogos devem ser

executados em máquinas diferentes dos servidores de contêiner. Se os seus servidores de catálogos e de contêiner tiverem que ser executados na mesma máquina, use instalações separadas do WebSphere eXtreme Scale para os servidores de catálogos e de contêiner. Ao usar as duas instalações, é possível fazer upgrade da instalação que está executando o servidor de catálogos primeiro. Consulte Atualizando Servidores eXtreme Scale.

Planejando a Topologia

Com WebSphere eXtreme Scale, sua arquitetura pode utilizar armazenamento em cache de dados em memória local ou armazenamento em cache de dados de cliente/servidor distribuídos. A arquitetura pode ter relacionamentos variados com seus bancos de dados. Também é possível configurar a topologia para estender diversos datacenters.

O WebSphere eXtreme Scale requer infraestrutura adicional mínima para operar. A infraestrutura consiste em scripts para instalar, iniciar e parar um aplicativo Java Platform, Enterprise Edition em um servidor. Os dados em cache são armazenados nos servidores de contêiner e os clientes se conectam remotamente com o servidor.

Ambientes em Memória

Quando implementar em um local, um ambiente em memória, o WebSphere eXtreme Scale é executado em uma única Java Virtual Machine e não é replicado. Para configurar um ambiente local, é possível usar um arquivo XML do ObjectGrid ou as APIs do ObjectGrid.

Ambientes Distribuídos

Quando você implementa em um ambiente distribuído, o WebSphere eXtreme Scale é executado em um conjunto de Java Virtual Machines, aumentando o desempenho, a disponibilidade e a escalabilidade. Com essa configuração, poderá utilizar a replicação de dados e criação de partições. Também é possível incluir servidores adicionais sem restaurar seus servidores eXtreme Scale existentes. Assim como ocorre com um ambiente local, um arquivo XML do ObjectGrid, ou uma configuração programática equivalente, é necessário em um ambiente distribuído. Você também deve fornecer um arquivo XML de política de implementação com detalhes de configuração.

É possível criar implementações simples ou grandes a nível de terabytes, em que milhares de servidores são necessários.

Cache de Memória Local

Em um caso mais simples, o WebSphere eXtreme Scale pode ser utilizado como um cache de grade de dados em memória local (não distribuído). O caso local pode beneficiar especialmente aplicativos de alta simultaneidade nos quais vários encadeamentos precisam acessar e modificar dados transientes. Os dados mantidos em uma grade de dados local podem ser indexados e recuperados utilizando consultas. As consultas ajudam você a trabalhar com grandes em conjuntos de dados de memória. O suporte fornecido com o Java Virtual Machine (JVM), embora esteja pronto para uso, tem uma estrutura de dados limitada.

A topologia de cache em memória local para WebSphere eXtreme Scale é usado para oferecer acesso transacional e consistente aos dados temporários dentro de uma única Java virtual machine.

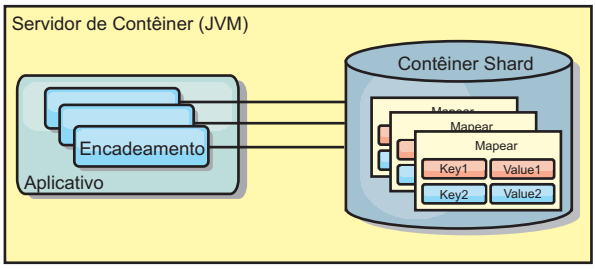


Figura 14. Cenário de Cache em Memória Local

Vantagens

- Configuração simples: Um ObjectGrid pode ser criado programaticamente ou declarativamente com o arquivo XML do descritor de implementação ObjectGrid ou com outras estruturas como Spring.
- Rápido: Cada BackingMap pode ser ajustado de maneira independente para utilização de memória e simultaneidade ideais.
- Ideal para topologias de uma única Java virtual machine com pequenos conjuntos de dados ou para armazenamento em cache de dados frequentemente acessados.
- Transacional. As atualizações BackingMap podem ser agrupadas em uma única unidade de trabalho e podem ser integradas como um último participante nas transações de duas fases como transações JTA (Java Transaction Architecture).

Desvantagens

- Não tolerante a falhas.
- Os dados não são replicados. Caches em memória são melhores para dados de referência somente para leitura.
- Não escalável. A quantidade de memória necessária pelo banco de dados pode ultrapassar a capacidade da Java virtual machine.
- Ocorrem problemas na inclusão de Java virtual machines:
  - Os dados não podem ser facilmente particionados
  - Você deve replicar manualmente o estado entre as Java virtual machines ou cada instância do cache poderá ter diferentes versões dos mesmos dados.
  - A invalidação é custosa.
  - Cada cache deve ser aquecido de maneira independente. O aquecimento é o período de carregamento de um conjunto de dados para que o cache seja preenchido com dados válidos.

Quando Utilizar

A topologia de implementação de cache em memória local deve ser usada somente quando a quantidade de dados a serem armazenados em cache for pequena (puder ser colocada em uma única Java virtual machine) e for relativamente estável. Dados antigos devem ser tolerados com esta abordagem. A utilização de evictors para manter os dados mais frequentemente ou recentemente usados no cache pode ajudar a diminuir o tamanho do cache e a aumentar a relevância dos dados.

Cache Local Replicado pelo Peer

Você deverá assegurar-se de que o cache esteja sincronizado se vários processos com instâncias de cache independentes existirem. Para assegurar-se de que as instâncias de cache estejam sincronizadas, ative um cache replicado por peer com o Java Message Service (JMS).

WebSphere eXtreme Scale inclui dois plug-ins que propagam automaticamente mudanças de transação entre instâncias do ObjectGrid peer. O plug-in JMSObjectGridEventListener propaga automaticamente as mudanças do eXtreme Scale usando JMS.

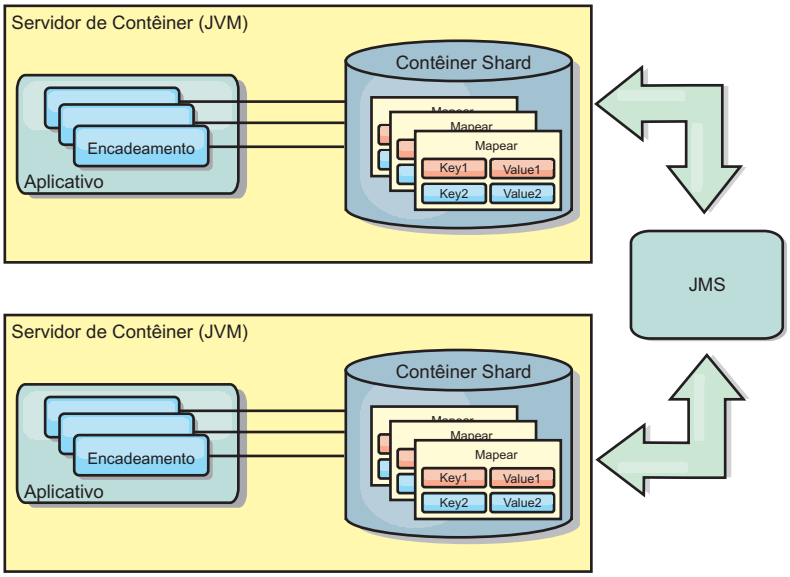


Figura 15. Cache Replicado pelo Peer com Alterações que são Propagadas com JMS

Se você estiver executando um ambiente doWebSphere Application Server, o plug-in TranPropListener também estará disponível. O plug-in TranPropListener usa o gerenciador de alta disponibilidade (HA) para propagar as mudanças em cada instância do cache de peer.

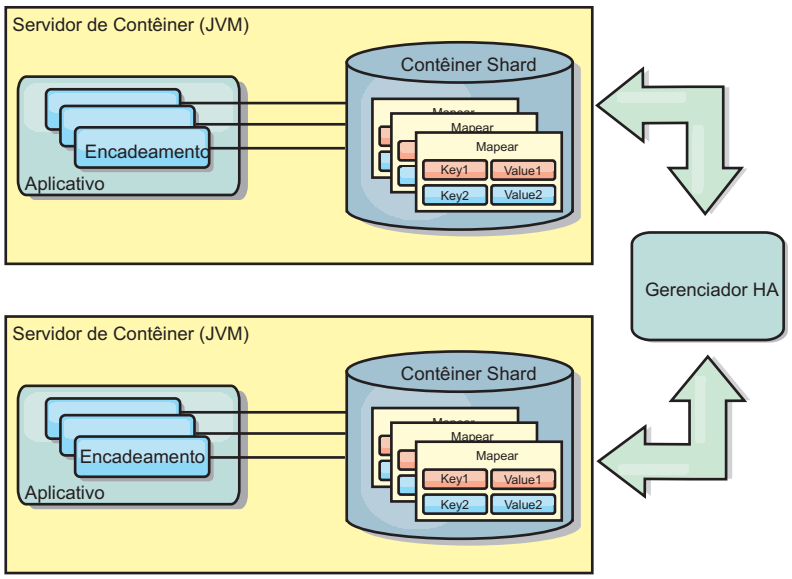


Figura 16. Cache Replicado pelo Peer com Alterações que são Propagadas com o Gerenciador de Alta Disponibilidade

Vantagens

- Os dados são mais válidos porque os dados são atualizados mais frequentemente.
- Com o plug-in TranPropListener, como no ambiente local, o eXtreme Scale pode ser criado programaticamente ou declarativamente com o arquivo XML descritor de implementação do eXtreme Scale ou com outras estruturas como Spring. A integração com o gerenciador de alta disponibilidade é feita automaticamente.
- Cada BackingMap pode ser independentemente ajustado para melhor utilização da memória e concorrência.
- As atualizações BackingMap podem ser agrupadas em uma única unidade de trabalho e podem ser integradas como um último participante nas transações de duas fases como transações JTA (Java Transaction Architecture).
- Ideal para poucas topologias JVM com um conjunto de dados razoavelmente pequeno ou para armazenamento em cache de dados frequentemente acessados.
- As atualizações em cada eXtreme Scale são replicadas para todas as instâncias do eXtreme Scale do peer. As alterações são consistentes desde que uma assinatura durável seja utilizada.

Desvantagens

- A configuração e a manutenção para o JMSObjectGridEventListener podem ser complexas. O eXtreme Scale pode ser criado programaticamente ou declarativamente com o arquivo XML descritor de implementação do eXtreme Scale ou com outras estruturas tais como Spring.
- Não escalável: A quantidade de memória necessária para que o banco de dados possa dominar a JVM.
- Funciona inadequadamente ao incluir Java Virtual Machines:
  - Os dados não podem ser facilmente particionados
  - A invalidação é custosa.
  - Cada cache deve ser aquecido de maneira independente

Quando Utilizar

Use a topologia de implementação apenas quando a quantia de dados a ser armazenada em cache for pequena, podendo ajustar-se a uma única JVM e se for relativamente estável.

Cache Integrado

As grades do WebSphere eXtreme Scale podem ser executadas nos processos existentes como servidores eXtreme Scale integrados ou podem ser gerenciadas como processos externos.

As grades integradas são úteis quando você está executando em um servidor de aplicativos, como o WebSphere Application Server. É possível iniciar servidores eXtreme Scale que não são integrados usando scripts da linha de comandos e executar em um processo Java.

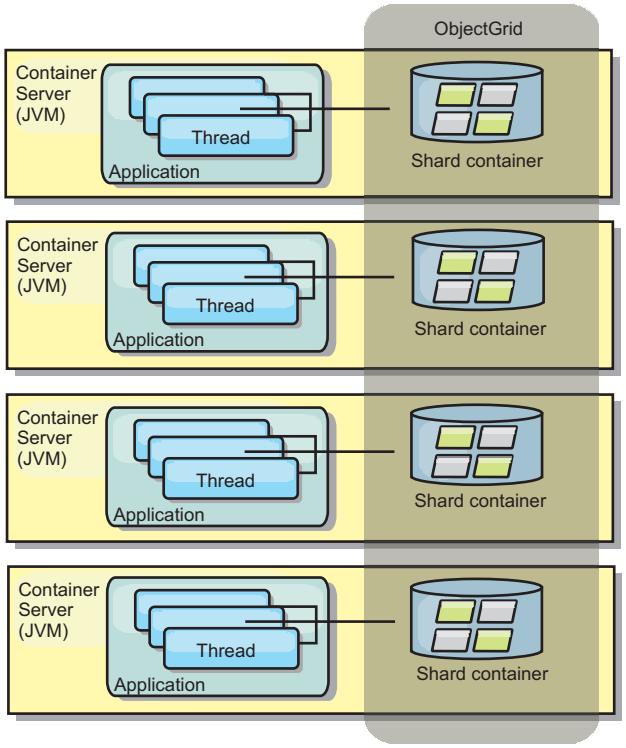


Figura 17. Cache Integrado

Vantagens

- Administração simplificada já que há menos processos para gerenciar.
- Implementação do aplicativo simplificada, já que a grade usa o carregador de classe do aplicativo cliente.
- Suporta particionamento e alta disponibilidade.

Desvantagens

- Aumento da área de cobertura da memória no processo do cliente já que todos os dados são colocados no processo.
- Aumento da utilização da CPU para atender pedidos de clientes.

- Mais difícil para manipular atualizações de aplicativo, pois os clientes estão usando os mesmos arquivos archive de Java do aplicativo que os servidores.
- Menos flexível. A escala dos clientes e servidores de grade não pode aumentar na mesma proporção. Quando os servidores são externamente definidos, é possível ter mais flexibilidade no gerenciamento do número de processos.

Quando Utilizar

Utilize grades integradas quando há grande quantidade de memória livre no processo do cliente para dados da grade e dados de failover potenciais.

Para obter mais informações, consulte Configurando a Sincronização do Cliente Baseada no Serviço de Mensagens Java (JMS) .

Cache Distribuído

O WebSphere eXtreme Scale é mais frequentemente usado como um cache compartilhado, para fornecer acesso transacional a dados para múltiplos componentes onde, caso contrário, um banco de dados tradicional seria usado. O cache compartilhado elimina a necessidade de configurar um banco de dados.

Coerência do Cache

O cache é coerente porque todos os clientes veem os mesmos dados no cache. Cada pedaço de dado é armazenado em exatamente um servidor no cache, evitando cópias de registros desperdiçadas que poderiam potencialmente conter diferentes versões dos dados. Um cache coerente também pode conter mais dados, à medida que mais servidores são incluídos na grade de dados, e escalado linearmente à medida que a grade cresce em tamanho. Como os clientes acessam dados a partir desta grade de dados com chamadas de processo remotas, ela também é conhecida como um cache remoto, ou cache distante. Através do particionamento de dados, cada processo contém um subconjunto exclusivo do conjunto de dados total. As grades de dados maiores podem conter mais dados e atender mais solicitações para esses dados. A coerência também elimina a necessidade de enviar dados de invalidação ao redor da grade de dados porque não há dados antigos. O cache coerente retém somente a cópia mais recente de cada pedaço de dados.

Se você estiver executando um ambiente doWebSphere Application Server, o plug-in TranPropListener também estará disponível. O plug-in TranPropListener usa o componente de alta disponibilidade (Gerenciador HA) do WebSphere Application Server para propagar as alterações para cada instância de cache ObjectGrid de peer.

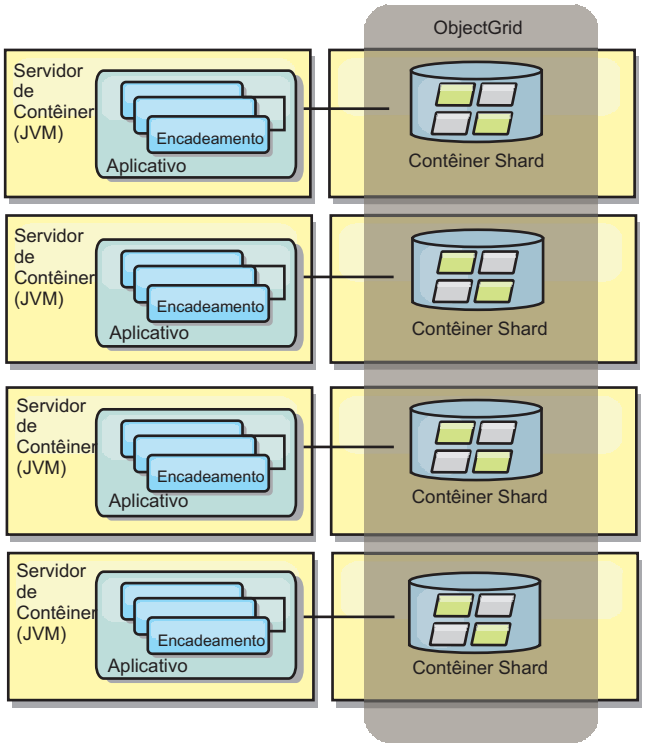


Figura 18. Cache Distribuído

Cache Local

Opcionalmente, os clientes têm um cache local, sequencial quando o eXtreme Scale é usado em uma topologia distribuída. Este cache opcional é chamado de cache local, um ObjectGrid independente em cada cliente, servindo como um cache para o cache remoto, do lado do cliente. O cache local é ativado por padrão quando o bloqueio é configurado como otimista ou nenhum e não pode ser utilizado quando é configurado como pessimista.

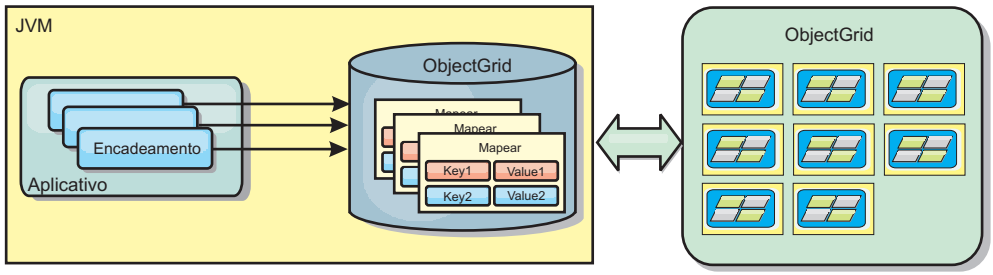


Figura 19. Cache Local

Um cache local é muito rápido porque fornece acesso em memória a um subconjunto do conjunto inteiro de dados em cache que é armazenado remotamente nos servidores do eXtreme Scale. O cache local não é particionado e contém dados de qualquer uma das partições eXtreme Scale remotas. O WebSphere eXtreme Scale pode ter até três camadas de cache, como a seguir.

1. O cache da camada da transação contém todas as alterações para uma única transação. O cache da transação contém uma cópia de trabalho dos dados até que a transação seja confirmada. Quando uma transação do cliente solicita dados de um ObjectMap, a transação é verificada primeiro.

2. O cache local na camada do cliente contém um subconjunto de dados da camada do servidor. Quando a camada da transação não possui os dados, eles são buscados em uma camada do cliente, se disponíveis, e inseridos no cache da transação.
3. A grade de dados na camada do servidor contém a maioria dos dados e é compartilhada entre todos os clientes. A camada do servidor pode ser particionada, o que permite que uma grande quantidade de dados seja armazenada em cache. Quando o cache local do cliente não possui os dados, eles são buscados na camada do servidor e inseridos no cache cliente. A camada do servidor também pode ter um plug-in do Utilitário de Carga. Quando a grade de dados não possui os dados solicitados, o Carregador é chamado e os dados resultantes são inseridos a partir do armazenamento de dados de backend na grade.

Para desativar o cache local, consulte Configurando o Cache Local.

Vantagem

- Tempo de resposta rápido porque todos os acessos aos dados é local. Procurar pelos dados no cache próximo primeiro economiza acesso à grade de servidores, o que torna até mesmo os dados remotos acessíveis localmente.

Desvantagens

- Aumenta a duração dos dados antigos porque o cache próximo em cada camada pode estar fora de sincronização com os dados atuais na grade de dados.
- Depende de um evictor para invalidar dados a fim de evitar a falta de memória.

Quando Utilizar

Utilize quando o tempo de resposta for importante e dados antigos puderem ser tolerados.

Integração com o Banco de Dados: Armazenamento em Cache Write-behind, Sequencial e Lateral

O WebSphere eXtreme Scale é usado para colocar um banco de dados tradicional na frente e eliminar a atividade de leitura que normalmente é armazenada no banco de dados. Um cache coerente pode ser utilizado com um aplicativo direta ou indiretamente, utilizando um mapeador relacional de objeto. O cache coerente pode transferir o banco de dados ou o backend a partir das leituras. Em um cenário levemente mais complexo, tal como o acesso transacional a um conjunto de dados no qual apenas parte dos dados requer garantias de persistência tradicional, a filtragem pode ser utilizada para transferir até mesmo transações de gravação.

É possível configurar o WebSphere eXtreme Scale para funcionar como um espaço de processamento de banco de dados em memória altamente flexível. Entretanto, o WebSphere eXtreme Scale não é um object relational mapper (ORM). Ele não reconhece de onde vieram os dados na grade de dados. Um aplicativo ou um ORM pode colocar dados em um servidor eXtreme Scale. É responsabilidade da origem dos dados certificar-se de que eles permaneçam consistentes com o banco de dados no qual os dados se originaram. Isto significa que o eXtreme Scale não pode invalidar dados que são extraídos de um banco de dados automaticamente. O aplicativo ou mapeador deve fornecer esta função e gerenciar os dados armazenados no eXtreme Scale.

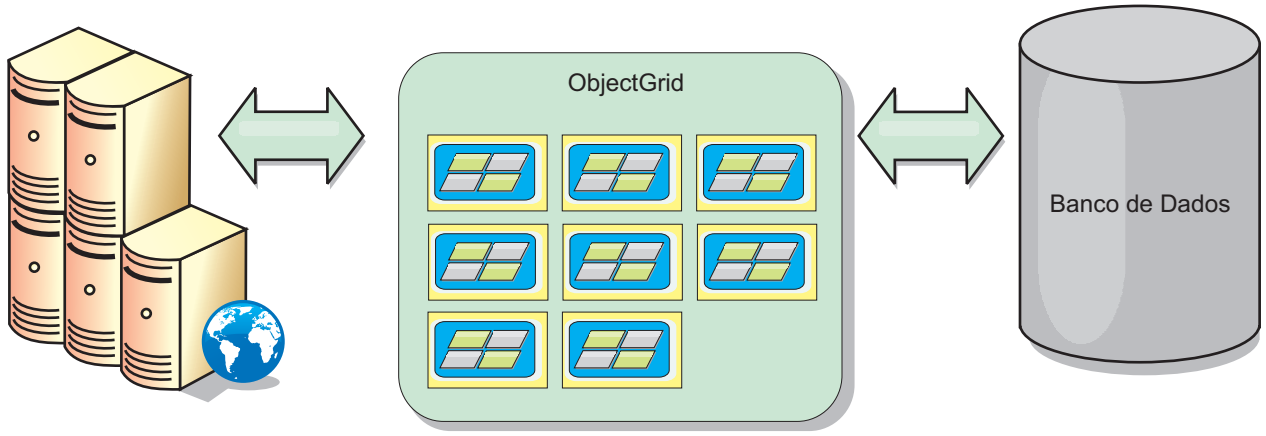


Figura 20. ObjectGrid como um Buffer de Banco de Dados

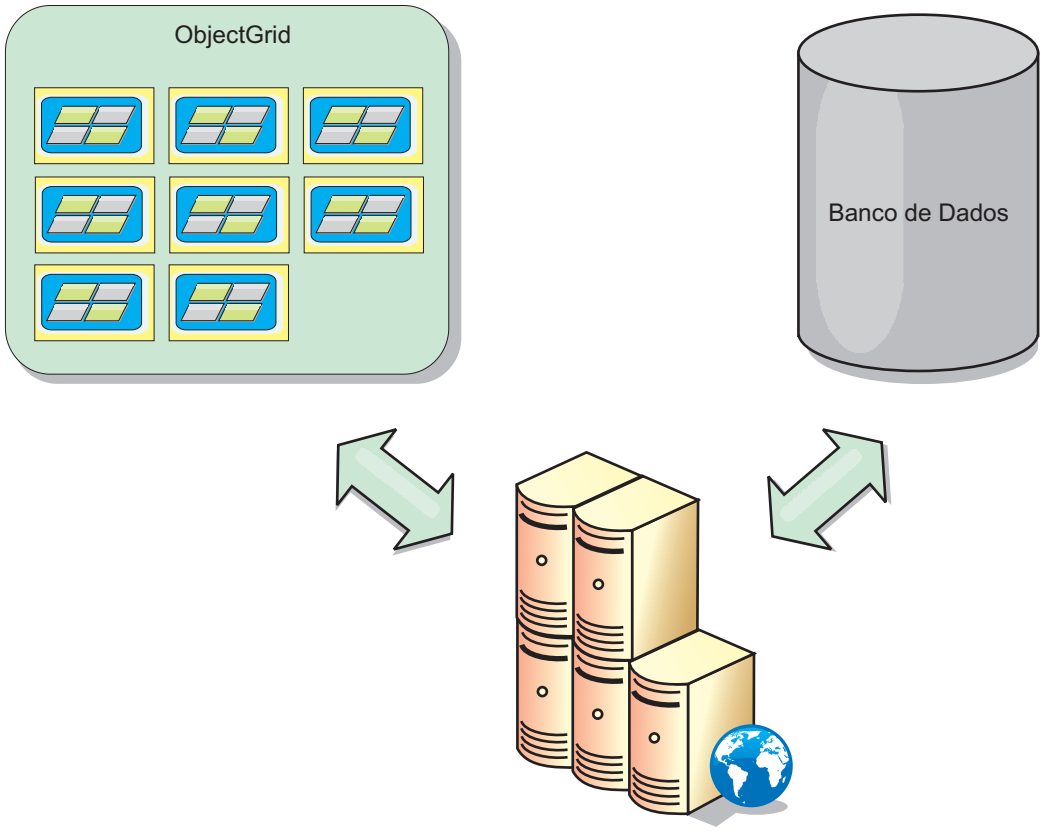


Figura 21. ObjectGrid como um Cache Secundário

Cache Disperso e Completo

O WebSphere eXtreme Scale pode ser utilizado como um cache disperso ou um cache completo. Um cache disperso mantém apenas um subconjunto do total de dados, enquanto que um cache completo mantém todos os dados. Ele também pode ser preenchido gradualmente, conforme os dados são necessários. Os caches dispersos normalmente são acessados usando chaves (ao invés de índices ou consultas) porque os dados estão disponíveis apenas parcialmente.

Cache Disperso

Quando uma chave não está presente em um cache disperso, ou os dados não estão disponíveis e uma falta de cache ocorre, a próxima camada é chamada. Os dados são buscados, a partir de um banco de dados, por exemplo, e inseridos na camada de cache da grade de dados. Se estiver usando uma consulta ou um índice, apenas os valores atualmente carregados serão acessados e as solicitações não serão encaminhadas para as outras camadas.

Cache Completo

Um cache completo contém todos os dados necessários e pode ser acessado usando atributos não-chaves com índices ou consultas. Um cache completo é pré-carregado com dados a partir do banco de dados antes que o aplicativo tente acessar os dados. Um cache completo pode funcionar como uma substituição do banco de dados após os dados serem carregados. Como todos os dados estão disponíveis, as consultas e índices podem ser usados para localizar e agregar dados.

Cache Secundário

Quando o WebSphere eXtreme Scale é usado como um cache secundário, o backend é usado com a grade de dados.

Cache Secundário

É possível configurar o produto como um cache secundário para a camada de acesso a dados de um aplicativo. Neste cenário, o WebSphere eXtreme Scale é utilizado para armazenar temporariamente objetos que normalmente poderiam ser recuperados de um banco de dados de backend. Aplicativos verificam se a grade de dados contém os dados. Se os dados estiverem na grade de dados, eles serão retornados para o responsável pela chamada. Se os dados não existirem, eles serão recuperados a partir do banco de dados de backend. Os dados são então inseridos na grade de dados para que a próxima solicitação possa usar a cópia em cache. O diagrama a seguir ilustra como o WebSphere eXtreme Scale pode ser usado como um cache secundário com uma camada de acesso a dados arbitrários, como OpenJPA ou Hibernate.

Plug-ins do cache secundário para Hibernate e OpenJPA

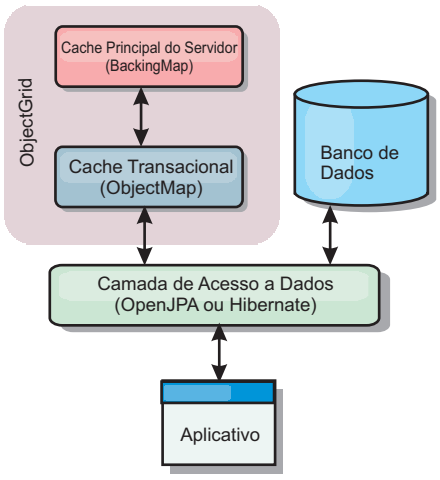


Figura 22. Cache Secundário

Os plug-ins de cache para ambos OpenJPA e Hibernate são incluídos no WebSphere eXtreme Scale, o que permite usar o produto como um cache secundário automático. Usar o WebSphere eXtreme Scale como um provedor de cache aumenta o desempenho ao ler e enfileirar dados e reduz a carga para o banco de dados. Existem vantagens que o WebSphere eXtreme Scale tem sobre as implementações de cache integrado porque o cache é automaticamente replicado entre todos os processos. Quando um cliente armazena em cache um valor, todos os outros clientes podem usar o valor em cache.

Cache Sequencial

É possível configurar em cache sequencial para um backend de banco de dados ou como um cache secundário para um banco de dados. O armazenamento em cache sequencial utiliza o eXtreme Scale como o meio principal de interação com os dados. Quando o eXtreme Scale é usado como um cache sequencial, o aplicativo interage com o backend usando um plug-in Loader.

Cache Sequencial

Quando usado como um cache sequencial, o WebSphere eXtreme Scale interage com o backend usando um plug-in Loader. Este cenário pode simplificar o acesso a dados porque os aplicativos podem acessar as APIs do eXtreme Scale diretamente. Vários cenários de armazenamento em cache diferentes são suportados no eXtreme Scale para garantir que os dados no cache e os dados no backend sejam sincronizados. O diagrama a seguir ilustra como um cache sequencial interage com o aplicativo e o back end.

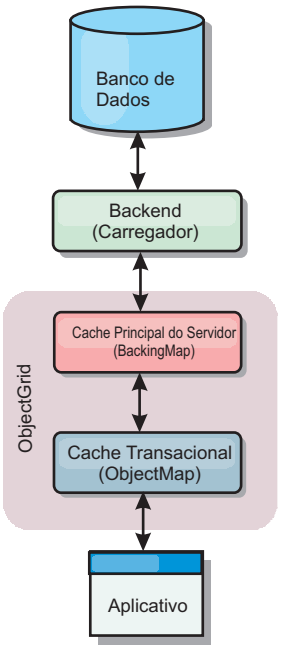


Figura 23. Cache Sequencial

A opção de armazenamento em cache em linha simplifica o acesso aos dados pois ela permite que os aplicativos acessem diretamente as APIs do eXtreme Scale. O WebSphere eXtreme Scale suporta diversos cenários de armazenamento em cache em linha, como os seguintes:

- Read-through
- Write-through

- Write-behind

Cenário de Armazenamento em Cache Read-through

Um cache read-through é um cache disperso que lentamente carrega entradas de dados por chave à medida que elas são solicitadas. Isto é feito sem exigir que o responsável pela chamada saiba quais entradas estão preenchidas. Se os dados não puderem ser localizados no cache do eXtreme Scale, o eXtreme Scale irá recuperar os dados ausentes do plug-in do utilitário de carga, que carrega os dados do banco de dados backend e insere os dados no cache. Pedidos subsequentes para a mesma chave de dados serão localizados no cache até que ele possa ser removido, invalidado ou despejado.

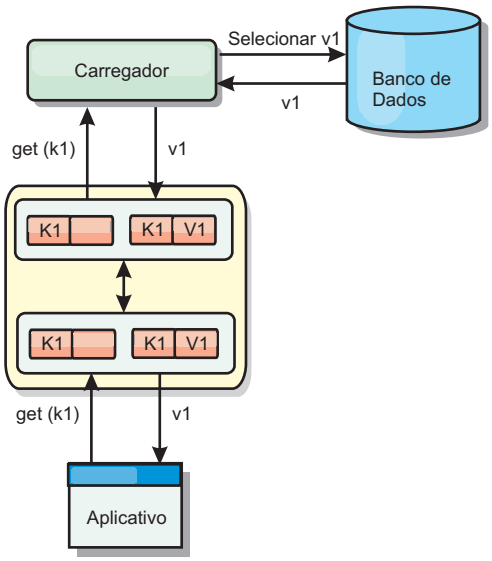


Figura 24. Armazenamento em Cache Read-through

Cenário de Armazenamento em Cache Write-through

Em um cache write-through, cada gravação no cache é gravada de maneira síncrona no banco de dados utilizando o Utilitário de Carga. Este método fornece consistência com o backend, mas diminui o desempenho de gravação pois a operação do banco de dados é síncrona. Como o cache e o banco de dados são ambos atualizados, as leituras subsequentes para os mesmos dados serão localizadas no cache, evitando a chamada do banco de dados. Um cache write-through sempre é utilizado em conjunto com um cache read-through.

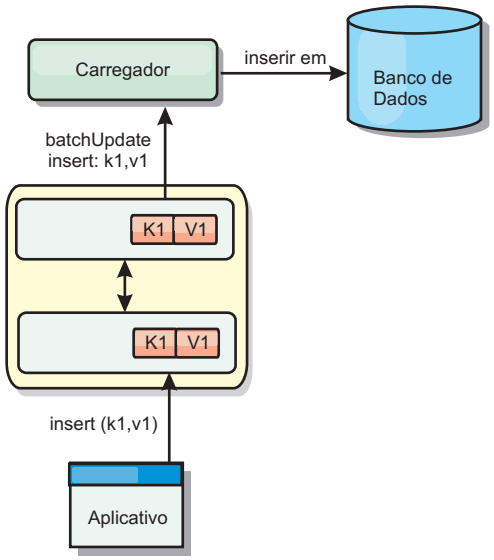


Figura 25. Armazenamento em Cache Write-through

Cenário de Armazenamento em Cache Write-behind

A sincronização do banco de dados pode ser aprimorada pela gravação de alterações de maneira assíncrona. Isto é conhecido como um cache write-behind ou write-back. Alterações que normalmente poderiam ser gravadas de maneira síncrona no utilitário de carga são, ao invés disso, armazenadas em buffer no eXtreme Scale e gravadas no banco de dados utilizando um encadeamento secundário. O desempenho de gravação é significativamente aumentado pois a operação do banco de dados é removida da transação do cliente e as gravações do banco de dados podem ser compactadas.

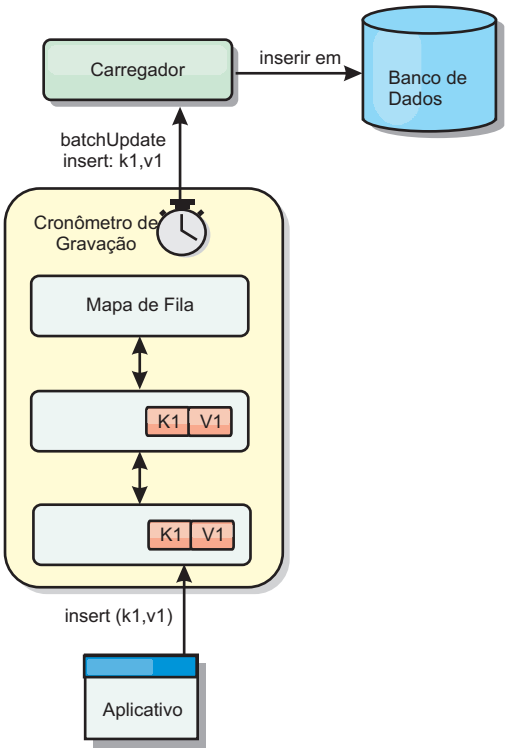


Figura 26. Armazenamento em Cache Write-behind

Armazenamento em Cache Write-behind

Java

É possível utilizar armazenamento em cache write-behind para reduzir o gasto adicional que ocorre durante a atualização de um banco de dados que você está utilizando como back end.

Visão Geral do Armazenamento em Cache Write-Behind

O armazenamento em cache write-behind enfileira assincronamente as atualizações no plug-in do Utilitário de Carga. É possível melhorar o desempenho desconectando atualizações, inserções e remoções para um mapa, a sobrecarga de atualização do banco de dados de backend. A atualização assíncrona é executada após um atraso baseado em tempo (por exemplo, cinco minutos) ou um atraso baseado em entradas (1000 entradas).

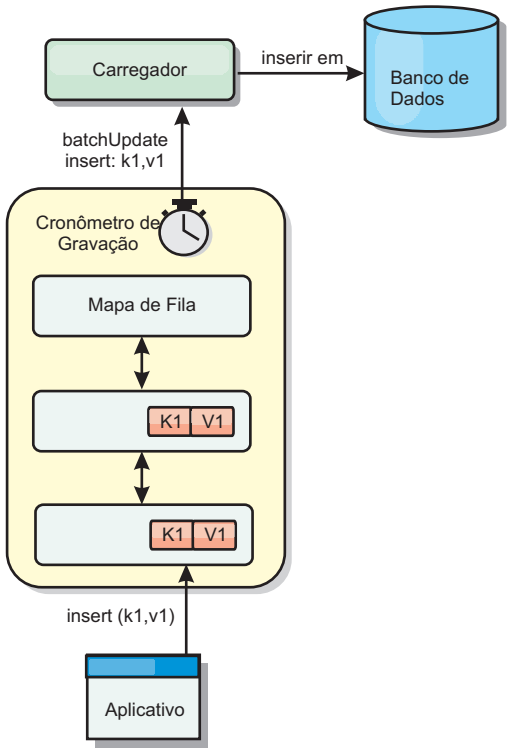


Figura 27. Armazenamento em Cache Write-behind

A configuração write-behind em um BackingMap cria um encadeamento entre o utilitário de carga e o mapa. O utilitário de carga então delega pedidos de dados através do encadeamento de acordo com as definições da configuração no método BackingMap.setWriteBehind. Quando uma transação do eXtreme Scale insere, atualiza ou remove uma entrada de um mapa, um objeto LogElement é criado para cada um destes registros. Estes elementos são enviados para o utilitário de carga write-behind e enfileirados em um ObjectMap especial denominado mapa de fila. Cada mapa de apoio com a configuração write-behind ativada possui seus próprios mapas de fila. Um encadeamento write-behind remove periodicamente os dados enfileirados dos mapas de fila e executa o push deles para o utilitário de carga de backend real.

O utilitário de carga write-behind enviará apenas os tipos insert, update e delete dos objetos LogElement para o utilitário de carga real. Todos os outros tipos de objetos LogElement, por exemplo, o tipo EVICT, são ignorados.

O suporte write-behind *é* uma extensão do plug-in do Carregador, que você usa para integrar o eXtreme Scale ao banco de dados. Por exemplo, consulte as informações do Configurando Utilitários de Carga do JPA sobre como configurar um carregador JPA.

Benefícios

Ativar o suporte write-behind possui os seguintes benefícios:

- **Isolamento de falha de backend:** O armazenamento em cache write-behind fornece uma camada de isolamento das falhas de backend. Quando o banco de dados de backend falha, as atualizações são enfileiradas no mapa de fila. Os

aplicativos podem continuar a conduzir transações para o eXtreme Scale. Quando o backend se recupera, os dados no mapa de fila são enviados para o backend.

- **Carga de backend reduzida:** O utilitário de carga write-behind mescla as atualizações em uma base de chave, portanto, apenas uma atualização mesclada por chave existe no mapa de fila. Esta mesclagem diminui o número de atualizações no backend.
- **Desempenho de transação aprimorado:** Tempos de transação do eXtreme Scale individuais são reduzidos porque a transação não precisa aguardar até que os dados sejam sincronizados com o backend.

Referências relacionadas:

Java "Exemplo: Gravando uma Classe Dumper no Modo write-behind" na página 625
Essa amostra de código de origem mostra como gravar um watcher (dumper) para manipular atualizações write-behind com falhas.

Utilitários de Carga

Java

Com um plug-in Carregador, uma grade de dados pode se comportar como um cache de memória para dados que normalmente são mantidos em um armazenamento persistente no mesmo sistema ou em outro sistema. Geralmente, um banco de dados ou sistema de arquivos é utilizado como o armazenamento persistente. Uma JVM (Java Virtual Machine) também pode ser usada como a origem de dados, permitindo que caches baseados em hub seja construído usando o eXtreme Scale. Um utilitário de carga possui a lógica para leitura e gravação de dados para um armazenamento persistente e a partir dele.

Visão Geral

Os utilitários de carga são plug-ins de mapa de apoio que são chamados quando são feitas alterações no mapa de apoio ou quando o mapa de apoio não pode atender a um pedido de dados (um erro de cache). O utilitário de carga é chamado quando o cache não pode satisfazer uma solicitação para uma chave, fornecendo capacidade read-through e lazy-population do cache. Um utilitário de carga também permite atualizações no banco de dados quando os valores do cache mudam. Todas as mudanças dentro de uma transação são agrupadas para permitir que o número de interações do banco de dados seja minimizado. Um plug-in TransactionCallback é usado em conjunto com o utilitário de carga para acionar a demarcação da transação backend. O uso deste plug-in é importante quando múltiplos mapas são incluídos em uma única transação ou quando os dados da transação forem enviados para o cache sem consolidação.

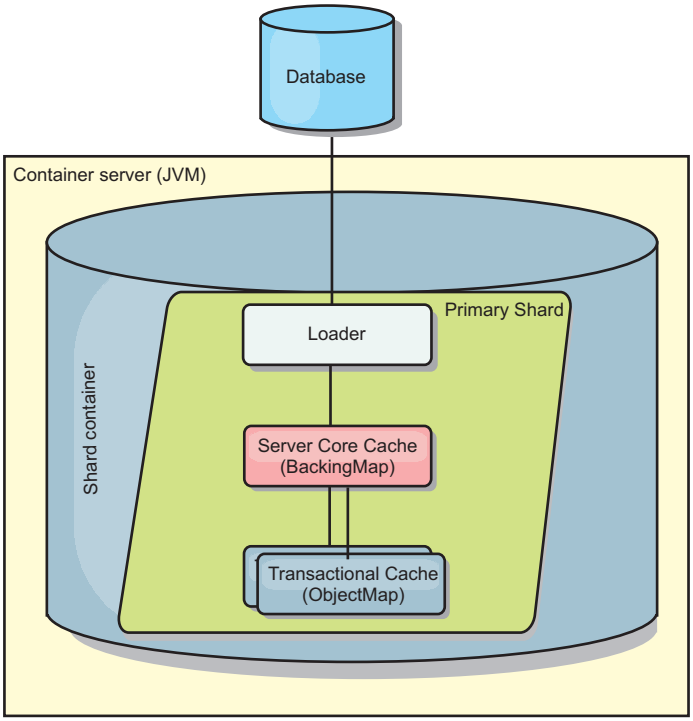


Figura 28. Utilitário de Carga

O utilitário de carga também pode usar atualizações super qualificadas para evitar manter bloqueios do banco de dados. Armazenar um atributo de versão no valor do cache, permite ao utilitário de carga ver a imagem antes e depois do valor quando ele for atualizado no cache. Este valor pode assim ser usado ao atualizar o banco de dados ou backend para verificar se os dados foram atualizados. Um Loader também pode ser configurado para pré-carregar a grade de dados quando for iniciado. Quando particionado, uma instância do utilitário de carga é associada a cada partição. Se o Mapa "Company" tiver dez partições, haverá dez instâncias do utilitário de carga, uma por partição primária. Quando shard primário para o Mapa é ativado, o método preloadMap para o utilitário de carga é chamado síncrona ou assincronamente, o qual permite o carregamento da partição do mapa com dados a partir do backend ocorra automaticamente. Quando chamado sincronamente, todas as transações do cliente são bloqueadas, evitando o acesso inconsistente à grade de dados. Como alternativa, um pré-utilitário de cliente pode ser usado para carregar a grade de dados inteira.

Dois utilitários de carga integrados podem simplificar muito a integração com back ends de banco de dados relacional. Os utilitários de carga JPA utilizam os recursos ORM (Object-Relational Mapping) de ambas as implementações OpenJPA e Hibernate da especificação JPA (Java Persistence API). Consulte “Carregadores JPA” na página 658 para obter mais informações.

Se estiver usando carregadores em uma configuração de diversos datacenters, você deverá considerar como dados de revisão e a consistência de cache são mantidos entre as grades de dados. Para obter informações adicionais, consulte “Considerações Sobre o Carregador em uma Topologia Multimestre” na página 289.

Configuração do Utilitário de Carga

Para incluir um Utilitário de Carga na configuração do BackingMap, é possível utilizar a configuração programática ou a configuração do XML. Um utilitário de carga possui o seguinte relacionamento com um mapa de apoio.

- Um mapa de apoio pode ter apenas um utilitário de carga.
- Um mapa de apoio de cliente (cache local) não pode ter um utilitário de carga.
- Uma definição de utilitário de carga pode ser aplicado a múltiplos mapas de apoio, mas cada mapa de apoio possui sua própria instância do utilitário de carga.

Referências relacionadas:

Java "Considerações sobre a Programação do Utilitário de Carga do JPA" na página 628
Um Utilitário de Carga do Java Persistence API (JPA) é uma implementação do plug-in do utilitário de carga que usa o JPA para interagir com o banco de dados. Use as seguintes considerações ao desenvolver um aplicativo que usa um utilitário de carga do JPA.

Pré-carregamento de Dados e Aquecimento

Em vários cenários que incorporam o uso de um carregador, é possível preparar sua grade de dados ao pré-carregá-lo com dados.

Quando usado como um cache completo, a grade de dados deve manter todos os dados e deve ser carregada antes que quaisquer clientes possam se conectar a ele. Quando estiver usando um cache esparso, é possível efetuar um warm-up do cache com dados para que os clientes possam ter acesso imediato aos dados quando eles se conectarem.

Existem duas abordagens para o pré-carregamento de dados na grade de dados: Usando um plug-in do Carregador ou usando um carregador do cliente, conforme descrito nas seguintes seções.

Plug-in do Utilitário de Carga

O plug-in do carregador é associado a cada mapa e é responsável pela sincronização de um único shard de partição primário com o banco de dados. O método preloadMap do plug-in do utilitário de carga é chamado automaticamente quando um shard é ativado. Por exemplo, se você tiver 100 partições, existem 100 instâncias do carregador, cada um carregando os dados para sua partição. Quando executado de modo síncrono, todos os clientes serão bloqueados até que o pré-carregamento seja concluído.

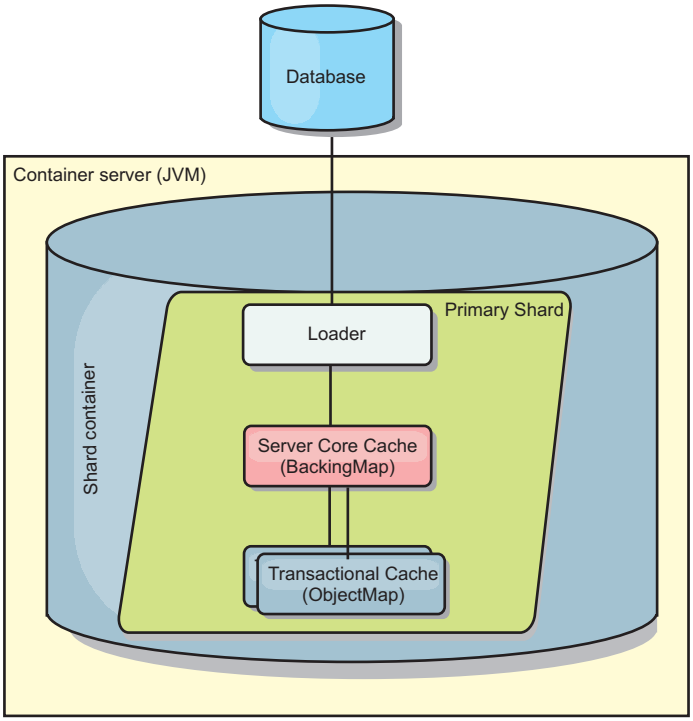


Figura 29. Plug-in do Utilitário de Carga

Consulte “Plug-ins para a Comunicação com os Bancos de Dados” na página 601 para obter mais informações.

Utilitário de Carga do Cliente

Um utilitário de carga do cliente é um padrão para uso de um ou mais clientes para carregar a grade com dados. O uso de múltiplos clientes para carregamento de dados da grade pode ser efetivo quando o esquema de partições não está armazenado no banco de dados. É possível chamar os carregadores de cliente manual ou automaticamente quando a grade de dados é iniciada. Os carregadores do cliente podem usar, opcionalmente, o StateManager para configurar o estado da grade de dados no modo de pré-carregamento, para que os clientes não possam acessar a grade enquanto ela estiver pré-carregando os dados. WebSphere eXtreme Scale inclui um carregador baseado em Java Persistence API (JPA)pode ser usado para carregar automaticamente a grade de dados com os provedores JPA OpenJPA ou Hibernate. Para obter mais informações sobre os provedores de cache, consulte Plug-in do Cache JPA Nível 2 (L2).

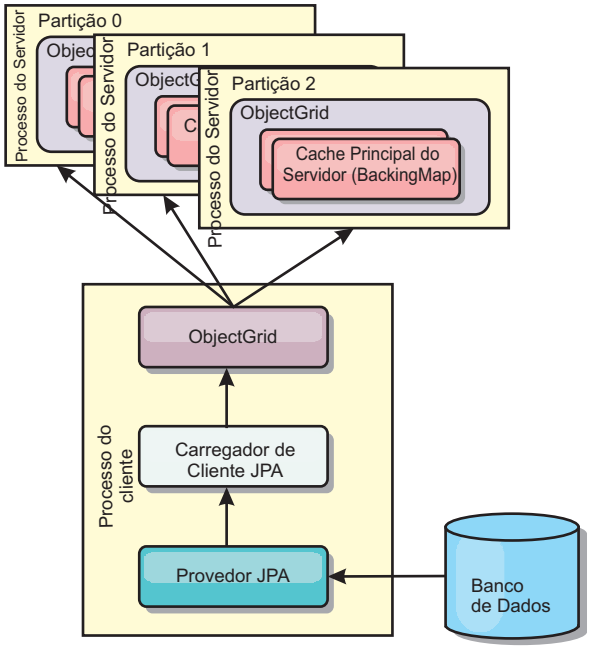


Figura 30. Utilitário de Carga do Cliente

Técnicas de Sincronização de Banco de Dados

Quando o WebSphere eXtreme Scale é utilizado como um cache, os aplicativos devem ser criados para tolerar dados antigos se o banco de dados puder ser atualizado de maneira independente de uma transação do eXtreme Scale. Para atuar como um espaço de processamento de banco de dados de memória sincronizado, o eXtreme Scale fornece várias maneiras de manter o cache atualizado.

Técnicas de Sincronização de Banco de Dados

Atualização periódica

O cache pode ser automaticamente invalidado ou atualizado automaticamente usando o atualizador de banco de dados baseado em tempo JPA (Java Persistence API).O atualizador periodicamente consulta o banco de dados usando um provedor JPA para todas as atualizações ou inserções que ocorreram desde a atualização anterior. Quaisquer alterações identificadas são automaticamente invalidadas ou atualizadas quando utilizadas com um cache disperso. Se utilizadas com um cache completo, as entradas podem ser descobertas e inseridas no cache. As entradas nunca são removidas do cache.

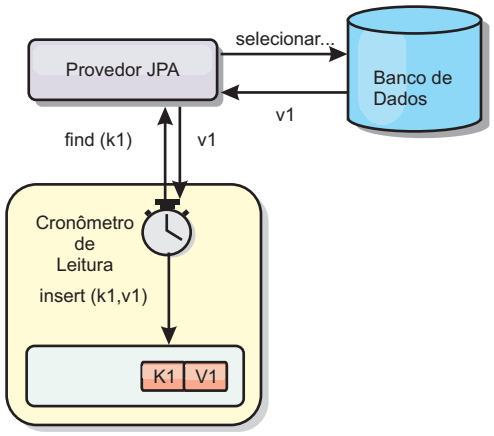


Figura 31. Atualização Periódica

Despejo

Os caches dispersos podem utilizar políticas de despejo para automaticamente remover dados do cache sem afetar o banco de dados. Há três políticas integradas incluídas no eXtreme Scale: time-to-live, least-recently-used e least-frequently-used. Todas as três políticas podem opcionalmente despejar dados mais agressivamente à medida que a memória torna-se restrita ao ativar a opção de despejo baseada em memória. Consulte o Plug-ins para Despejar Objetos de Cache para obter mais detalhes.

Invalidação Baseada em Eventos

Caches dispersos e completos podem ser invalidados ou atualizados usando um gerador de eventos como JMS (Java Message Service). A invalidação utilizando JMS pode ser manualmente vinculada a qualquer processo que atualiza o backend utilizando um acionador do banco de dados. Um plug-in ObjectGridEventListener do JMS é fornecido no eXtreme Scale que pode notificar quando o cache do servidor tiver qualquer alteração. Isto pode diminuir a quantidade de tempo que o cliente pode visualizar dados antigos.

Invalidação programática

As APIs do eXtreme Scale permitem interação manual do cache local e do servidor usando os métodos de API Session.beginNoWriteThrough(), ObjectMap.invalidate() e EntityManager.invalidate(). Se um processo do cliente ou servidor não precisar mais de uma parte dos dados, os métodos de invalidação podem ser utilizados para remover dados do cache local ou do servidor. O método beginNoWriteThrough aplica qualquer operação ObjectMap ou EntityManager para o cache local sem chamar o utilitário de carga. Se chamada a partir de um cliente, a operação é aplicável apenas para o cache local (o utilitário de carga remoto não é chamado). Se chamada no servidor, a operação é aplicável apenas ao cache principal do servidor sem chamar o utilitário de carga.

Invalidação de Dados

Para remover dados antigos do cache, você pode utilizar os mecanismos de invalidação.

Invalidação Administrativa

É possível usar o console da web ou o utilitário **xscmd** para invalidar os dados baseados na chave. É possível filtrar os dados em cache com uma expressão regular e então invalidar os dados baseados na expressão regular.

Invalidação Baseada em Evento

Caches dispersos e completos podem ser invalidados ou atualizados usando um gerador de eventos como JMS (Java Message Service). A invalidação utilizando JMS pode ser manualmente vinculada a qualquer processo que atualiza o backend utilizando um acionador do banco de dados. É fornecido um plug-in JMS ObjectGridEventListener no eXtreme Scale que pode notificar os clientes quando o cache do servidor é alterado. Esse tipo de notificação diminui a quantidade de tempo em que o cliente pode ver dados antigos.

A invalidação baseada em evento normalmente consiste nos três componentes a seguir.

- **Fila de eventos:** Uma fila de eventos armazena os eventos de mudança de dados. Ela pode ser uma fila JMS, um banco de dados, uma fila FIFO em memória ou qualquer tipo de manifesto, contanto que possa gerenciar os eventos de mudança de dados.
- **Publicador de evento:** Um publicador de evento publica os eventos de mudança de dados na fila de eventos. Um publicador de evento geralmente é um aplicativo que você cria ou uma implementação de plug-in do eXtreme Scale. O publicador de evento sabe quando os dados são alterados ou quando ele mesmo altera os dados. Quando uma transação é confirmada, eventos são gerados para os dados alterados e o publicador de eventos publica esses eventos na fila de eventos.
- **Consumidor de evento:** Um consumidor de evento consome eventos de mudança de dados. O consumidor de evento geralmente é um aplicativo para garantir que os dados da grade de destino sejam atualizados com a mudança mais recente das outras grades. Esse consumidor de evento interage com a fila de eventos para obter a mudança de dados mais recente, além de aplicar as mudanças de dados na grade de destino. Os consumidores de evento podem utilizar APIs do eXtreme Scale para invalidar dados antigos ou atualizar a grade com os dados mais recentes.

Por exemplo, JMSObjectGridEventListener tem uma opção para um modelo de cliente/servidor, no qual a fila de eventos é um destino JMS designado. Todos os processos do servidor são publicadores de eventos. Quando uma transação é confirmada, o servidor obtém as mudanças de dados e as publica no destino JMS designado. Todos os processos do cliente são consumidores de evento. Eles recebem as mudanças de dados do destino JMS designado e aplicam as mudanças no cache perto do cliente.

Consulte Configurando a Sincronização do Cliente Baseada no Serviço de Mensagens Java (JMS) para obter informações adicionais.

Invalidação Programática

As APIs do WebSphere eXtreme Scale permitem interação manual do cache local e do servidor usando os métodos de API Session.beginNoWriteThrough(), ObjectMap.invalidate() e EntityManager.invalidate(). Se um processo do cliente ou servidor não precisar mais de uma parte dos dados, os métodos de invalidação

podem ser utilizados para remover dados do cache local ou do servidor. O método beginNoWriteThrough aplica qualquer operação ObjectMap ou EntityManager para o cache local sem chamar o utilitário de carga. Se chamada a partir de um cliente, a operação é aplicável apenas para o cache local (o utilitário de carga remoto não é chamado). Se chamada no servidor, a operação é aplicável apenas ao cache principal do servidor sem chamar o utilitário de carga.

É possível utilizar invalidação programática com outras técnicas para determinar quando invalidar os dados. Por exemplo, esse método de invalidação utiliza mecanismos de invalidação baseados em evento para receber eventos de mudança de dados e depois utiliza as APIs para invalidar os dados antigos.

8.6+
Invalidação do Cache Local

Se você estiver utilizando um cache local, poderá configurar uma invalidação assíncrona que seja acionada cada vez que uma operação de atualização, exclusão, invalidação é executada na grade de dados. Como a operação é assíncrona, você ainda poderá ver dados antigos na grade de dados.

Para ativar a invalidação do cache local, configure o atributo **nearCacheInvalidationEnabled** no mapa de apoio no arquivo XML do descritor do ObjectGrid.

Indexação

Java

Use o plug-in MapIndexPlugin para construir um índice ou vários índices em um BackingMap para suportar acesso a dados sem chave.

Tipos e Configuração de Índice

O recurso de indexação é representado pelo plug-in MapIndexPlugin ou Index, para abreviar. O Índice é um plug-in BackingMap. Um BackingMap pode ter múltiplos plug-ins de Índice configurados, enquanto cada um seguir as regras de configuração de Índice.

O recurso de indexação pode ser usado para construir um ou mais índices em um BackingMap. Um índice é construído a partir de um atributo ou uma lista de atributos de um objeto no BackingMap. Este recurso fornece uma maneira para os aplicativos localizarem determinados objetos mais rapidamente. Com o recurso de indexação, os aplicativos podem localizar objetos com um valor específico ou em um intervalo com os valores de atributos indexados.

Dois tipos de indexação são possíveis: estática e dinâmica. Com a indexação estática, é necessário configurar o plug-in de índice no BackingMap antes de inicializar a instância do ObjectGrid. É possível fazer esta configuração com a configuração XML ou programática do BackingMap. A indexação estática inicia a construção de um índice durante a inicialização do ObjectGrid. O índice é sempre sincronizado com o BackingMap e está pronto para utilização. Depois de o processo de indexação estático iniciar, a manutenção do índice é parte do processo de gerenciamento de transação do eXtreme Scale. Quando as consolidações de transações mudam, estas alterações também atualizam o índice estático, e as alterações de índice são recuperadas se a transação for recuperada.

Com a indexação dinâmica, é possível criar um índice num BackingMap antes ou depois da inicialização da instância do ObjectGrid que o contém. Os aplicativos possuem controle de ciclo de vida sobre o processo de indexação dinâmica para que você possa remover um índice dinâmico quando ele não for mais necessário. Quando um aplicativo cria um índice dinâmico, o índice pode não estar pronto para utilização imediata devido ao tempo gasto na conclusão do processo de construção do índice. Como a quantidade de tempo depende da quantidade de dados indexados, a interface DynamicIndexCallback é fornecido para aplicativos que desejam receber notificações quando ocorrem determinados eventos de indexação. Estes eventos incluem ready, error e destroy. Os aplicativos podem implementar esta interface de retorno de chamada e registrar-se no processo de indexação dinâmica.

8.6+ Se um BackingMap tiver um plug-in de índice configurado, você pode obter o objeto de proxy do índice do aplicativo a partir do ObjectMap correspondente. Chamar o método getIndex no ObjectMap e passar o nome do plug-in de índice retornam o objeto de proxy do índice. Você deve lançar o objeto proxy de índice em uma interface de índice do aplicativo apropriada, tal como MapIndex, MapRangeIndex, MapGlobalIndex ou uma interface de índice customizada. Após obter o objeto de proxy do índice, é possível utilizar métodos definidos na interface do índice do aplicativo para localizar objetos armazenados em cache.

As etapas para utilizar a indexação estão resumidas na lista a seguir:

- Incluir plug-ins de indexação, estáticos ou dinâmicos, no BackingMap;
- Obter um objeto de proxy de indexação do aplicativo, emitindo o método getIndex do ObjectMap.
- Direcione o objeto de proxy de índice a uma interface de índice de aplicativo apropriado, como MapIndex, MapRangeIndex, ou uma interface de índice customizada.
- Utilizar os métodos definidos na interface Index do aplicativo para localizar objetos no cache.

8.6+ A classe HashIndex é a implementação de plug-in de índice integrada que pode suportar as seguintes interfaces de índice do aplicativo integrado:

- MapIndex
- MapRangeIndex
- MapGlobalIndex

Também é possível criar seus próprios índices. É possível incluir HashIndex como um índice estático ou dinâmico no BackingMap, obter o objeto proxy do índice MapIndex, MapRangeIndex ou MapGlobalIndex e usar o objeto proxy do índice para localizar objetos armazenados em cache.

8.6+ Índice Global

O índice global é uma extensão da classe HashIndex integrada que é executada em shards em ambientes de grade de dados distribuídos, particionados. Ele controla o local dos atributos indexados e fornece maneiras eficientes para localizar partições, chaves, valores ou entradas utilizando atributos em grandes ambientes de grade de dados particionados.

Se o índice global está ativado no plug-in HashIndex integrado, os aplicativos podem converter um objeto proxy do índice para o tipo MapGlobalIndex e utilizá-lo para localizar dados.

Índice Padrão

Se desejar iterar por meio das chaves em um mapa local, o índice padrão poderá ser usado. Este índice não requer nenhuma configuração, porém ele deve ser usado com relação ao shard, usando um agente ou uma instância do ObjectGrid recuperados a partir do método ShardEvents.shardActivated(shard do ObjectGrid).

Consideração sobre a Qualidade dos Dados

Os resultados dos métodos de consulta de índice somente representar uma captura instantânea de dados em um determinado ponto no tempo. Nenhum bloqueio contra as entradas de dados é obtido depois do retorno dos resultados para o aplicativo. O aplicativo deve estar ciente de que podem ocorrer atualizações de dados em um conjunto de dados retornado. Por exemplo, o aplicativo obtém a chave de um objeto armazenado em cache executando o método findAll de MapIndex. Este objeto de chave retornado está associado a uma entrada de dados no cache. O aplicativo deve poder executar o método get no ObjectMap para localizar um objeto fornecendo o objeto chave. Se outra transação remover o objeto de dados do cache imediatamente antes de o método get ser chamado, o resultado retornado será nulo.

Considerações sobre Desempenho de Indexação

Um dos principais objetivos do recurso de indexação é melhorar o desempenho geral do BackingMap. Se a indexação não for utilizada corretamente, o desempenho do aplicativo poderá ficar comprometido. Considere os seguintes fatores antes de usar este retorno.

- **A quantidade de transações de gravação concorrentes:** O processamento de índices pode ocorrer todas as vezes que uma transação gravar dados em um BackingMap. O desempenho será afetado se muitas transações gravarem dados no mapa simultaneamente quando um aplicativo tentar operações de consulta ao índice.
- **O tamanho do conjunto de resultados que é retornado por uma operação de consulta:** Como o tamanho do conjunto de resultados aumenta, o desempenho da consulta cai. O desempenho tente a degradas quando o tamanho do conjunto de resultados é de 15% (ou mais) do BackingMap.
- **A quantidade de índices construídos sobre o mesmo BackingMap:** Cada índice consome os recursos do sistema. Conforme a quantidade dos índices construídos sobre o BackingMap aumenta, o desempenho diminui.

A função de indexação pode aumentar significativamente o desempenho do BackingMap. Os casos ideais ocorrem quando o BackingMap possui a maioria de operações de leitura, o conjunto de resultados da consulta é de uma porcentagem pequena das entradas do BackingMap, e somente poucos índices são construídos sobre o BackingMap.

Tarefas relacionadas:

Java "Configurando o Plug-in HashIndex" na página 586
É possível configurar o HashIndex integrado, a classe com.ibm.websphere.objectgrid.plugins.index.HashIndex, com um arquivo XML, programaticamente ou com uma anotação de entidade em um mapa de entidade.

Java "Acessando Dados com Índices (API de Índice)" na página 359
Use indexação para acesso a dados mais eficiente.

Referências relacionadas:

Java "Atributos do Plug-in HashIndex" na página 589
É possível usar os seguintes atributos para configurar o plug-in HashIndex. Esses atributos definem propriedades, como se você estiver usando um atributo ou HashIndex composto ou se a indexação do intervalo estiver ativada.

Java "Atributos do Plug-in InverseRangeIndex" na página 583
É possível usar os seguintes atributos para configurar o plug-in InverseRangeIndex. Esses atributos definem propriedades sobre como o índice é construído.

Java Interface GlobalIndex

Planejando Diversas Topologias do Datacenter

Ao usar a replicação assíncrona multimestre, duas ou mais grades de dados podem se tornar cópias exatas de uns dos outros. Cada grade de dados é hospedada em um domínio do serviço de catálogo independente, com seu próprio serviço de catálogo, servidores de contêiner e um nome exclusivo. Com a replicação assíncrona multimestre, é possível usar links para conectar uma coleção de domínios do serviço de catálogo. Os domínios do serviço de catálogo são então sincronizados usando a replicação sobre os links. É possível construir quase qualquer topologia por meio da definição de links entre os domínios de serviço de catálogo.

Tarefas relacionadas:

Configurando Diversas Topologias do Datacenter
Com a replicação assíncrona multimestre, um conjunto de domínios de serviço de catálogo é vinculado. Os domínios de serviço de catálogo conectados são então sincronizado usando a replicação sobre os links. É possível definir os links usando arquivos de propriedades, no tempo de execução com programas Java Management Extensions (JMX) ou com utilitários de linha de comandos. O conjunto de links atuais para um domínio é armazenado no serviço de catálogo. É possível incluir e remover links sem reiniciar o domínio de serviço de catálogo que hospeda a grade de dados.

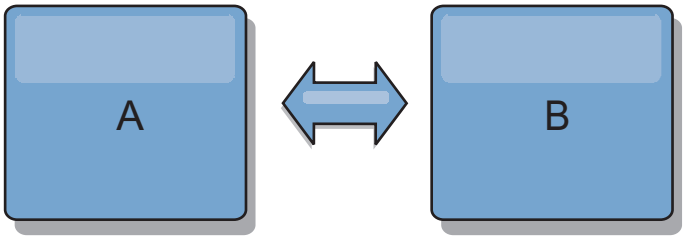
"Desenvolvendo Árbitros Customizados para a Replicação Multimestre" na página 553
Poderão ocorrer colisões de mudanças se os mesmos registros puderem ser alterados simultaneamente em dois locais. Em uma topologia de replicação multimestre, os domínios do serviço de catálogo detectam colisões automaticamente. Quando um domínio de serviço de catálogo detecta uma colisão, ele chama um árbitro. Geralmente, as colisões são resolvidas com o árbitro de colisão padrão. No entanto, um aplicativo pode fornecer um árbitro de colisão customizado.

Topologias para Replicação Multimaster

Você tem várias opções diferentes ao escolher a topologia para sua implementação que incorpora replicação multimaster.

Links Conectando domínios de serviço de catálogo

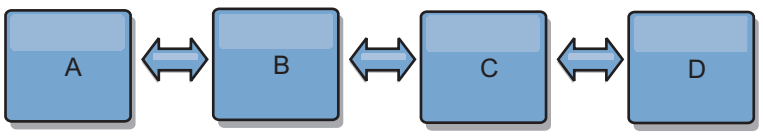
Uma infraestrutura de grade de dados de replicação é um gráfico conectado de domínios de serviço de catálogo com links bidirecionais entre eles. Com um link, dois domínios de serviço de catálogo podem comunicar as mudanças de dados. Por exemplo, a topologia mais simples é um par de domínios de serviço de catálogo com um único link entre eles. Os domínios de serviço de catálogo são nomeados em ordem alfabética: A, B, C e assim por diante, a partir da esquerda. Um link pode cruzar uma rede de longa distância (WAN), expandindo-se para grandes distâncias. Mesmo se o link for interrompido, os dados ainda poderão ser alterados em qualquer domínio de serviço de catálogo. A topologia reconcilia as mudanças quando o link reconecta os domínios de serviço de catálogo. Os links tentarão automaticamente reconectar se a conexão com a rede for interrompida.



Depois que você configura os links, o produto tenta primeiro tornar cada domínio de serviço de catálogo idêntico. Em seguida, o eXtreme Scale tenta manter as condições idênticas conforme as mudanças ocorrem em qualquer domínio de serviço de catálogo. O objetivo é que cada domínio de serviço de catálogo seja um espelho exato de qualquer outro domínio de serviço de catálogo conectado pelos links. Os links de replicação entre os domínios de serviço de catálogo ajudam a assegurar que as mudanças feitas em um domínio de serviço de catálogo sejam copiadas para os outros domínios de serviço de catálogo.

Topologias em Linha

Embora esta seja uma implementação muito simples, uma topologia em linha demonstra algumas qualidades dos links. Primeiro, não é necessário que um domínio de serviço de catálogo esteja conectado diretamente a outro domínio de serviço de catálogo para receber as mudanças. O domínio de serviço de catálogo B extrai as mudanças do domínio de serviço de catálogo A. O domínio de serviço de catálogo C recebe mudanças do domínio de serviço de catálogo A por meio do domínio de serviço de catálogo B, que conecta os domínios de serviço de catálogo A e C. De modo semelhante, o domínio de serviço de catálogo D recebe mudanças dos outros domínios de serviço de catálogo por meio do domínio de serviço de catálogo C. Essa capacidade difunde o carregamento de distribuição de mudanças para fora da origem das mudanças.



Observe que, se o domínio de serviço de catálogo C falhar, as ações a seguir ocorrerão:

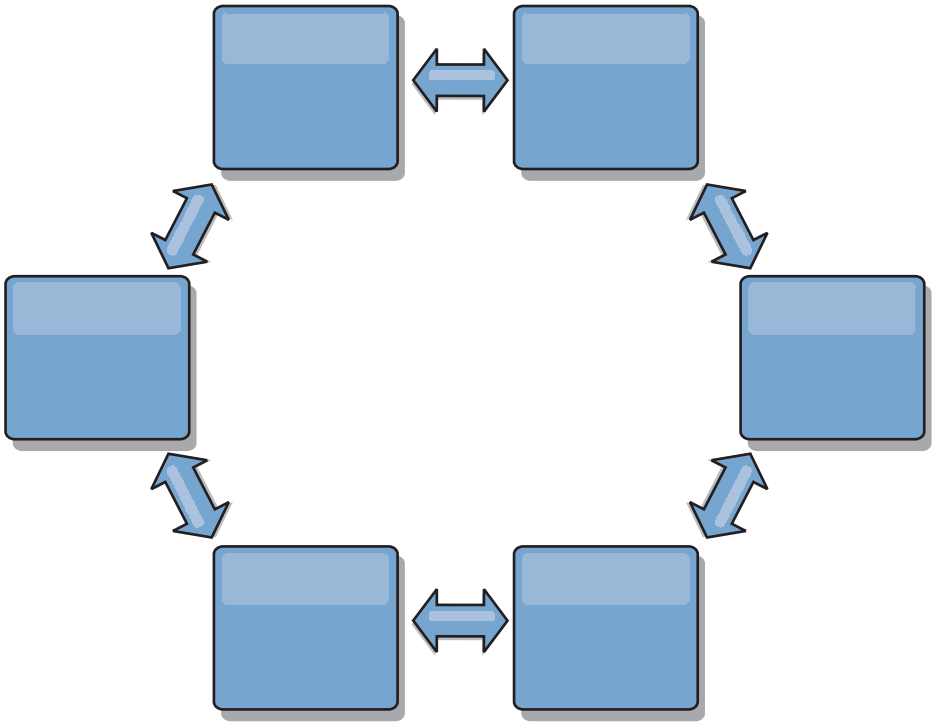
1. O domínio de serviço de catálogo D ficará órfão até o domínio de serviço de catálogo C ser reiniciado

2. O domínio de serviço de catálogo C se sincronizará com o domínio de serviço de catálogo B, que é uma cópia do domínio de serviço de catálogo A
3. O domínio de serviço de catálogo D usará o domínio de serviço de catálogo C para se sincronizar com as mudanças no domínio de serviço de catálogo A e B. Essas mudanças ocorreram inicialmente enquanto o domínio de serviço de catálogo D estava órfão (enquanto o domínio de serviço de catálogo C estava inativo).

Por fim, os domínios de serviço de catálogo A, B, C e D se tornarão todos idênticos entre si novamente.

Topologias em Anel

As topologias em anel são um exemplo de uma topologia mais resiliente. Quando um domínio de serviço de catálogo ou um único link falha, os domínios de serviço de catálogo sobreviventes ainda podem obter as mudanças. Os domínios de serviço de catálogo se deslocam ao redor do anel, longe da falha. Cada domínio de serviço de catálogo tem no máximo dois links para outros domínios de serviço de catálogo, não importa o tamanho da topologia em anel. A latência para propagar as mudanças pode ser grande. As mudanças a partir de um domínio de serviço de catálogo particular podem precisar percorrer vários links antes que todos os domínios de serviço de catálogo possuam as mudanças. Uma topologia em linha tem a mesma característica.

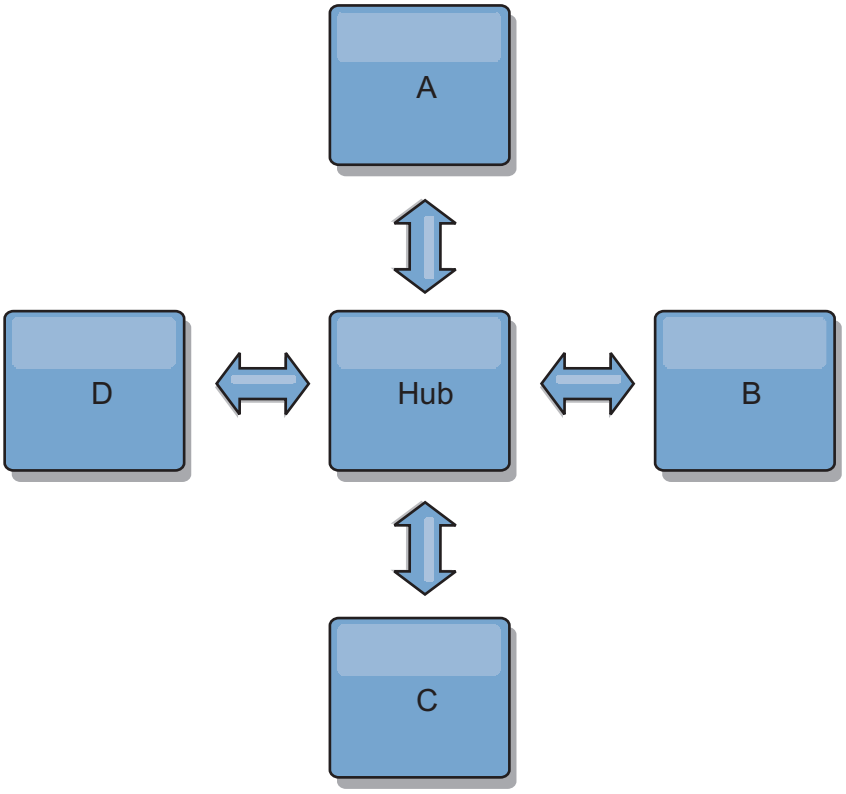


Também é possível implementar uma topologia em anel mais sofisticada, com um domínio de serviço de catálogo raiz no centro do anel. O domínio de serviço de catálogo raiz funciona como o ponto central da reconciliação. Os outros domínios de serviço de catálogo agem como pontos remotos de reconciliação para mudanças que ocorrem no domínio de serviço de catálogo raiz. O domínio de serviço de catálogo raiz pode arbitrar mudanças entre os domínios de serviço de catálogo. Se uma topologia em anel contiver mais de um anel ao redor de um domínio de serviço de catálogo raiz, o domínio de serviço de catálogo poderá arbitrar apenas

as mudanças entre o anel mais interno. No entanto, os resultados da arbitragem se difundem por todos os domínios de serviço de catálogo nos outros anéis.

Topologias Hub-and-Spoke

Com uma topologia hub-and-spoke, as mudanças percorrem um domínio de serviço de catálogo hub. Como o hub é apenas o domínio de serviço de catálogo intermediário especificado, as topologias hub-and-spoke possuem latência inferior. O domínio de serviço de catálogo hub é conectado a cada domínio de serviço de catálogo spoke por meio de um link. O hub distribui as mudanças entre os domínios de serviço de catálogo. O hub atua como um ponto de reconciliação de colisões. Em um ambiente com uma alta taxa de atualização, o hub pode precisar executar em mais hardware do que os spokes devem permanecer sincronizados. O WebSphere eXtreme Scale é projetado para escalar linearmente, o que significa que é possível aumentar o hub, conforme necessário, sem dificuldade. No entanto, se o hub falhar, as mudanças não são distribuídas até ele ser reiniciado. Quaisquer mudanças nos domínios de serviço de catálogo spoke serão distribuídas depois que o hub for reconectado.



Também é possível usar uma estratégia com clientes totalmente replicados, uma variação de topologia que usa um par de servidores sendo executados como um hub. Cada cliente cria uma grade de dados autocontida de contêiner único com um catálogo na JVM do cliente. Um cliente usa a grade de dados para se conectar com o catálogo do hub. Esta conexão faz com que o cliente seja sincronizado com o hub assim que o cliente estabelecer uma conexão com o hub.

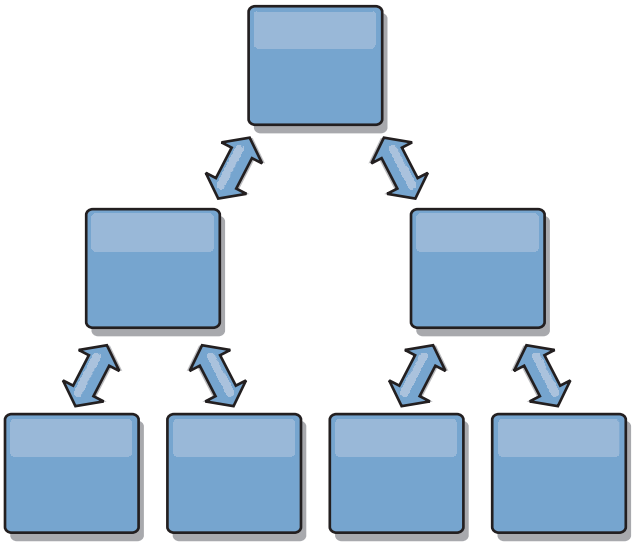
Todas as mudanças feitas pelo cliente são locais para o cliente e são replicadas de forma assíncrona para o hub. O hub age como um domínio de serviço de catálogo de arbitragem, distribuindo mudanças para todos os clientes conectados. A topologia de clientes totalmente replicados fornece um cache L2 confiável para um

mapeador relacional de objeto, como OpenJPA. As mudanças serão distribuídas rapidamente entre as JVMs de cliente por meio do hub. Se o tamanho do cache puder estar contido no espaço de heap disponível, a topologia será uma arquitetura confiável para este estilo de L2.

Use diversas partições para escalar o domínio de serviço de catálogo hub em diversas JVMs, se necessário. Como todos os dados ainda devem se ajustar em uma única JVM de cliente, diversas partições aumentam a capacidade do hub para distribuir e arbitrar as mudanças. No entanto, ter diversas partições não altera a capacidade de um único domínio de serviço de catálogo.

Topologias em Árvore

Também é possível usar uma árvore direcionada acíclica. Uma árvore acíclica não tem ciclos ou loops e uma configuração direcionada limita a criação de links apenas entre pais e filhos. Essa configuração é útil para topologias que possuem vários domínios de serviço de catálogo. Nestas topologias, não é viável ter um hub central conectado a cada spoke possível. Esse tipo de topologia também pode ser útil quando você deve incluir domínios de serviço de catálogo filhos sem atualizar o domínio de serviço de catálogo raiz.



Uma topologia em árvore ainda pode ter um ponto central de reconciliação no domínio de serviço de catálogo raiz. O segundo nível pode ainda funcionar como um ponto de reconciliação remoto para mudanças que ocorrem no domínio de serviço de catálogo abaixo dele. O domínio de serviço de catálogo raiz pode arbitrar as mudanças entre os domínios de serviço de catálogo apenas no segundo nível. Também é possível usar N árvores, cada uma delas possuindo N filhos em cada nível. Cada domínio de serviço de catálogo se conecta com *n* links.

Clientes Totalmente Replicados

Essa variação de topologia envolve um par de servidores sendo executados como um hub. Cada cliente cria uma grade de dados autocontida de contêiner único com um catálogo na JVM do cliente. Um cliente usa a grade de dados para se conectar com o catálogo do hub, fazendo com que o cliente seja sincronizado com o hub assim que estabelecer uma conexão com o hub.

Todas as mudanças feitas pelo cliente são locais para o cliente e são replicadas de forma assíncrona para o hub. O hub age como um domínio de serviço de catálogo de arbitragem, distribuindo mudanças para todos os clientes conectados. A topologia de clientes totalmente replicada fornece um bom cache L2 para um mapeador relacional de objeto, como OpenJPA. As mudanças serão distribuídas rapidamente entre as JVMs de cliente por meio do hub. Contanto que o tamanho do cache possa estar contido no espaço de heap disponível dos clientes, esta topologia será uma boa arquitetura para este estilo de L2.

Use diversas partições para escalar o domínio de serviço de catálogo hub em diversas JVMs, se necessário. Como todos os dados ainda devem se ajustar a uma única JVM de cliente, usar diversas partições aumenta a capacidade do hub para distribuir e arbitrar mudanças, mas não altera a capacidade de um único domínio de serviço de catálogo.

Tarefas relacionadas:

Configurando Diversas Topologias do Datacenter
Com a replicação assíncrona multimestre, um conjunto de domínios de serviço de catálogo é vinculado. Os domínios de serviço de catálogo conectados são então sincronizado usando a replicação sobre os links. É possível definir os links usando arquivos de propriedades, no tempo de execução com programas Java Management Extensions (JMX) ou com utilitários de linha de comandos. O conjunto de links atuais para um domínio é armazenado no serviço de catálogo. É possível incluir e remover links sem reiniciar o domínio de serviço de catálogo que hospeda a grade de dados.

"Desenvolvendo Árbitros Customizados para a Replicação Multimestre" na página 553
Poderão ocorrer colisões de mudanças se os mesmos registros puderem ser alterados simultaneamente em dois locais. Em uma topologia de replicação multimestre, os domínios do serviço de catálogo detectam colisões automaticamente. Quando um domínio de serviço de catálogo detecta uma colisão, ele chama um árbitro. Geralmente, as colisões são resolvidas com o árbitro de colisão padrão. No entanto, um aplicativo pode fornecer um árbitro de colisão customizado.

Considerações de Configuração para Topologias Multimestre

Considere os seguintes problemas ao decidir se e como usar as topologias de replicação multimestre.

- **Requisitos do conjunto de mapa**

  Os conjuntos de mapa devem ter as seguintes características para replicar as mudanças nos links de domínio do serviço de catálogo:

  – O nome do ObjectGrid e o nome do conjunto de mapas dentro de um domínio do serviço de catálogo devem corresponder ao nome do ObjectGrid e ao nome do conjunto de mapas de outros domínios de serviço de catálogo. Por exemplo, o ObjectGrid "og1" e o conjunto de mapas "ms1" devem ser configurados no domínio do serviço de catálogo A e no domínio do serviço de catálogo B para replicar os dados no conjunto de mapas entre os domínios do serviço de catálogo.

  – Ser uma grade de dados `FIXED_PARTITION`. As grades de dados `PER_CONTAINER` não podem ser replicadas.

  – Ter o mesmo número de partições em cada domínio do serviço de catálogo. O conjunto de mapa pode ou não ter o mesmo número e tipos de réplicas.

  – Ter os mesmos tipos de dados sendo replicados em cada domínio do serviço de catálogo.

– Contém os mesmos mapas e modelos de mapas dinâmicos em cada domínio do serviço de catálogo.
– Não usar o gerenciador de entidades. Um conjunto de mapas contendo um mapa de entidade não é replicado entre os domínios do serviço de catálogo.
– Não usar o suporte de armazenamento em cache write-behind. Um conjunto de mapas contendo um mapa configurado com o suporte write-behind não é replicado entre os domínios de serviço de catálogo.

Quaisquer conjuntos de mapas com as características anteriores começam a serem replicados depois que os domínios do serviço de catálogo na topologia forem iniciados.

- **Carregadores de classe com diversos domínios do serviço de catálogo**

  Os domínios do serviço de catálogo devem ter acesso a todas as classes que são usadas como chaves e valores. Todas as dependências devem ser refletidas em todos os caminhos da classe para as Java virtual machine do contêiner da grade para todos os domínios. Se um plug-in CollisionArbiter recuperar o valor para uma entrada de cache, as classes para os valores deverão estar presentes para o domínio que está iniciando o mecanismo de resolução de conflitos.

Tarefas relacionadas:

Configurando Diversas Topologias do Datacenter
Com a replicação assíncrona multimestre, um conjunto de domínios de serviço de catálogo é vinculado. Os domínios de serviço de catálogo conectados são então sincronizado usando a replicação sobre os links. É possível definir os links usando arquivos de propriedades, no tempo de execução com programas Java Management Extensions (JMX) ou com utilitários de linha de comandos. O conjunto de links atuais para um domínio é armazenado no serviço de catálogo. É possível incluir e remover links sem reiniciar o domínio de serviço de catálogo que hospeda a grade de dados.

"Desenvolvendo Árbitros Customizados para a Replicação Multimestre" na página 553
Poderão ocorrer colisões de mudanças se os mesmos registros puderem ser alterados simultaneamente em dois locais. Em uma topologia de replicação multimestre, os domínios do serviço de catálogo detectam colisões automaticamente. Quando um domínio de serviço de catálogo detecta uma colisão, ele chama um árbitro. Geralmente, as colisões são resolvidas com o árbitro de colisão padrão. No entanto, um aplicativo pode fornecer um árbitro de colisão customizado.

Considerações Sobre o Carregador em uma Topologia Multimestre

Quando estiver usando os carregadores em uma topologia multimestre, você deve considerar a possibilidade de colisão e desafios de manutenção das informações de revisão. A grade de dados mantém as informações de revisão sobre os itens nela para que colisões possam ser detectadas quando outros shards primários na configuração gravarem entradas na grade de dados. Quando as entradas são incluídas a partir de um carregador, essas informações de revisão não são incluídas e a entrada assume uma nova revisão. Como a revisão da entrada parece ser uma nova inserção, uma colisão false poderá ocorrer se outro shard primário também alterar esse estado ou obtiver as mesmas informações a partir de um carregador.

As mudanças na replicação chamam o método get no carregador com uma lista das chaves que ainda não estão na grade de dados, porém serão alteradas durante a transação da replicação. Quando a replicação ocorre, essas entradas são entradas de colisão. Quando as colisões são definidas e a revisão é aplicada, uma

atualização em lote é chamada no carregador para aplicar as mudanças no banco de dados. Todos os mapas que foram alterados na janela de revisão são atualizados na mesma transação.

Desafio do Pré-Carregamento

Considere uma topologia de dois datacenters, com o datacenter A e o datacenter B. Ambos os datacenters possuem bancos de dados independente, mas apenas o datacenter A possui uma grade de dados em execução. Quando você estabelece um link entre os datacenters por uma configuração multimestre, as grades de dados no datacenter A começam a enviar dados para as novas grades de dados do datacenter B, causando uma colisão com cada entrada. Outro maior problema que ocorre é com os dados que estão no banco de dados do datacenter B, mas não no banco de dados no datacenter A. Essas linhas não são preenchidas e definidas, resultando em inconsistências que não são resolvidas.

Solução para o Desafio de Pré-Carregamento

Como os dados que residem apenas no banco de dados não podem ter revisões, a grade de dados sempre deve ser pré-carregada completamente a partir do banco de dados local antes de estabelecer o link multimestre. Em seguida, ambas as grades de dados podem revisar e definir os dados, eventualmente chegando a um estado consistente.

Desafio de Cache Disperso

Com um cache disperso, o primeiro aplicativo tenta localizar os dados na grade de dados. Se os dados não estiverem na grade de dados, eles serão procurados no banco de dados usando o carregador. As entradas são despejadas da grade de dados periodicamente para manter um tamanho de cache pequeno.

Este tipo de cache pode ser problemático em um cenário de configuração multimestre porque as entradas dentro da grade de dados possuem metadados de revisão que ajudam a detectar quando colisões ocorrem e qual lado fez as mudanças. Quando os links entre os datacenters não estiverem funcionando, um datacenter pode atualizar uma entrada e depois, eventualmente, atualizar o banco de dados e invalidar a entrada na grade de dados. Quando o link é recuperado, os datacenters tentam sincronizar as revisões entre si. No entanto, como o banco de dados foi atualizado e a entrada da grade de dados foi invalidada, a mudança é perdida a partir da perspectiva do datacenter que ficou inativo. Como resultado, os dois lados da grade de dados estão fora de sincronização e não estão consistentes.

Solução para o Desafio de Cache Disperso

Topologia Hub e Spoke:

É possível executar o carregador apenas no hub de uma topologia de hub e spoke, mantendo a consistência dos dados, enquanto a escala da grade de dados é ajustada. No entanto, se você estiver considerando essa implementação, observe que os carregadores podem permitir que a grade de dados seja parcialmente carregada, significando que um evictor foi configurado. Se o spokes de sua configuração forem caches dispersos, mas não possuírem nenhum carregador, quaisquer perdas de cache não terão como recuperar dados do banco de dados. Devido a esta restrição, você deve usar uma topologia de cache totalmente preenchida com uma configuração de hub e spoke.

Invalidações e Despejo

Uma invalidação cria inconsistência entre a grade de dados e o banco de dados. Os dados podem ser removidos da grade de dados, seja de modo programático ou com o despejo. Ao desenvolver seu aplicativo, você deve estar ciente de que a manipulação de revisão não replica mudanças que são invalidadas, resultando em inconsistências entre os shards primários.

Os eventos de invalidação não são mudanças de estado de cache e não resultam em replicação. Todos os evictors configurados são executados independentemente de outros evictors na configuração. Por exemplo, você pode ter um evictor configurado para um limite de memória em um domínio do serviço de catálogo, e um tipo diferente de evictor menos agressivo no outro domínio do serviço de catálogo vinculado. Quando as entradas da grade dedados são removidas devido à política de limite de memória, as entradas no outro domínio do serviço de catálogo não são afetadas.

Atualizações do banco de dados e invalidação da grade de dados

Problemas ocorrem quando o banco de dados é atualizado diretamente no plano de fundo ao chamar a invalidação na grade de dados para as entradas atualizadas em uma configuração multimestre. Esse problema ocorre porque a grade de dados não pode replicar a mudança para os outros shards primários até que algum tipo de acesso ao cache mova a entrada para a grade de dados.

Diversos Gravadores para um Único Banco de Dados Lógico

Quando um banco de dados único é usado com diversos shards primários conectados por meio de um carregador, isso pode resultar em conflitos transacionais. Sua implementação do carregador deve manipular especialmente esses tipos de cenários.

Espelhando Dados Usando Replicação Multimestre

É possível configurar bancos de dados independentes que estão conectados a domínios do serviço de catálogo independentes. Nessa configuração, o carregador pode enviar mudanças de um datacenter para o outro.

Tarefas relacionadas:

Configurando Diversas Topologias do Datacenter
Com a replicação assíncrona multimestre, um conjunto de domínios de serviço de catálogo é vinculado. Os domínios de serviço de catálogo conectados são então sincronizado usando a replicação sobre os links. É possível definir os links usando arquivos de propriedades, no tempo de execução com programas Java Management Extensions (JMX) ou com utilitários de linha de comandos. O conjunto de links atuais para um domínio é armazenado no serviço de catálogo. É possível incluir e remover links sem reiniciar o domínio de serviço de catálogo que hospeda a grade de dados.

"Desenvolvendo Árbitros Customizados para a Replicação Multimestre" na página 553
Poderão ocorrer colisões de mudanças se os mesmos registros puderem ser alterados simultaneamente em dois locais. Em uma topologia de replicação multimestre, os domínios do serviço de catálogo detectam colisões automaticamente. Quando um domínio de serviço de catálogo detecta uma colisão, ele chama um árbitro. Geralmente, as colisões são resolvidas com o árbitro de colisão padrão. No entanto, um aplicativo pode fornecer um árbitro de colisão customizado.

Considerações de Design para Replicação Multimestre

Ao implementar da replicação multimestre, você deve considerar aspectos de design, como arbitragem, vinculação e desempenho.

Considerações sobre Arbitragem no Design de Topologia

Poderão ocorrer colisões de mudanças se os mesmos registros puderem ser alterados simultaneamente em dois locais. Configure cada domínio de serviço de catálogo para ter aproximadamente a mesma quantia de processador, memória e recursos de rede. Observe que os domínios de serviço de catálogo que executam a manipulação da colisão de mudanças (arbitragem) usam mais recursos que outros domínios de serviço de catálogo. As colisões são detectadas automaticamente. Elas são manipuladas com um desses dois mecanismo:

- **Árbitro de conflito padrão**: O protocolo padrão deve usar as mudanças a partir do domínio de serviço de catálogo mais baixo denominado de maneira lexical. Por exemplo, se os domínios de serviço de catálogo A e B gerarem um conflito para um registro, a mudança no domínio de serviço de catálogo B será ignorada. O domínio de serviço de catálogo A mantém sua versão e o registro no domínio de serviço de catálogo B é alterado para corresponder ao registro do domínio de serviço de catálogo A. Esse comportamento também se aplica aos aplicativos nos quais os usuários ou as sessões são normalmente ligados ou têm afinidade com uma das grades de dados.
- **Árbitro de colisão customizado**: Os aplicativos podem fornecer um árbitro customizado. Quando um domínio do serviço de catálogo detecta uma colisão, ele inicia o árbitro. Para obter informações sobre como desenvolver um árbitro útil customizado, consulte "Desenvolvendo Árbitros Customizados para a Replicação Multimestre" na página 553.

Para topologias nas quais as colisões são possíveis, considere implementar uma topologia hub-and-spoke ou uma topologia em árvore. Essas duas topologias tendem a evitar colisões constantes, o que pode acontecer nos seguintes cenários:

1. Diversos domínios de serviço de catálogo experimentam uma colisão.
2. Cada domínio de serviço de catálogo manipula a colisão localmente, produzindo revisões.

3. As revisões colidem, resultando em revisões de revisões

Para evitar colisões, escolha um domínio de serviço de catálogo específico, chamado de *domínio de serviço de catálogo de arbitragem* como o árbitro de colisão para um subconjunto de domínios de serviço de catálogo. Por exemplo, uma topologia hub-and-spoke pode usar o hub como o manipulador de colisão. O manipulador de colisão spoke ignora quaisquer colisões que forem detectadas pelos domínios de serviço de catálogo spoke. O domínio de serviço de catálogo do hub cria revisões, evitando revisões de colisão inesperadas. O domínio de serviço de catálogo designado para manipular colisões deve ser vinculado a todos os domínios os quais ele é responsável por manipular as colisões. Em uma topologia em árvore, os domínios pais internos manipulam colisões para seus filhos imediatos. Em contraste, se usar uma topologia em anel, não será possível designar um domínio de serviço de catálogo no anel como o árbitro.

A tabela a seguir resume as abordagens de arbitragem que são mais compatíveis com várias topologias.

Tabela 7. Abordagens de Arbitragem. Esta tabela define se a arbitragem de aplicativo é compatível com várias tecnologias.

Topologia	Arbitragem do Aplicativo?	Notas
Uma linha de dois domínios de serviço de catálogo	Sim	Escolha um domínio do serviço de catálogo como o árbitro.
Uma linha de três domínios de serviço de catálogo	Sim	O domínio de serviço de catálogo médio deve ser o árbitro. Considere o domínio de serviço de catálogo médio como sendo o hub em uma topologia hub-and-spoke simples.
Uma linha de mais de três domínios de serviço de catálogo	Não	A arbitragem de aplicativo não é suportada.
Um hub com N spokes	Sim	O hub com links para todos os spokes deve ser o domínio de serviço de catálogo de arbitragem.
Um anel de N domínios de serviço de catálogo	Não	A arbitragem de aplicativo não é suportada.
Uma árvore acíclica, direcionada (árvore n-ary)	Sim	Todos os nós-raiz devem classificar apenas seus descendentes diretos.

Considerações sobre Links no Design de Topologia

De forma ideal, uma topologia inclui um número mínimo de links enquanto otimiza trade-offs entre latência de mudança, tolerância a falhas e características de desempenho.

- **Latência de mudança**

  A latência de mudança é determinada pelo número de domínios de serviço de catálogo intermediários onde uma mudança deve passar antes de chegar a um domínio do serviço de catálogo específico.

  Uma topologia tem a melhor latência de mudança quando ele elimina os domínios de serviço de catálogo intermediários ao vincular cada domínio de serviço de catálogo a outro domínio. No entanto, um domínio de serviço de

catálogo deve executar o trabalho de replicação proporcionalmente ao seu número de links. Para topologias grandes, o número de links absoluto a ser definido pode causar uma carga administrativa.

A velocidade com que uma mudança é copiada para outros domínios do serviço de catálogo depende de fatores adicionais, como:

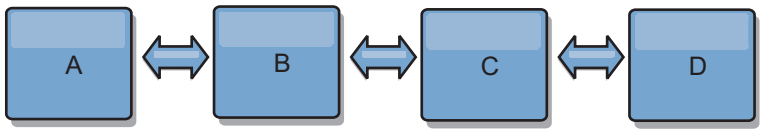
- Processador e largura da banda da rede no domínio de serviço de catálogo de origem
- O número de domínios de serviço de catálogo intermediários e de links entre o domínio de serviço de catálogo de origem e de destino
- Os recursos de processador e de rede disponíveis para os domínios de serviço de catálogo de origem, de destino e intermediários

- **Tolerância a falhas**

  A tolerância a falhas é determinada pela quantia de caminhos que existem entre dois domínios de serviço de catálogo para a replicação de mudança.

  Se houver apenas um link entre um determinado par de domínios de serviço de catálogo, uma falha de link não permitirá a propagação das mudanças. Da mesma forma, as mudanças não serão propagadas entre os domínios de serviço de catálogo se ocorrer uma falha de link em qualquer um dos domínios intermediários. Sua topologia pode ter um único link a partir de um domínio de serviço de catálogo para outro, de modo que o link passe pelos domínios intermediários. Caso positivo, as mudanças não serão propagadas se qualquer um dos domínios de serviço de catálogo intermediários estiver inativo.

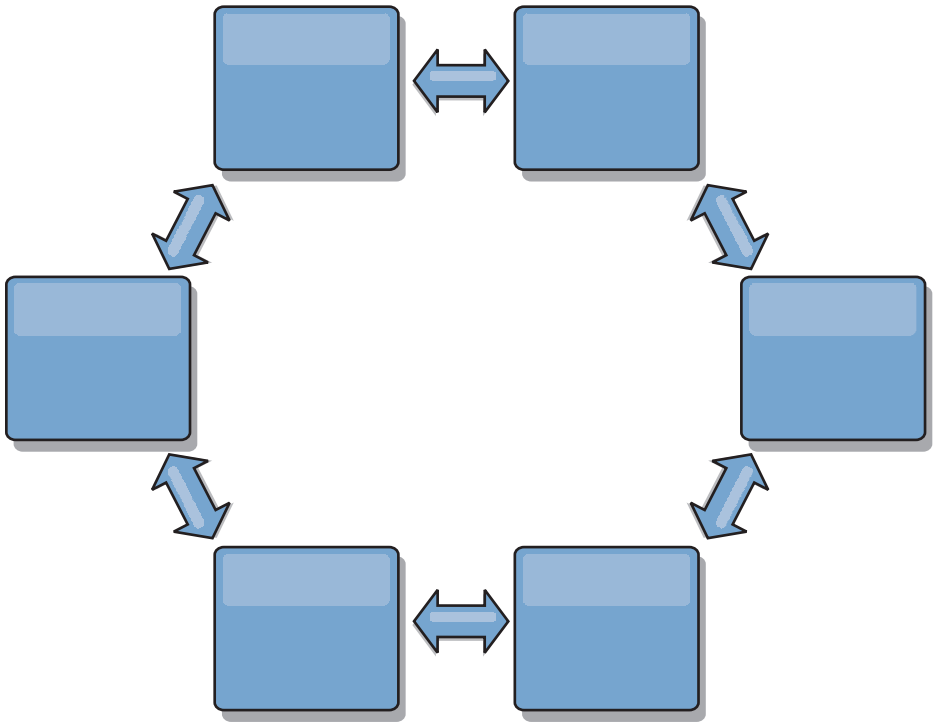
  Considere a topologia em linha com quatro domínios de serviço de catálogo, A, B, C e D:

  Se qualquer uma dessas condições for mantida, o Domínio D não verá nenhuma mudança a partir do A:

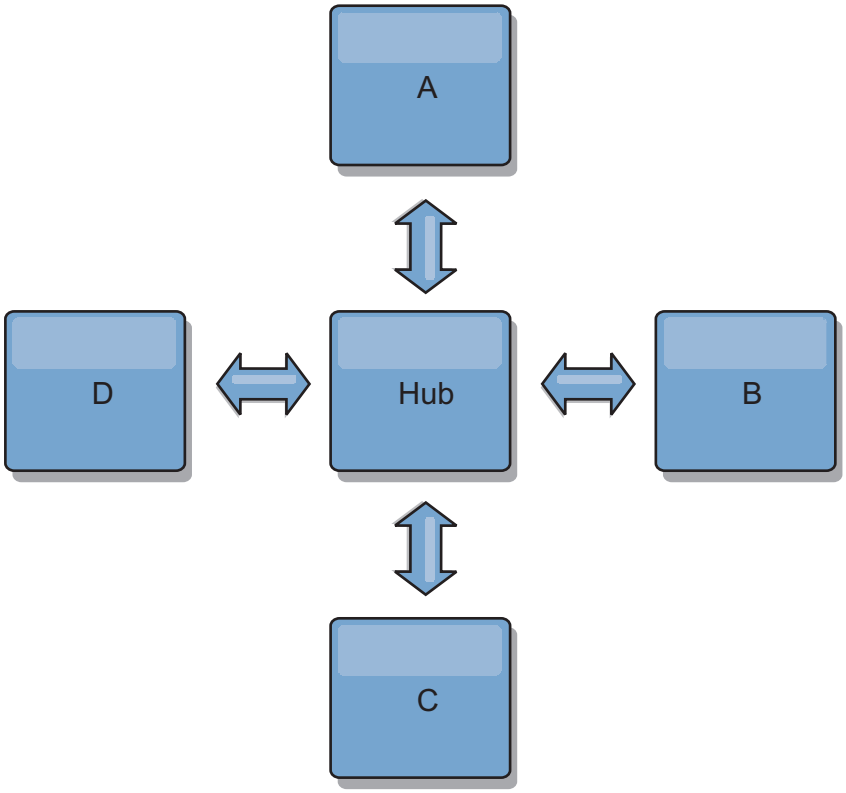
  - O Domínio A está ativo e o B está inativo
  - Os Domínios A e B estão ativos e C está inativo
  - O link entre A e B está inativo
  - O link entre B e C está inativo
  - O link entre C e D está inativo

  Em contraste, com uma topologia em anel, cada domínio de serviço de catálogo pode receber mudanças a partir de qualquer direção.



Por exemplo, se um determinado serviço de catálogo em sua topologia em anel estiver inativo, os dois domínios adjacentes ainda poderão obter as mudanças diretamente entre si.

Todas as mudanças são propagadas por meio do hub. Assim, em oposição às topologia de linha e em anel, o design hub-and-spoke será suscetível à interrupção se o hub falhar.



Um domínio de serviço de catálogo único é resiliente a uma determinada perda de quantidade de serviço. No entanto, falhas maiores, como interrupções ou perda de links em uma rede maior entre os datacenters físicos pode interromper qualquer um dos domínios de serviço de catálogo.

- **Vínculo e desempenho**

  O número de links definido em um domínio de serviço de catálogo afeta o desempenho. Mais links usam mais recursos e o desempenho de replicação pode diminuir como resultado. A capacidade de recuperar mudanças para um domínio A por meio de outros domínios isenta efetivamente o domínio A da replicação de suas transações em todo lugar. O carregamento de distribuição de mudança em um domínio é limitado pelo número de links que ele usa, e não pela quantia de domínios presentes na topologia. Esta propriedade carregamento fornece escalabilidade, de modo que os domínios na topologia possam compartilhar a carga de distribuição de mudança.

  Um domínio de serviço de catálogo pode recuperar as mudanças indiretamente por meio de outros domínios de serviço de catálogo. Considere uma topologia em linha com cinco domínios de serviço de catálogo.

  ```
  A <=> B <=> C <=> D <=> E
  ```

  – A pega mudanças de B, C, D e E por meio de B
  – B pega mudanças de A e C diretamente e mudanças de D e E por meio de C
  – C pega mudanças de B e D diretamente e mudanças de A por meio de B e E por meio de D
  – D pega mudanças de C e E diretamente e mudanças de A e B por meio de C
  – E pega mudanças de D diretamente e mudanças de A, B e C por meio de D

  O carregamento de distribuição nos domínios de serviço de catálogo A e E é o mais baixo, porque cada um deles possui um link apenas para um domínio de serviço de catálogo único. Cada um dos domínios B, C e D possui um link para dois domínios. Assim, o carregamento de distribuição nos domínios B, C e D é o dobro do carregamento nos domínios A e E. A carga de trabalho depende do número de links em cada domínio, e não do número geral de domínios na topologia. Assim, a distribuição dos carregamentos descrita permaneceria constante, mesmo se a linha contivesse 1.000 domínios.

Considerações de Desempenho de Replicação Multimestre

Leve em consideração as seguintes limitações quando usar topologias de replicação multimestre:

- **Alterar ajuste de distribuição**, conforme discutido na seção anterior.
- **Desempenho do link de replicação** O WebSphere eXtreme Scale cria um único soquete TCP/IP entre qualquer par de JVMs. Todo o tráfego entre as JVMs ocorre por meio deste soquete único, incluindo o tráfego de replicação multimestre. Os domínios do serviço de catálogo são hospedados em pelo menos *n* JVMs de contêiner, fornecendo pelo menos *n* links TCP para os domínios de serviço de catálogo equivalentes. Assim, os domínios de serviço de catálogo com números maiores de contêineres têm níveis maiores de desempenho de replicação. Mais contêineres requerem mais recursos de processador e de rede.
- **Ajuste da janela deslizante TCP e o RFC 1323** O suporte do RFC 1323 em ambas as extremidades de um link geram mais dados para um roundtrip. Este suporte resulta em maior rendimento, expandindo a capacidade da janela em um fator de aproximadamente 16.000.

  A rechamada desses soquetes TCP usa um mecanismo de janela deslizante para controlar o fluxo de dados em massa. Este mecanismo geralmente limita o

soquete para 64 KB para um intervalo de roundtrip. Se o intervalo de roundtrip for de 100 ms, a largura de banda será limitada a 640 KB/segundo sem ajuste adicional. Usar totalmente a largura de banda disponível em um link pode exigir um ajuste específico para um sistema operacional. A maioria dos sistemas operacionais inclui parâmetros de ajuste, inclusive opções RFC 1323, para aprimorar o rendimento por meio dos links de alta latência.

Vários fatores podem afetar o desempenho de replicação:

- A velocidade com que o eXtreme Scale recupera as mudanças.
- A velocidade com que o eXtreme Scale pode atender às solicitações de replicação de recuperação.
- A capacidade da janela de deslizamento.
- Com o ajuste do buffer de rede em ambos os lados de um link, o eXtreme Scale recupera as mudanças por meio do soquete de modo eficiente.

- **Serialização de Objeto** Todos os dados devem ser serializáveis. Se um domínio de serviço de catálogo não estiver usando `COPY_TO_BYTES`, o domínio de serviço de catálogo deverá usar a serialização Java ou ObjectTransformers para otimizar o desempenho da serialização.
- **Compactação** O WebSphere eXtreme Scale compacta todos os dados enviados entre os domínios de serviço de catálogo por padrão. Desativar a compactação não está disponível atualmente.
- **Ajuste de memória** O uso de memória para uma topologia de replicação multimestre é altamente independente do número de domínios de serviço de catálogo na topologia.

  A replicação multimaster inclui uma quantidade fixa de processamento por entrada de Mapa para manipular a versão. Cada contêiner também controla uma quantia fixa de dados em cada domínio de serviço de catálogo na topologia. Uma topologia com dois domínios de serviço de catálogo usa aproximadamente a mesma memória que uma topologia com 50 domínios de serviço de catálogo. O WebSphere eXtreme Scale não usa logs de reprodução ou filas semelhantes em sua implementação. Assim, não há nenhuma estrutura de recuperação pronta caso um link de replicação esteja indisponível por um período prolongado e reinícios posteriores.

Tarefas relacionadas:

Configurando Diversas Topologias do Datacenter
Com a replicação assíncrona multimestre, um conjunto de domínios de serviço de catálogo é vinculado. Os domínios de serviço de catálogo conectados são então sincronizado usando a replicação sobre os links. É possível definir os links usando arquivos de propriedades, no tempo de execução com programas Java Management Extensions (JMX) ou com utilitários de linha de comandos. O conjunto de links atuais para um domínio é armazenado no serviço de catálogo. É possível incluir e remover links sem reiniciar o domínio de serviço de catálogo que hospeda a grade de dados.

"Desenvolvendo Árbitros Customizados para a Replicação Multimestre" na página 553
Poderão ocorrer colisões de mudanças se os mesmos registros puderem ser alterados simultaneamente em dois locais. Em uma topologia de replicação multimestre, os domínios do serviço de catálogo detectam colisões automaticamente. Quando um domínio de serviço de catálogo detecta uma colisão, ele chama um árbitro. Geralmente, as colisões são resolvidas com o árbitro de colisão padrão. No entanto, um aplicativo pode fornecer um árbitro de colisão customizado.

Interoperabilidade com Outros Produtos

É possível integrar o WebSphere eXtreme Scale com outros produtos, como WebSphere Application Server e WebSphere Application Server Community Edition.

WebSphere Application Server

É possível integrar o WebSphere Application Server em vários aspectos de sua configuração do WebSphere eXtreme Scale. É possível implementar os aplicativos da grade de dados e usar o WebSphere Application Server para hospedar os servidores de contêiner e de catálogos. Ou, você pode usar um ambiente misto que tenha o WebSphere eXtreme Scale Client instalado no ambiente WebSphere Application Server com servidores de contêiner e catálogo independente. Também é possível usar a segurança do WebSphere Application Server no ambiente do WebSphere eXtreme Scale .

Produtos WebSphere Business Process Management and Connectivity

Os produtos WebSphere Business Process Management and Connectivity, incluindo o WebSphere Integration Developer, o WebSphere Enterprise Service Bus e o WebSphere Process Server, se integram aos sistemas back end, tais como CICS, serviços da web, bancos de dados ou tópicos e filas JMS. É possível incluir o WebSphere eXtreme Scale na configuração para armazenar em cache a saída destes sistemas back end, aumentando o desempenho geral de sua configuração.

WebSphere Commerce

O WebSphere Commerce pode alavancar o armazenamento em cache WebSphere eXtreme Scale como uma substituição ao cache dinâmico. Ao eliminar as entradas de cache dinâmico duplicadas e o processamento de invalidação frequente necessário para manter o cache sincronizado durante situações de alto stress, você pode melhorar o desempenho, o ajuste de escala e a alta disponibilidade.

Portal WebSphere

É possível persistir as sessões HTTP a partir do WebSphere Portal em uma grade de dados no WebSphere eXtreme Scale. Além disso, o IBM Web Content Manager no IBM WebSphere Portal pode utilizar as instâncias de cache dinâmico para armazenar conteúdo renderizado que é recuperado do Web Content Manager quando o armazenamento em cache avançado está ativado. O WebSphere eXtreme Scale oferece uma implementação de cache dinâmico que armazena o conteúdo em cache em uma grade de dados elástica em vez de utilizar a implementação de cache dinâmico padrão.

WebSphere Application Server Community Edition

O WebSphere Application Server Community Edition pode compartilhar estado de sessão, mas não de uma maneira eficiente e escalável. O WebSphere eXtreme Scale fornece uma camada de persistência distribuída e de alto desempenho, que pode ser utilizada para replicar o estado, mas não se integra prontamente a qualquer servidor de aplicativos fora do WebSphere Application Server. Estes dois produtos podem ser integrados para fornecer uma solução de gerenciamento de sessões escalável.

WebSphere Real Time

Com suporte para o WebSphere Real Time, a oferta Java real líder de mercado, o WebSphere eXtreme Scale permite que os aplicativos do Extreme Transaction Processing (XTP) tenham tempos de resposta mais consistentes e previsíveis.

Monitoramento

O WebSphere eXtreme Scale pode ser monitorado usando diversas soluções populares de monitoramento corporativo. Os agentes do plug-in estão incluídos no IBM Tivoli Monitoring and Hyperic HQ, os quais monitoram o WebSphere eXtreme Scale usando os beans de gerenciamento acessíveis. O CA Wily Introscope usa a instrumentação do método Java para capturar estatísticas.

.NET 8.6+

Ambientes Microsoft Visual Studio, IIS e .NET

Para obter mais informações sobre ambientes Microsoft Visual Studio, IIS e .NET suportados, consulte “Considerações sobre o Microsoft .NET” na página 308.

Tarefas relacionadas:

Configurando o Gerenciador de Sessões HTTP para Vários Servidores de Aplicativos
O WebSphere eXtreme Scale é fornecido com uma implementação de gerenciamento de sessões que substitui o gerenciador de sessões padrão para um contêiner da web. Esta implementação fornece replicação de sessão, alta disponibilidade, melhor escalabilidade e opções de configuração. É possível ativar o gerenciador de replicação de sessão do WebSphere eXtreme Scale e a inicialização de contêiner de ObjectGrid integrada genérica.

Configurando o Gerenciador de Sessões HTTP com WebSphere Portal
É possível persistir as sessões HTTP a partir do WebSphere Portal em uma grade de dados.

Configurando o Gerenciador de Sessões HTTP com WebSphere Application Server
Enquanto o WebSphere Application Server fornece a função de gerenciamento de sessões, o desempenho diminui conforme o número de solicitações aumenta. O WebSphere eXtreme Scale vem com uma implementação de gerenciamento de sessões que fornece opções de replicação de sessão, alta disponibilidade, melhor escalabilidade e configuração mais firme.

Configurando o WebSphere eXtreme Scale com o WebSphere Application Server
É possível executar um serviço de catálogo e processos de servidor de contêiner no WebSphere Application Server. O processo para configurar esses servidores é diferente de uma configuração independente. O serviço de catálogo pode ser iniciado automaticamente nos servidores ou gerenciadores de implementação do WebSphere Application Server. O processo do contêiner é iniciado quando um aplicativo eXtreme Scale for implementado e iniciado no ambiente do WebSphere Application Server.

Informações relacionadas:

Configure o WebSphere Commerce para usar o WebSphere eXtreme Scale para que o cache dinâmico melhore o desempenho e a escala

Integração do WebSphere Business Process Management and Connectivity

Usando o WebSphere eXtreme Scale para Aprimorar o Desempenho do WebSphere Portal e do IBM Web Content Manager

Planejando para Configuração

Antes de configurar o hardware ou software, entenda as considerações a seguir.

Planejamento para Portas de Rede

WebSphere eXtreme Scale é um cache distribuído que requer portas de abertura para comunicação entre Java virtual machines. Planeje e controle suas portas, principalmente em um ambiente com firewall, e quando estiver usando um serviço de catálogo e contêineres em diversas portas.

Importante: Quando estiver especificando os números de portas, evite configurar portas que estejam no intervalo temporário para seu sistema operacional. Se usar uma porta que esteja no intervalo temporário, poderão ocorrer conflitos de porta.

Domínio do Serviço de Catálogo

Um domínio do serviço de catálogo requer as seguintes portas para ser definido:

peerPort
Especifica a porta para o gerenciador de alta disponibilidade (HA) se

comunicar entre servidores de catálogo de peer sobre uma pilha TCP. No WebSphere Application Server, esta configuração é herdada pela configuração da porta do gerenciador de alta disponibilidade.

clientPort
Especifica a porta para servidores de catálogo acessarem dados do serviço de catálogo. No WebSphere Application Server, essa porta é configurada por meio da configuração do domínio de serviço de catálogo.

listenerPort
Especifica o número da porta ao qual o transporte Object Request Broker (ORB) ou eXtremeIO (XIO) se conecta. Essa definição configura contêineres e clientes para comunicação com o serviço de catálogo. Não WebSphere Application Server, listenerPort é herdado pela porta BOOTSTRAP_ADDRESS (quando você está usando o transporte ORB) ou pela configuração de porta XIO_address (quando você está usando o transporte XIO). Esta propriedade se aplica ao servidor de contêiner e ao serviço de catálogo.

Padrão: 2809

JMXConnectorPort
Define a porta Secure Sockets Layer (SSL) à qual o serviço Java Management Extensions (JMX) se conecta.

JMXServicePort
Especifica o número da porta na qual o servidor MBean recebe a comunicação com Java Management Extensions (JMX). A propriedade JMXServicePort especifica a porta não SSL para o JMX. Você deve usar um número da porta diferente para cada JVM na configuração. Se desejar usar JMX/RMI, especifique explicitamente **JMXServicePort** e o número da porta, mesmo se desejar usar o valor de porta padrão. Essa propriedade se aplica ao servidor de contêiner e ao serviço de catálogo. (Necessário somente para ambientes independentes.)

Padrão: 1099 para servidores de catálogos

jvmArgs (opcional)
Especifica uma lista de argumentos da Java virtual machine (JVM). Quando a segurança é ativada, você deve usar o argumento a seguir no script **startOgServer** ou **startXsServer** para configurar a porta Secure Socket Layer (SSL): -jvmArgs -Dcom.ibm.CSI.SSLPort=<sslPort>.

Servidores de Contêineres

Os servidores de contêineres do WebSphere eXtreme Scale também precisam de várias portas para operar. Por padrão, o servidor de contêiner do eXtreme Scale gera sua porta do gerenciador HA e porta do listener automaticamente com portas dinâmicas. Para um ambiente que possui um firewall, é recomendado planejar e controlar as portas. Para os servidores de contêiner para iniciar com as portas específicas, é possível usar as seguintes opções no comando **startOgServer** ou **startXsServer**.

haManagerPort
Especifica o número da porta que o gerenciador de alta disponibilidade usa. Se a propriedade não estiver configurada, uma porta livre é escolhida. Essa propriedade é ignorada nos ambientes WebSphere Application Server.

listenerPort
Especifica o número da porta ao qual o transporte Object Request Broker

(ORB) ou eXtremeIO (XIO) se conecta. Essa definição configura contêineres e clientes para comunicação com o serviço de catálogo. Não WebSphere Application Server, listenerPort é herdado pela porta BOOTSTRAP_ADDRESS (quando você está usando o transporte ORB) ou pela configuração de porta XIO_address (quando você está usando o transporte XIO). Esta propriedade se aplica ao servidor de contêiner e ao serviço de catálogo.

Padrão: 2809

JMXConnectorPort
Define a porta Secure Sockets Layer (SSL) à qual o serviço Java Management Extensions (JMX) se conecta.

JMXServicePort
Especifica o número da porta na qual o servidor MBean recebe a comunicação com Java Management Extensions (JMX). A propriedade JMXServicePort especifica a porta não SSL para o JMX. Você deve usar um número da porta diferente para cada JVM na configuração. Se desejar usar JMX/RMI, especifique explicitamente **JMXServicePort** e o número da porta, mesmo se desejar usar o valor de porta padrão. Essa propriedade se aplica ao servidor de contêiner e ao serviço de catálogo. (Necessário somente para ambientes independentes.)

Padrão: 1099 para servidores de catálogos

xioChannel.xioContainerTCPSecure.Port

Reprovado: 8.6+ Esta propriedade foi descontinuada. O valor que é especificado pela propriedade listenerPort é usado.
Especifica o número de porta SSL do eXtremeIO no servidor. Esta propriedade é usada somente quando a propriedade **transportType** é configurada como SSL-Supported ou SSL-Required.

xioChannel.xioContainerTCPNonSecure.Port

Reprovado: 8.6+ Esta propriedade foi descontinuada. O valor que é especificado pela propriedade listenerPort é usado.
Especifica o número de porta listener não segura do eXtremeIO no servidor. Se esse valor não for configurado, uma porta temporária será usada. Esta propriedade é usada somente quando a propriedade **transportType** é configurada como TCP/IP.

Restrição: A propriedade xioChannel.xioContainerTCPNonSecure.Port não é suportada no perfil do Liberty.

jvmArgs (opcional)
Especifica uma lista de argumentos da Java virtual machine (JVM). Quando a segurança é ativada, você deve usar o argumento a seguir no script **startOgServer** ou **startXsServer** para configurar a porta Secure Socket Layer (SSL): -jvmArgs -Dcom.ibm.CSI.SSLPort=<sslPort>.

Planejar adequadamente o controle da porta é essencial quando centenas de Java virtual machines são iniciadas em um servidor. Se existir um conflito de portas, os servidores de contêiner não são iniciados.

Clientes

Os clientes do WebSphere eXtreme Scale podem receber retornos de chamada de servidores quando estiver usando a API do DataGrid ou vários outros comandos. Use a propriedade **listenerPort** no arquivo de propriedades do cliente para especificar a porta na qual o cliente atende aos retornos de chamada do servidor.

haManagerPort
Especifica o número da porta que o gerenciador de alta disponibilidade usa. Se a propriedade não estiver configurada, uma porta livre é escolhida. Essa propriedade é ignorada nos ambientes WebSphere Application Server.

JVM arguments (opcional)
Especifica uma lista de argumentos da Java virtual machine (JVM). Quando a segurança está ativada, você deve usar a propriedade de sistema a seguir ao iniciar o processo do cliente: `-jvmArgs -Dcom.ibm.CSI.SSLPort=<sslPort>`.

listenerPort
Especifica o número da porta ao qual o transporte Object Request Broker (ORB) ou eXtremeIO (XIO) se conecta. Essa definição configura contêineres e clientes para comunicação com o serviço de catálogo. Não WebSphere Application Server, listenerPort é herdado pela porta BOOTSTRAP_ADDRESS (quando você está usando o transporte ORB) ou pela configuração de porta XIO_address (quando você está usando o transporte XIO). Esta propriedade se aplica ao servidor de contêiner e ao serviço de catálogo.

Padrão: 2809

Portas no WebSphere Application Server

- 8.6+ O valor **listenerPort** é herdado. O valor é diferente dependendo do tipo de transporte que você está utilizando:
  - Se estiver usando o transporte de ORB, o valor de **BOOTSTRAP_ADDRESS** para cada servidor de aplicativos do WebSphere Application Server será usado.
  - Se você estiver usando o transporte do IBM eXtremeIO, o valor **XIO_ADDRESS** será usado.
- Os valores **haManagerPort** e **peerPort** são herdados do valor **DCS_UNICAST_ADDRESS** para cada servidor de aplicativos do WebSphere Application Server.

É possível definir um domínio do serviço de catálogo no console administrativo. Para obter informações adicionais, consulte Criando Domínios do Serviço de Catálogo no WebSphere Application Server.

Você pode visualizar as portas para um determinado servidor ao clicar em um dos seguintes caminhos no console administrativo:

- WebSphere Application Server Network Deployment Versão 7.0 e posterior: **Servidores** > **Tipos de Servidor** > **WebSphere Application Servers** > *server_name* > **Portas** > ***port_name***.

Planejando Usar o IBM eXtremeMemory

Ao configurar o eXtremeMemory, é possível armazenar os objetos na memória nativa em vez de armazenar no heap Java. Ao configurar o eXtremeMemory, você pode permitir que a quantidade padrão de memória seja utilizada ou você pode calcular a quantidade de memória que deseja dedicar ao eXtremeMemory.

Antes de Iniciar

- Para aprender mais sobre o eXtremeMemory, consulte IBM eXtremeMemory.
- Você deve usar conjuntos de mapas que tenham todos os mapas configurados com os modos de cópia `COPY_TO_BYTES` ou `COPY_TO_BYTES_RAW`. Se quaisquer mapas dentro do conjunto de mapas não estiverem utilizando um desses modos de cópia, os objetos serão armazenados no heap Java .
- Linux Você deve ter o recurso compartilhado, libstdc++.so.5, instalado. Use o instalador de pacote de sua distribuição do Linux de 64 bits para instalar o arquivo de recursos necessário. Para obter informações adicionais, consulte "Resolução de Problemas do IBM eXtremeMemory" na página 875.
- Não é possível utilizar eXtremeMemory nos seguintes cenários de configuração:
  - Quando estiver usando plug-ins do evictor customizados.
  - Quando estiver usando índices compostos.
  - Quando estiver usando índices dinâmicos.
  - Quando estiver usando os carregadores write-behind integrados.
- Você deve ter uma grade de dados existente a partir da qual pode determinar os tamanhos de mapa total.

Sobre Esta Tarefa

Por padrão, o eXtremeMemory utiliza 25% da memória total no sistema. É possível alterar esse padrão com a propriedade **maxXMSize**, que especifica o número de megabytes a serem dedicados para uso pelo eXtremeMemory.

Procedimento

Opcional: Planeje o valor da propriedade **maxXMSize** apropriado para uso. Este valor configura a quantidade máxima de memória, em megabytes, que é usada pelo servidor para o eXtremeMemory.

1. Em sua configuração existente, determine o tamanho por entrada. Execute o comando **xscmd -c showMapSizes** para determinar este tamanho.
2. Calcule o valor de **maxXMSize**. Para obter tamanho total máximo de entradas (*maximum_total_size*), multiplique a *size_per_entry* * *maximum_number_of_entries*. Use no máximo 60% de **maxXMSize** para a conta para processamento de metadados. Multiplique *maximum_total_size** 1.65 para obter o valor de **maxXMSize**.

O que Fazer Depois

Conceitos relacionados:

IBM eXtremeMemory
O IBM eXtremeMemory permite que os objetos sejam armazenados na memória nativa em vez do heap Java. Movendo objetos para fora do heap Java, é possível evitar pausas da coleta de lixo, levando ao desempenho mais constante e tempos de resposta atribuíveis.

Visão Geral de Segurança

WebSphere eXtreme Scale pode proteger o acesso a dados, incluindo permissão para integração com provedores de segurança externos.

Nota: Em um armazenamento de dados fora do cache existente, como um banco de dados, provavelmente é necessário ter recursos de segurança integrados que podem não ser necessários para configuração ou ativação de modo ativo.

Entretanto, após ter armazenado seus dados em cache com o eXtreme Scale, você deve considerar a importante situação resultante de que seus recursos de segurança de backend não estão mais em vigor. É possível configurar a segurança do eXtreme Scale no níveis necessários para que a nova arquitetura armazenada em cache para os seus dados também fique segura.
A seguir é apresentado um breve resumo sobre os recursos de segurança do eXtreme Scale. Para obter mais informações detalhadas sobre como configurar a segurança, consulte o *Guia de Administração* e o *Guia de Programação*.

Fundamentos sobre Segurança Distribuída

A segurança distribuída do eXtreme Scale é baseada em três conceitos fundamentais:

Autenticação confiável
: A habilidade de determinar a identidade do solicitante. O WebSphere eXtreme Scale suporta autenticação cliente-para-servidor e servidor-para-servidor.

Autorização
: A habilidade de dar permissões para conceder direitos de acesso ao solicitante. O WebSphere eXtreme Scale suporta diferentes autorizações para várias operações.

Transporte Seguro
: A transmissão segura dos dados sobre uma rede. O WebSphere eXtreme Scale suporta os protocolos TLS/SSL (Transport Layer Security/Secure Sockets Layer).

Autenticação

O WebSphere eXtreme Scale suporta uma estrutura de cliente e servidor distribuída. Uma infraestrutura de segurança de cliente e servidor está estabelecida para proteger o acesso aos servidores eXtreme Scale. Por exemplo, quando a autenticação é necessária pelo servidor do eXtreme Scale, um cliente do eXtreme Scale deve fornecer credenciais para se autenticar no servidor. Essas credenciais podem ser um par de nome de usuário e senha, um certificado cliente, um ticket Kerberos ou dados que são apresentados em um formato acordado entre o cliente e o servidor.

Autorização

As autorizações do WebSphere eXtreme Scale são baseadas em assuntos e permissões. É possível utilizar o Java Authentication and Authorization Services (JAAS) para autorizar o acesso ou é possível conectar uma abordagem customizada, tal como Tivoli Access Manager (TAM), para tratar as autorizações. As seguintes autorizações podem ser fornecidas a um cliente ou grupo:

Autorização de mapa
: Execute operações insert, read, update, evict ou delete nos Mapas.

Autorização do ObjectGrid
: Execute consultas em objetos ou entidades nos objetos ObjectGrid.

Autorização do agente do DataGrid
: Permita que os agentes do DataGrid sejam implementados em um ObjectGrid.

Autorização do mapa do lado do servidor
Replique um mapa de servidor para o lado do cliente ou crie um índice dinâmico para o mapa do servidor.

Autorização de administração
Execute tarefas de administração.

Segurança do Transporte

Para garantir a segurança da comunicação entre cliente e o servidor, o WebSphere eXtreme Scale suporta TLS/SSL. Estes protocolos fornecem segurança da camada de transporte com autenticidade, integridade e confidencialidade para uma conexão segura entre um cliente e um servidor do eXtreme Scale.

Segurança da Grade

Em um ambiente seguro, um servidor deve poder verificar a autenticidade de outro servidor. O WebSphere eXtreme Scale utiliza um mecanismo de cadeia de chave secreta compartilhado para este propósito. Este mecanismo de chave secreta é semelhante a uma senha compartilhada. Todos os servidores eXtreme Scale aceitam uma cadeia secreta compartilhada. Quando um servidor se junta à grade de dados, o servidor é desafiado a apresentar a sequência secreta. Se a cadeia secreta do servidor que está se juntando corresponder a uma cadeia no servidor principal, então o servidor que está se juntando pode ser unir á grade. Caso contrário, o pedido de junção será rejeitado.

Não é seguro enviar um segredo em texto não-criptografado. A infraestrutura de segurança do eXtreme Scale fornece um plug-in SecureTokenManager para possibilitar que o servidor faça a segurança deste segredo antes de enviá-lo. É possível escolher como implementar a operação segura. O WebSphere eXtreme Scale fornece uma implementação, na qual a operação segura é implementada para criptografar e assinar o segredo.

Segurança Java Management Extensions (JMX) em uma Topologia de Implementação Dinâmica

A segurança JMX MBean é suportada em todas as versões do eXtreme Scale. Clientes dos MBeans do servidor de catálogos e MBeans do servidor de contêineres podem ser autenticados e o acesso às operações do MBean podem ser impostos.

Segurança Local do eXtreme Scale

A segurança local do eXtreme Scale é diferente do modelo distribuído do eXtreme Scale porque o aplicativo instancia diretamente e utiliza uma instância do ObjectGrid. Seu aplicativo e as instâncias do eXtreme Scale estão na mesma Java virtual machine (JVM). Como não há nenhum conceito de cliente/servidor neste modelo, a autenticação não é suportada. Seu aplicativo deve gerenciar sua própria autenticação e, então, passar o objeto Subject autenticado para o eXtreme Scale. Porém, o mecanismo de autorização usado para o modelo de programação do eXtreme Scale local é o mesmo que o usado para o modelo cliente/servidor.

Configuração e Programação

Para obter mais informações sobre como configurar e programar a segurança, consulte o “Integração de Segurança com Provedores Externos” na página 789 e o “API de Segurança” na página 808.

Tarefas relacionadas:

"Tutorial: Configurando a Segurança do Java SE" na página 20
Com o seguinte tutorial, é possível criar um ambiente eXtreme Scale distribuído em um ambiente Java Platform, Standard Edition.

Informações relacionadas:

"Introdução: Integre a Segurança do WebSphere eXtreme Scale com o WebSphere Application Server usando os Plug-ins do WebSphere Application Server Authentication" na página 47
Neste tutorial, integre a segurança do WebSphere eXtreme Scale com o WebSphere Application Server. Primeiro, configure a autenticação com um aplicativo da web simples que usa as credenciais do usuário autenticado a partir do encadeamento atual para se conectar ao ObjectGrid. Em seguida, investigue a criptografia dos dados que são transferidos entre o cliente e o servidor com a segurança da camada de transporte. Para conceder aos usuários diversos níveis de permissões, o Java Authentication and Authorization Service (JAAS) pode ser configurado. Depois de concluir a configuração, será possível usar o utilitário **xscmd** para monitorar suas grades de dados e mapas.

WebSphere Application Server: Protegendo Aplicativos e Seu Ambiente

Planejando para Instalação

Antes de instalar o produto, você deve considerar os requisitos de software e de hardware e as configurações de ambiente Java.

Requisitos de Hardware e Software

Pesquisar uma visão geral de hardware e de requisitos do sistema operacional. Embora não seja necessário usar um nível específico de hardware ou sistema operacional para o WebSphere eXtreme Scale, as opções de hardware e software formalmente suportadas estão disponíveis na página Requisitos do Sistema do site de suporte do produto. Se existir um conflito entre o centro de informações e a página Requisitos do Sistema, as informações no website terão precedência. As informações de pré-requisito no centro de informações são fornecidas apenas como uma conveniência.

Consulte a Página de Requisitos do Sistema para obter o conjunto de oficial de requisitos de hardware e software.

É possível instalar e implementar o produto nos ambientes do Java EE e do Java SE. Também é possível incluir em pacote configurável o componente do cliente com os aplicativos Java EE diretamente sem integrar com o WebSphere Application Server.

Requisitos de Hardware

O WebSphere eXtreme Scale não requer um nível específico de hardware. Os requisitos de hardware dependem do hardware suportado para a instalação do Java Platform, Standard Edition que é utilizado para executar o WebSphere eXtreme Scale. Se você estiver usando o eXtreme Scale com oWebSphere Application Server ou outra implementação do Java Platform, Enterprise Edition, os requisitos de hardware dessas plataformas são suficientes para oWebSphere eXtreme Scale.

Requisitos do Sistema Operacional

.NET **8.6+** Para obter detalhes sobre os requisitos para um ambiente do cliente .NET, consulte "Considerações sobre o Microsoft .NET".

Java Cada implementação de Java SE e Java EE necessita de diferentes níveis de sistema operacional ou correções para problemas que são descobertos durante o teste da implementação de Java. Os níveis que as implementações necessitam são suficientes para oeXtreme Scale.

Requisitos do Installation Manager

Antes de instalar o WebSphere eXtreme Scale, você deve instalar o Installation Manager. É possível instalar o Installation Manager usando a mídia do produto, usando um arquivo obtido do site do Passport Advantage ou usando um arquivo que contém a versão mais recente do Installation Manager a partir do Website de download do IBM Installation Manager. Consulte o Instalando o IBM Installation Manager e as ofertas do produto WebSphere eXtreme Scale para obter informações adicionais.

Requisitos do Navegador da Web

O console da web suporta os seguintes navegadores da Web:

- Mozilla Firefox, versão 3.5.x e posterior
- Microsoft Internet Explorer, versão 7 e posterior

Requisitos do WebSphere Application Server

8.6+

- WebSphere Application Server Versão 7.0.0.21 ou posterior
- WebSphere Application Server Versão 8.0.0.2 ou posterior

Consulte as Correções recomendadas para o WebSphere Application Server para obter informações adicionais.

Requisitos de Java

8.6+ Outras implementações de Java EE podem usar o tempo de execução do eXtreme Scale como uma instância local ou como um cliente para servidores eXtreme Scale. Para implementar Java SE, você deve usar a Versão 6 ou posterior.

Considerações sobre o Microsoft .NET

.NET

Dois ambientes .NET existem no WebSphere eXtreme Scale: o ambiente de desenvolvimento e o ambiente de tempo de execução. Esses ambientes têm conjuntos específicos de requisitos.

Requisitos do Ambiente de Desenvolvimento

Versão do Microsoft .NET
O .NET 3.5 e as versões mais recentes são suportados, incluindo a execução em um ambiente apenas .NET 4.0.

Microsoft Visual Studio

É possível usar uma das versões a seguir do Visual Studio:

- Visual Studio 2008 SP1
- Visual Studio 2010 SP1

Windows

Qualquer versão do Windows que é suportada pela liberação do Visual Studio que você está utilizando é suportada. Consulte os seguintes links para obter informações adicionais sobre os requisitos do Windows para Visual Studio:

- Requisitos do Sistema Visual Studio 2008
- Requisitos do Sistema Visual Studio 2010 Professional

Memória

- 1 GB (instalação de 32 bits)
- 2 GB (instalação de 64 bits)

Espaço em Disco

O WebSphere eXtreme Scale requer 50 MB de espaço em disco disponível além de quaisquer requisitos do Visual Studio.

Ambiente de Tempo de Execução

Versão do Microsoft .NET

O .NET 3.5 e as versões mais recentes são suportados, incluindo a execução em um ambiente apenas .NET 4.0.

Windows

- Windows Server 2003 (32 bits e 64 bits) Enterprise, Standard, Datacenter, Web Editions SP2
- Windows Server 2003 R2 (32 bits e 64 bits) Enterprise, Standard, Datacenter, Web Editions SP2
- Windows Server 2008 (32 bits e 64 bits) Enterprise, Standard, Datacenter, Web Editions SP2
- Windows Server 2008 R2 (32 bits e 64 bits) Enterprise, Standard, Datacenter, Web Editions SP2
-
- Hypervisor do Windows Hyper-V que hospeda qualquer uma das versões listadas do Windows

Servidor Internet Information Services (IIS)

- IIS 6.0 (fornecido com o Windows Server 2003)
- IIS 7.0 (fornecido com o Windows Server 2008)
- IIS 7.5 (fornecido com o Windows Server 2008 R2)

Memória

Espaço em Disco

O WebSphere eXtreme Scale requer 20 MB de espaço em disco disponível. Quando o rastreio está ativado, é necessário espaço em disco adicional.

WebSphere eXtreme Scaleruntime

Você deve estar usando o mecanismo de transporte eXtremeIO ao usar aplicativos clientes .NET. Para obter mais informações sobre eXtremeIO, consulte “Configurando o IBM eXtremeIO (XIO)” na página 119.

Considerações sobre o Java SE

Java

WebSphere eXtreme Scale requer Java SE 6, or Java SE 7. Em geral, as versões mais recentes do Java SE têm melhor funcionalidade e desempenho.

Versões Suportadas

É possível usar o WebSphere eXtreme Scale com o Java SE 6 e Java SE 7. A versão que você utiliza deve ser atualmente suportada pelo fornecedor do Java Runtime Environment (JRE). Se desejar utilizar SSL (Secure Sockets Layer), você deverá utilizar um IBM Runtime Environment.

O IBM Runtime Environment, o Java Technology Edition Versão 6 e Versão 7 são suportados para uso geral com o produto. A Versão 6 Liberação de Serviço 9 Fix Pack 2 é um JRE totalmente suportado instalado como parte das instalações independentes do WebSphere eXtreme Scale and WebSphere eXtreme Scale Client no diretório *wxs_install_root*/java e está disponível para ser usado por clientes e servidores. Se estiver instalando o WebSphere eXtreme Scale no WebSphere Application Server, o JRE incluído na instalação do WebSphere Application Server poderá ser usado. Para o console da web, você deve usar o IBM Runtime Environment, Java Technology Edition Versão 6 Service Release 7 e liberações de serviço posteriores apenas.

O WebSphere eXtreme Scale obtém vantagem da funcionalidade do Versão 6 e Versão 7 conforme ela se torna disponível. Geralmente, as versões mais recentes do Java Development Kit (JDK) e do Java SE têm melhor desempenho e funcionalidade.

Para obter informações adicionais, consulte Software Suportado.

Recursos do WebSphere eXtreme Scale que São Dependentes do Java SE

Tabela 8. Recursos que Requerem Java SE 6e Java SE 7.

O WebSphere eXtreme Scale usa a funcionalidade que é introduzida no Java SE 6 para fornecer os seguintes recursos do produto.

Recurso	**Suportado no Java SE 5 e liberações de serviço posteriores** **Nota:** O Java SE 5 não é suportado no WebSphere eXtreme Scale Versão 8.6	**Suportado no Java SE Versão 6 , Versão 7 e liberações de serviço posteriores**
Anotações EntityManager API (Opcional: Também é possível usar os arquivos XML)	X	X
Java Persistence API (JPA): carregador JPA, carregador do cliente JPA e atualizador baseado em tempo JPA	X	X
Despejo com base em memória (usa MemoryPoolMXBean)	X	X

Tabela 8. Recursos que Requerem Java SE 6e Java SE 7 (continuação).

O WebSphere eXtreme Scale usa a funcionalidade que é introduzida no Java SE 6 para fornecer os seguintes recursos do produto.

Recurso	**Suportado no Java SE 5 e liberações de serviço posteriores** **Nota:** O Java SE 5 não é suportado no WebSphere eXtreme Scale Versão 8.6	**Suportado no Java SE Versão 6 , Versão 7 e liberações de serviço posteriores**
Agentes de instrumentação: • `wxssizeagent.jar`: Aumenta a exatidão das métricas de mapa de bytes usados. • `ogagent.jar`: Aumenta o desempenho de entidades de acesso a campo.	X	X
Console da web para monitoramento		X

Atualizando o JDK no WebSphere eXtreme Scale

Perguntas comuns sobre o processo de upgrade para liberações do WebSphere eXtreme Scale em ambos os ambientes, independente e do WebSphere Application Server, estão a seguir:

- Como atualizar o JDK que é incluído com o WebSphere eXtreme Scale para WebSphere Application Server?

  É necessário utilizar o processo de upgrade do JDK que é disponibilizado pelo WebSphere Application Server. Para obter mais informações, consulte http://www-304.ibm.com/support/docview.wss?uid=swg21427178
- Qual versão do JDK devo utilizar ao usar o WebSphere eXtreme Scale em um ambiente do WebSphere Application Server?

  Você pode utilizar qualquer nível de JDK que seja suportado pelo WebSphere Application Server, para a versão suportada de WebSphere Application Server.

Referências relacionadas:

Script **`startOgServer`** (ORB)
(Descontinuado) O script **`startOgServer`** inicia servidores de contêiner e de catálogos que usam o mecanismo de transporte do Object Request Broker (ORB). É possível utilizar uma variedade de parâmetros quando você inicia seu servidores para ativar o rastreio, especificar números de porta e assim por diante.

Informações relacionadas:

Ajustando a Máquina Virtual IBM para Java

Considerações sobre o Java EE

Java

Conforme você se prepara para integrar o WebSphere eXtreme Scale em um ambiente Java Platform, Enterprise Edition, considere determinados itens, como versões, opções de configuração, requisitos e limitações e implementação e gerenciamento de aplicativo.

Executando Aplicativos eXtreme Scale em um Ambiente Java EE

Um aplicativo Java EE pode se conectar a um aplicativo eXtreme Scale remoto. Além disso, o ambiente do WebSphere Application Server suporta o início de um servidor eXtreme Scale conforme um aplicativo é iniciado no servidor de aplicativos.

Se você utilizar um arquivo XML para criar uma instância de ObjectGrid, e o arquivo XML estiver no módulo do arquivo enterprise archive (EAR), acesse o arquivo utilizando o método getClass().getClassLoader().getResource("META-INF/objGrid.xml") para obter um objeto URL para utilizar para criar uma instância de ObjectGrid. Substitua o nome do arquivo XML que você está utilizando na chamada de método.

É possível utilizar beans de inicialização para um aplicativo para autoinicializar uma instância do ObjectGrid quando o aplicativo for iniciado e para destruir a instância quando o aplicativo for parado. Um bean de inicialização é um bean de sessão stateless com um local remoto com.ibm.websphere.startupservice.AppStartUpHome e uma interface remota com.ibm.websphere.startupservice.AppStartUp. A interface remota possui dois métodos: o método start e o método stop. Utilize o método start para autoinicializar a instância e o método stop para destruir a instância. O aplicativo usa o método ObjectGridManager.getObjectGrid para manter uma referência à instância. Consulte o "Interagindo com um ObjectGrid Usando a Interface ObjectGridManager" na página 350 para obter mais informações.

Utilizando Carregadores de Classes

Quando módulos aplicativos que utilizam carregadores de classes diferentes compartilharem uma única instância de ObjectGrid em um aplicativo Java EE, verifique se os objetos estão armazenados no eXtreme Scale e se os plug-ins para o produto estão em um carregador comum no aplicativo.

Gerenciando o Ciclo de Vida de Instâncias do ObjectGrid em um Servlet

Para gerenciar o ciclo de vida de uma instância do ObjectGrid em um servlet, é possível usar o método init para criar a instância e o método destroy para remover a instância. Se a instância estiver armazenada em cache, ela será recuperada e manipulada no código do servlet. Consulte o "Interagindo com um ObjectGrid Usando a Interface ObjectGridManager" na página 350 para obter mais informações.

Referências relacionadas:

Script **startOgServer** (ORB)
(Descontinuado) O script **startOgServer** inicia servidores de contêiner e de catálogos que usam o mecanismo de transporte do Object Request Broker (ORB). É possível utilizar uma variedade de parâmetros quando você inicia seu servidores para ativar o rastreio, especificar números de porta e assim por diante.

Informações relacionadas:

Ajustando a Máquina Virtual IBM para Java

Convenções de Diretório

As seguintes convenções de diretório devem ser usadas em todo o documento para referenciar diretórios especiais, como *wxs_install_root* e *wxs_home*. Acesse esses

diretórios durante vários cenários diferentes, inclusive durante a instalação e durante o uso das ferramentas de linha de comandos.

wxs_install_root
O diretório *wxs_install_root* é o diretório-raiz no qual os arquivos do produto WebSphere eXtreme Scale são instalados. O diretório *wxs_install_root* pode ser o diretório no qual o archive de teste é extraído ou o diretório no qual o produto WebSphere eXtreme Scale é instalado.

- Exemplo ao extrair o teste:

  Exemplo: `/opt/IBM/WebSphere/eXtremeScale`
- Exemplo quando o WebSphere eXtreme Scale é instalado em um diretório independente:

  UNIX **Exemplo:** `/opt/IBM/eXtremeScale`

  Windows **Exemplo:** `C:\Program Files\IBM\WebSphere\eXtremeScale`
- Exemplo quando o WebSphere eXtreme Scale é integrado com o WebSphere Application Server:

  Exemplo: `/opt/IBM/WebSphere/AppServer`

wxs_home
O diretório *wxs_home* é o diretório raiz das bibliotecas, amostras e componentes do produto WebSphere eXtreme Scale. Esse diretório é o mesmo que o diretório *wxs_install_root* quando o teste é extraído. Para instalações independentes, o diretório *wxs_home* é o subdiretório `ObjectGrid` no diretório *wxs_install_root* . Para instalações que estão integradas ao WebSphere Application Server, esse diretório é o diretório `optionalLibraries/ObjectGrid` dentro do diretório *wxs_install_root*.

- Exemplo ao extrair o teste:

  Exemplo: `/opt/IBM/WebSphere/eXtremeScale`
- Exemplo quando o WebSphere eXtreme Scale é instalado em um diretório independente:

  UNIX **Exemplo:** `/opt/IBM/eXtremeScale/ObjectGrid`

  Windows **Exemplo:** *wxs_install_root*`\ObjectGrid`
- Exemplo quando o WebSphere eXtreme Scale é integrado com o WebSphere Application Server:

  Exemplo: `/opt/IBM/WebSphere/AppServer/optionalLibraries/ObjectGrid`

was_root
O diretório *was_root* é o diretório-raiz de uma instalação do WebSphere Application Server:

Exemplo: `/opt/IBM/WebSphere/AppServer`

.NET 8.6+ **net_client_home**
O diretório *net_client_home* é o diretório-raiz de uma instalação do cliente .NET.

Exemplo: `C:\Arquivos de Programas\IBM\WebSphere\eXtreme Scale .NET Client`

restservice_home
O diretório *restservice_home* é o diretório no qual as bibliotecas e amostras do serviço de dados REST do WebSphere eXtreme Scale estão localizadas. Este diretório é denominado `restservice` e é um subdiretório sob o diretório *wxs_home* .

- Exemplo para implementações independentes:

  Exemplo: `/opt/IBM/WebSphere/eXtremeScale/ObjectGrid/restservice`

  Examplo: *wxs_home*`\restservice`
- Exemplo para implementações integradas do WebSphere Application Server:

  Exemplo: `/opt/IBM/WebSphere/AppServer/optionalLibraries/ObjectGrid/restservice`

tomcat_root
O *tomcat_root* é o diretório-raiz da instalação do Apache Tomcat.

Exemplo: `/opt/tomcat5.5`

wasce_root
O *wasce_root* é o diretório-raiz da instalação do WebSphere Application Server Community Edition.

Exemplo: `/opt/IBM/WebSphere/AppServerCE`

java_home
java_home é o diretório-raiz de uma instalação de Java Runtime Environment (JRE).

UNIX **Exemplo:** `/opt/IBM/WebSphere/eXtremeScale/java`

Windows **Examplo:** *wxs_install_root*`\java`

samples_home
O *samples_home* é o diretório no qual os arquivos de amostra usados para os tutoriais são extraídos.

UNIX **Examplo:** *wxs_home*`/samples`

Windows **Examplo:** *wxs_home*`\samples`

dvd_root
O diretório *dvd_root* é o diretório-raiz do DVD que contém o produto.

Exemplo: `dvd_root/docs/`

equinox_root
O diretório *equinox_root* é o diretório raiz da instalação da estrutura do Eclipse Equinox OSGi.

Exemplo:`/opt/equinox`

user_home
O diretório *user_home* é o local no qual arquivos de usuário são armazenados, tais como perfis de segurança.

Windows `c:\Documents and Settings\`*user_name*

UNIX `/home/`*user_name*

Capacidade do Ambiente de Planejamento

Se você tiver um tamanho de conjunto de dados inicial e um tamanho de conjunto de dados projetado, é possível planejar a capacidade necessária para executar o WebSphere eXtreme Scale. Usando esses exercícios de planejamento, é possível implementar o WebSphere eXtreme Scale eficientemente para futuras mudanças e maximizar a elasticidade da grade de dados, o que não haveria com um cenário diferente, como um banco em memória ou outro tipo de banco de dados.

Ativando Estouro de Disco

Quando o estouro de disco está ativado, é possível estender a capacidade da grade de dados movendo as entradas de cache para fora da memória e para o disco. Use a propriedade diskOverflowEnabled no arquivo de propriedades de servidor para ativar o recurso de estouro de disco. Quando ativado, entradas que não se ajustam na capacidade de memória disponível dos servidores de contêineres são armazenadas no disco. O armazenamento em disco não é um armazenamento persistente. Entradas gravadas no disco são excluídas quando servidores de contêineres são reiniciados, da mesma maneira que entradas de cache armazenadas na memória são perdidas durante uma reinicialização de servidor de contêiner.

Antes de Iniciar

Você deve ativar o eXtreme Memory para este recurso funcionar. Para obter informações adicionais, consulte Configurando o IBM eXtremeMemory.

Sobre Esta Tarefa

Quando o estouro de disco está ativado, ele tenta manter as entradas de cache mais recentemente usadas na memória. O estouro de disco move as entradas de cache para o disco somente quando o número de entradas na memória exceder a alocação máxima de memória, conforme definido pela propriedade do servidor **maxXMSize**. Se existirem mais entradas do que se ajustam na memória, as entradas menos usadas recentemente serão movidas para o disco. Como resultado, as operações que acessam entradas que estão no disco são mais lentas do que o tempo de resposta para entradas que estão na memória. Após o acesso inicial, o item permanece na memória, a menos que se torne novamente uma entrada menos usada recentemente. Quando uma entrada for menos usada recentemente, ela será movida para o disco em favor de alguma outra entrada.

Procedimento

1. Pare o servidor de contêiner no qual você deseja ativar o estouro de disco. Para obter informações adicionais, consulte Parando Servidores Independentes que Utilizam o Transporte IBM eXtremeIO.
2. Configure as propriedades a seguir no arquivo de propriedades de servidor:

   diskOverflowEnabled
   Ativa o recurso de disco de estouro nativo. Você deve ativar o eXtreme Memory para este recurso funcionar.

   Padrão: `false`

   diskOverflowCapBytes
   Especifica a quantidade máxima de espaço em disco utilizado por este servidor para o estouro de disco, em bytes. O valor padrão especifica que não há limite sobre a quantidade armazenada em disco.

   Padrão: `Long.MAX_VALUE`

   diskStoragePath
   Especifica o caminho absoluto para um local de diretório utilizado para armazenar conteúdo de estouro.

   diskOverflowMinDiskSpaceBytes
   Especifica que as entradas não serão movidas para o disco se houver menos do que esta quantidade de espaço livre no diskStoragePath, em bytes.

Padrão: `0`

3. Reinicie seus servidores de contêiner. Para obter informações adicionais, consulte “Iniciando Servidores Independentes (XIO)” na página 128.

Dimensionamento de Memória e Cálculo de Contagem de Partições

É possível calcular a quantidade de memória e partições necessárias para sua configuração específica.

Atenção: Este tópico se aplica quando você **não** estiver usando o modo de cópia COPY_TO_BYTES. Se estiver usando o modo COPY_TO_BYTES, o tamanho da memória será muito menor e o procedimento de cálculo será diferente. Para obter informações adicionais sobre este modo, consulte “Ajustando o Modo de Cópia” na página 730.

O WebSphere eXtreme Scale armazena dados no espaço de endereço das Java Virtual Machines (JVM). Cada JVM fornece espaço no processador para criar, recuperar, atualizar e excluir chamadas para os dados que estão armazenados na JVM. Além disso, cada JVM fornece espaço de memória para entradas de dados e réplicas. Objetos Java variam de tamanho, assim você deve medir para fazer uma estimativa de quanta memória você precisa.

Para dimensionar a memória necessária, carregue os dados do seu aplicativo em uma única JVM. Quando o uso do heap alcança 60%, observe o número de objetos que são utilizados. Este número é a contagem máxima recomendada de objetos para cada uma de suas Java Virtual Machines. Para obter o dimensionamento mais exato, utilize dados realistas e inclua quaisquer índices definidos em seu dimensionamento porque os índices também consomem memória. A melhor forma de dimensionar o uso da memória é executar a saída **verbosegc** da coleta de lixo pois esta saída fornece os números após a coleta de lixo. É possível consultar o uso do heap em qualquer ponto específico por meio de MBeans ou programaticamente, porém essas consultas fornecem apenas uma captura instantânea atual do heap. Essa captura instantânea pode incluir lixo não coletado, portanto, usar esse método não indica precisamente a memória consumida.

Escalando a Configuração

Quantidade de shards por partição (numShardsPerPartition value)

Para calcular a quantidade de shards por partição, ou o valor de numShardsPerPartition, inclua 1 para o shard primário mais a quantidade total de shards de réplica que desejar. Para obter informações adicionais sobre o particionamento, consulte Particionamento.

```
numShardsPerPartition = 1 + total_number_of_replicas
```

Quantidade de Java Virtual Machines (valor minNumJVMs)

Para escalar sua configuração, primeiro, decida o número máximo de objetos necessários a serem armazenados no total. Para determinar a quantidade de Java Virtual Machines que precisa, use a seguinte fórmula:

```
minNumJVMS=(numShardsPerPartition * numObjs) / numObjsPerJVM
```

Arredonde este valor para cima para o valor de número inteiro mais próximo.

Quantidade de shards (valor numShards)

No tamanho de crescimento final, use 10 shards para cada JVM. Conforme descrito anteriormente, cada JVM possui um shard principal e (N-1) shards para as réplicas, ou neste caso, nove réplicas. Como você já possui uma quantidade de Java Virtual Machines para armazenar os dados, você pode multiplicar a quantidade de Java Virtual Machines por 10 para determinar a quantidade de shards:

```
numShards = minNumJVMs * 10 shards/JVM
```

Número de Partições Se uma partição tiver um shard primário e um shard de réplica, então, a partição possui dois shards (primário e de réplica). O número de partições é a contagem de shards dividido por 2, arredondado para o número primo mais próximo. Se a partição possui um primário e duas réplicas, então, o número de partições é a contagem de shards dividida por 3, arredondada para o número primo mais próximo.

```
numPartitions = numShards / numShardsPerPartition
```

Exemplo de Escala

Neste exemplo, o número de entrada inicia em 250 milhões. A cada ano, o número de entradas aumenta em cerca de 14%. Após sete anos, o número total de entrada será de 500 milhões, portanto, você deve planejar sua capacidade de acordo. Para alta disponibilidade, uma única réplica é necessária. Com uma réplica, o número de entradas duplica, ou seja, passa a ser 1 bilhão de réplicas. Como um teste, 2 milhões de entradas podem ser armazenadas em cada JVM. Utilizando os cálculos neste cenário, a seguinte configuração é necessária:

- 500 Java Virtual Machines para armazenar o número final de entradas.
- 5000 shards, calculados ao multiplicar 500 Java Virtual Machines por 10.
- 2500 partições, ou 2503 como o próximo número primo mais alto, calculados ao obter 5000 shards, divididos por dois para shards primários e de réplica.

Iniciando a Configuração

Com base nos cálculos anteriores, inicie com 250 Java Virtual Machines e cresça até 500 Java Virtual Machines ao longo de cinco anos. Com essa configuração, é possível gerenciar o crescimento incremental até chegar ao número final de entradas.

Nessa configuração, cerca de 200.000 entradas são armazenadas por partição (500 milhões de entradas dividido por 2503 partições).

Quando o número máximo de Java Virtual Machines é atingido

Quando atingir o número máximo de 500 Java Virtual Machines, sua grade de dados ainda poderá crescer. À medida que o número de Java Virtual Machines aumenta além de 500, a contagem de shards começa a diminuir abaixo de 10 para cada JVM, que está abaixo do número recomendado. Os shards começam a ficar maiores, o que pode causar problemas. Repita o processo de dimensionamento considerando novamente um crescimento futuro e reconfigure a contagem da partição. Esta prática requer um reinício completo da grade de dados, ou uma ocorrerá uma interrupção da sua grade de dados.

Número de Servidores

Atenção: Não utilize paginação em um servidor sob nenhuma circunstância.

Uma única JVM utiliza mais memória do que o tamanho do heap. Por exemplo, 1 GB de heap para uma JVM na verdade utiliza 1.4 GB de memória real. Determine a RAM livre disponível no servidor. Divida a quantidade de RAM pela memória por JVM para obter o número máximo da Java Virtual Machines no servidor.

Dimensionando a CPU por Partição para Transações

Embora a maior funcionalidade do eXtreme Scale seja sua capacidade de efetuar escala elástica, também é importante considerar o dimensionamento e o ajuste do número ideal de CPUs para efetuar scale up.

Os custos do processador incluem:

- Custos dos serviços das operações create, retrieve, update e delete a partir dos clientes
- Custo de replicação do outro Java Virtual Machines.
- Custo de invalidação
- Custo da política de desocupação
- Custo da coleta de lixo
- Custo da lógica de aplicativo
- Custo de serialização

Java Virtual Machines por servidor

Utilize dois servidores e inicie a contagem máxima de JVM por servidor. Utilize as contagens de partição calculadas da seção anterior. Em seguida, pré-carregue a Java Virtual Machines com dados suficientes para ajuste apenas nestes dois computadores. Utilize um servidor separado como um cliente. Execute uma simulação de transação realista junto a esta grade de dados de dois servidores.

Para calcular a linha de base, tente saturar o uso do processador. Se não for possível saturar o processador, então, é provável que a rede esteja saturada. Se a rede estiver saturada, inclua mais cartões de rede e execute o round robin da Java Virtual Machines sobre os vários cartões de rede.

Execute os computadores em 60% de uso do processador, meça a taxa de transações de criação, recuperação, atualização e exclusão. Esta medida fornece o rendimento nos dois servidores. Este número duplica com quatro servidores, duplica novamente em 8 servidores e assim por diante. Esta escala assume que a capacidade da rede e a capacidade do cliente também tenham a capacidade de escalar.

Como resultado, o tempo de resposta do eXtreme Scale deve ser estável à medida que o número de servidores é escalado para cima. O rendimento da transação deve escalar linearmente à medida que os computadores são incluídos na grade de dados.

Dimensionando CPUs para Transações Paralelas

As transações de partição única possuem escala de rendimento linear à medida que a grade de dados cresce. Transações paralelas são diferentes de transações de partição única, pois elas acessam um conjunto de servidores (pode ser todos os servidores).

Se uma transação acessar todos os servidores, o rendimento será limitado ao rendimento do cliente que inicia a transação ou ao servidor mais lento que está

sendo acessado. Grades de dados maiores propagam mais os dados e fornecem mais espaço do processador, memória, rede e assim por diante. Entretanto, o cliente deve aguardar que o servidor mais lento responda, e o cliente deve consumir os resultados da transação.

Quando uma transação acessa um subconjunto de servidores, M entre N servidores obtêm uma solicitação. O rendimento é então dividido N por M vezes mais rápido do que o rendimento do servidor mais lento. Por exemplo, se você tiver 20 servidores e uma transação que acessa 5 servidores, o rendimento será 4 vezes o rendimento do servidor mais lento na grade de dados.

Quando uma transação paralela é concluída, os resultados são enviados para o encadeamento do cliente que iniciou a transação. Este cliente deve então agregar os resultados únicos encadeados. Este tempo de agregação aumenta à medida que os número de servidores acessados pela transação aumentam. Entretanto, este tempo depende do aplicativo porque é possível que cada servidor retorne um resultado menor à medida que a grade de dados aumenta.

Normalmente, as transações paralelas acessam todos os servidores na grade de dados porque as partições são distribuídas de maneira uniforme pela grade. Neste caso, o rendimento é limitado ao primeiro caso.

Resumo

Com este dimensionamento, são obtidas três métricas como a seguir:

- Número de partições.
- Número de servidores que são necessários para a memória que é necessária.
- Número de servidores que são necessários para o rendimento necessário.

Se você precisar de 10 servidores para requisitos de memória mas estiver obtendo apenas 50% do rendimento necessário devido à saturação do processador, então precisa do dobro de servidores.

Para maior estabilidade, você deve executar seus servidores a um carregamento de processador de 60% e JVMheaps a um carregamento de heap de 60%. Os picos podem então conduzir o uso do processador a 80-90%, mas não execute seus servidores regularmente em níveis superiores a este.

Planejando para Desenvolver Aplicativos do WebSphere eXtreme Scale

Configure seu ambiente de desenvolvimento e aprenda onde localizar detalhes sobre as interfaces de programação disponíveis.

8.6+ Sobre Esta Tarefa

Quando você tem uma grade de dados corporativos configurada, é possível criar aplicativos Java e Microsoft .NET que acessam a mesma grade de dados. Estes ambientes de desenvolvimento possuem pré-requisitos e requisitos diferentes para investigação antes de você iniciar o desenvolvimento de seus aplicativos.

Planejamento para Desenvolver Aplicativos Microsoft .NET

Seu ambiente Microsoft .NET deve atender aos requisitos para o ambiente de desenvolvimento, a versão de .NET e assim por diante.

Considerações sobre o Microsoft .NET

.NET

Dois ambientes .NET existem no WebSphere eXtreme Scale: o ambiente de desenvolvimento e o ambiente de tempo de execução. Esses ambientes têm conjuntos específicos de requisitos.

Requisitos do Ambiente de Desenvolvimento

Versão do Microsoft .NET
O .NET 3.5 e as versões mais recentes são suportados, incluindo a execução em um ambiente apenas .NET 4.0.

Microsoft Visual Studio
É possível usar uma das versões a seguir do Visual Studio:

- Visual Studio 2008 SP1
- Visual Studio 2010 SP1

Windows
Qualquer versão do Windows que é suportada pela liberação do Visual Studio que você está utilizando é suportada. Consulte os seguintes links para obter informações adicionais sobre os requisitos do Windows para Visual Studio:

- Requisitos do Sistema Visual Studio 2008
- Requisitos do Sistema Visual Studio 2010 Professional

Memória

- 1 GB (instalação de 32 bits)
- 2 GB (instalação de 64 bits)

Espaço em Disco
O WebSphere eXtreme Scale requer 50 MB de espaço em disco disponível além de quaisquer requisitos do Visual Studio.

Ambiente de Tempo de Execução

Versão do Microsoft .NET
O .NET 3.5 e as versões mais recentes são suportados, incluindo a execução em um ambiente apenas .NET 4.0.

Windows

- Windows Server 2003 (32 bits e 64 bits) Enterprise, Standard, Datacenter, Web Editions SP2
- Windows Server 2003 R2 (32 bits e 64 bits) Enterprise, Standard, Datacenter, Web Editions SP2
- Windows Server 2008 (32 bits e 64 bits) Enterprise, Standard, Datacenter, Web Editions SP2
- Windows Server 2008 R2 (32 bits e 64 bits) Enterprise, Standard, Datacenter, Web Editions SP2
-
- Hypervisor do Windows Hyper-V que hospeda qualquer uma das versões listadas do Windows

Servidor Internet Information Services (IIS)

- IIS 6.0 (fornecido com o Windows Server 2003)
- IIS 7.0 (fornecido com o Windows Server 2008)

- IIS 7.5 (fornecido com o Windows Server 2008 R2)

Memória

Espaço em Disco
O WebSphere eXtreme Scale requer 20 MB de espaço em disco disponível. Quando o rastreio está ativado, é necessário espaço em disco adicional.

WebSphere eXtreme Scaleruntime
Você deve estar usando o mecanismo de transporte eXtremeIO ao usar aplicativos clientes .NET. Para obter mais informações sobre eXtremeIO, consulte "Configurando o IBM eXtremeIO (XIO)" na página 119.

Visão Geral da API .NET

.NET

Os aplicativos Microsoft .NET que acessam a grade de dados usam um conjunto especializado de APIs.

Planejamento para Desenvolver Aplicativos Java

Java

Antes de desenvolver aplicativos Java, você deve estar familiarizado com as APIs disponíveis, os plug-ins e quaisquer considerações que sejam necessárias.

Visão Geral da API Java

Java

O WebSphere eXtreme Scale fornece diversos recursos que são acessados programaticamente usando a linguagem de programação Java através de interfaces de programação de aplicativos (APIs) e interfaces de programação do sistema.

APIs do WebSphere eXtreme Scale

Quando estiver utilizando APIs do eXtreme Scale, você deve distinguir entre operações transacionais e não-transacionais. Uma operação transitória é uma operação executada dentro de uma transação. As APIs de ObjectMap, EntityManager, Query e DataGrid são APIs transacionais contidas no Session que é um contêiner transacional. As operações não-transitórias não estão relacionadas a uma transação, como por exemplo operações de configuração.

As APIs ObjectGrid, BackingMap e de plug-in não são transitórias. ObjectGrid, BackingMap e outras APIs de configuração são categorizadas como API Principal do ObjectGrid. Os plug-ins servem para customizar o cache para obter as funções desejadas e são categorizados como a API de Programação do Sistema. Um plug-in no eXtreme Scale é um componente que fornece um determinado tipo de função aos componentes conectáveis do eXtreme Scale que incluem ObjectGrid e BackingMap. Um recurso representa uma função ou característica específica de um componente do eXtreme Scale, incluindo ObjectGrid, Session, BackingMap, ObjectMap e assim por diante. Geralmente, os recursos são configuráveis com APIs de configuração. Os plug-ins podem ser internos, mas podem requerer o desenvolvimento de seus próprios plug-ins em algumas situações.

É possível configurar normalmente o ObjectGrid e o BackingMap para atender aos requisitos do seu aplicativo. Quando o aplicativo possui requisitos especiais, considere o uso de plug-ins especializados. O WebSphere eXtreme Scale pode ter

plug-ins integrados que atendam aos seus requisitos. Por exemplo, se for necessário um modelo de replicação ponto a ponto entre duas instâncias do ObjectGrid ou duas grades distribuídas do eXtreme Scale, o JMSObjectGridEventListener integrado estará disponível. Se nenhum dos plug-ins internos puder resolver seus problemas de negócios, consulte a API de Programação do Sistema para fornecer seus próprios plug-ins.

ObjectMap é uma API baseada em mapa simples. Se os objetos armazenados em cache forem simples e nenhum relacionamento estiver envolvido, a API do ObjectMap será ideal para seu aplicativo. Se os relacionamentos de objetos estiverem envolvidos, use a API EntityManager, que suporta relacionamentos como gráfico.

Query é um mecanismo poderoso para localização de dados no ObjectGrid. Session e EntityManager fornecem o recurso de consulta tradicional.

A API do DataGrid é um recurso de computação poderoso em um ambiente distribuído do eXtreme Scale que envolve muitas máquinas, réplicas e partições. Os aplicativos podem executar lógica de negócios em paralelo a todos os nós do ambiente distribuído do eXtreme Scale. O aplicativo pode obter a API do DataGrid por meio da API do ObjectMap.

O serviço de dados REST do WebSphere eXtreme Scale é um serviço HTTP Java que é compatível com Microsoft WCF Data Services (formalmente, ADO.NET Data Services) e que implementa o Open Data Protocol (OData). O serviço de dados REST permite que qualquer cliente HTTP acesse uma grade do eXtreme Scale. Ele é compatível com o suporte do WCF Data Services fornecido com o Microsoft .NET Framework 3.5 SP1. Aplicativos RESTful podem ser desenvolvidos com um rico conjunto de ferramentas fornecido pelo Microsoft Visual Studio 2008 SP1. Para obter mais detalhes, consulte o Guia do Usuário do Serviço de Dados REST do eXtreme Scale.

Tarefas relacionadas:

“Introdução ao Desenvolvimento de Aplicativos” na página 254
Para iniciar o desenvolvimento de aplicativos WebSphere eXtreme Scale, você deve configurar seu ambiente de desenvolvimento, aprender sobre APIs que podem ser usadas e, em seguida, desenvolver e testar seu aplicativo.

“Acessando a Documentação da API Java” na página 338
É possível acessar a documentação da API Java para WebSphere eXtreme Scale fazendo download de um archive de arquivo zip, incorporando a documentação da API em seu ambiente de desenvolvimento ou visualizando a documentação da API no centro de informações.

“Configurando o Ambiente de Desenvolvimento Java” na página 337
Antes de iniciar o desenvolvimento de aplicativos Java, você deve configurar seu ambiente de desenvolvimento.

“Configurando um Ambiente de Desenvolvimento Independente no Eclipse” na página 339
Configure um ambiente de desenvolvimento integrado baseado no Eclipse para construir e executar um aplicativo Java SE com a versão independente do WebSphere eXtreme Scale.

“Executando um Aplicativo Cliente ou do Servidor do WebSphere eXtreme Scale com o Apache Tomcat no Rational Application Developer” na página 341
Independente se você tiver um aplicativo cliente ou do servidor, use as mesmas etapas básicas para executar o aplicativo no Apache Tomcat no Rational Application Developer. Para um aplicativo cliente, você deseja configurar e executar um aplicativo da web para usar um cliente do WebSphere eXtreme Scale no Rational Application Developer. Siga estas instruções para criar um projeto da Web para executar um contêiner ou serviço de catálogo do WebSphere eXtreme Scale. Para um aplicativo do servidor, você deseja ativar um aplicativo Java EE na interface do Rational Application Developer com uma instalação independente do WebSphere eXtreme Scale. Siga estas instruções para configurar um projeto do aplicativo Java EE para usar a biblioteca do cliente do WebSphere eXtreme Scale.

“Executando um Cliente ou um Servidor de Aplicativos Integrado com o WebSphere Application Server no Rational Application Developer” na página 344
Configure e execute um aplicativo Java EE com um cliente ou servidor WebSphere eXtreme Scale com o tempo de execução integrado do WebSphere Application Server no Rational Application Developer. Se estiver configurando um servidor, iniciar o WebSphere Application Server inicia automaticamente o WebSphere eXtreme Scale.

“Introdução ao Desenvolvimento de Aplicativos” na página 254
Para iniciar o desenvolvimento de aplicativos WebSphere eXtreme Scale, você deve configurar seu ambiente de desenvolvimento, aprender sobre APIs que podem ser usadas e, em seguida, desenvolver e testar seu aplicativo.

Java “Acessando a Documentação da API Java” na página 338
É possível acessar a documentação da API Java para WebSphere eXtreme Scale fazendo download de um archive de arquivo zip, incorporando a documentação da API em seu ambiente de desenvolvimento ou visualizando a documentação da API no centro de informações.

Java “Configurando o Ambiente de Desenvolvimento Java” na página 337
Antes de iniciar o desenvolvimento de aplicativos Java, você deve configurar seu ambiente de desenvolvimento.

Java “Configurando um Ambiente de Desenvolvimento Independente no Eclipse” na página 339
Configure um ambiente de desenvolvimento integrado baseado no Eclipse para construir e executar um aplicativo Java SE com a versão independente do

WebSphere eXtreme Scale.

Java "Executando um Aplicativo Cliente ou do Servidor do WebSphere eXtreme Scale com o Apache Tomcat no Rational Application Developer" na página 341
Independente se você tiver um aplicativo cliente ou do servidor, use as mesmas etapas básicas para executar o aplicativo no Apache Tomcat no Rational Application Developer. Para um aplicativo cliente, você deseja configurar e executar um aplicativo da web para usar um cliente do WebSphere eXtreme Scale no Rational Application Developer. Siga estas instruções para criar um projeto da Web para executar um contêiner ou serviço de catálogo do WebSphere eXtreme Scale. Para um aplicativo do servidor, você deseja ativar um aplicativo Java EE na interface do Rational Application Developer com uma instalação independente do WebSphere eXtreme Scale. Siga estas instruções para configurar um projeto do aplicativo Java EE para usar a biblioteca do cliente do WebSphere eXtreme Scale.

Java "Executando um Cliente ou um Servidor de Aplicativos Integrado com o WebSphere Application Server no Rational Application Developer" na página 344
Configure e execute um aplicativo Java EE com um cliente ou servidor WebSphere eXtreme Scale com o tempo de execução integrado do WebSphere Application Server no Rational Application Developer. Se estiver configurando um servidor, iniciar o WebSphere Application Server inicia automaticamente o WebSphere eXtreme Scale.

Java "Introdução ao Desenvolvimento de Aplicativos" na página 254
Para iniciar o desenvolvimento de aplicativos WebSphere eXtreme Scale, você deve configurar seu ambiente de desenvolvimento, aprender sobre APIs que podem ser usadas e, em seguida, desenvolver e testar seu aplicativo.

Informações relacionadas:

Documentação da API

Java Documentação da API

Visão Geral dos Plug-ins Java

Java

Um plug-in do WebSphere eXtreme Scale é um componente que fornece um certo tipo de função para os componentes conectáveis que incluem ObjectGrid e BackingMap. O WebSphere eXtreme Scale fornece vários pontos de conexão para permitir que os aplicativos e provedores de cache se integrem com vários armazéns de dados, APIs de cliente alternativo e para melhorar o desempenho geral do cache. O produto é fornecido com vários plug-ins padrão pré-construídos, mas também é possível criar plug-ins customizados com o aplicativo.

Todos os plug-ins são classes concretas que implementam uma ou mais interfaces do plug-in eXtreme Scale. Tais classes são divididas em instâncias e chamadas pelo ObjectGrid nos momentos apropriados. O ObjectGrid e os BackingMaps permitem que plug-ins customizados sejam registrados.

Plug-ins do ObjectGrid

Os seguintes plug-ins estão disponíveis para uma instância do ObjectGrid. Se o plug-in for apenas do lado do servidor, os plug-ins serão removidas nas instâncias ObjectGrid e BackingMap do cliente. As instâncias do ObjectGrid e BackingMap são apenas do lado do servidor.

- **TransactionCallback**: Um plug-in TransactionCallback fornece eventos do ciclo de vida de transação. Se o plug-in TransactionCallback for a implementação de

classe JPATxCallback integrada (com.ibm.websphere.objectgrid.jpa.JPATxCallback), o plug-in será apenas do lado do servidor. Entretanto, as subclasses da classe JPATxCallback não são apenas do lado do servidor.

- **ObjectGridEventListener**: Um plug-in ObjectGridEventListener fornece eventos de ciclo de vida ObjectGrid para o ObjectGrid, shards e transações.
- **ObjectGridLifecycleListener**: Um plug-in ObjectGridLifecycleListener fornece eventos de ciclo de vida ObjectGrid para a instância do ObjectGrid. O plug-in ObjectGridLifecycleListener pode ser usado como uma interface combinada opcional para todos os outros plug-ins do ObjectGrid.
- **ObjectGridPlugin**: Um ObjectGridPlugin é uma interface combinada opcional que fornece eventos de gerenciamento de ciclo de vida estendida para todos os outros plug-ins do ObjectGrid.
- **SubjectSource, ObjectGridAuthorization, SubjectValidation**: eXtreme Scale fornece vários terminais de segurança para permitir que mecanismos de autenticação customizados sejam integrados ao eXtreme Scale. (Apenas do lado do servidor)

Requisitos Comuns do Plug-in do ObjectGrid

O ObjectGrid instancia e inicializa as instâncias de plug-in usando as convenções JavaBeans. Todas as implementações do plug-in apresentam os seguintes requisitos:

- A classe de plug-in deve ser uma classe pública de alto nível
- Ela deve apresentar um construtor público, sem argumentos.
- A classe de plug-in deve estar disponível no caminho de classe dos servidores e clientes (como apropriado).
- Os atributos devem ser definidos utilizando os métodos de propriedade de estilo do JavaBeans.
- Os plug-ins, exceto quando indicado de outra forma, são registrados antes da inicialização do ObjectGrid e não podem ser alterados depois de tal inicialização.

Plug-ins do BackingMap

Os seguintes plug-ins estão disponíveis para um BackingMap:

- **Evictor** - Um plug-in evictor é um mecanismo padrão fornecido para descartar entradas de cache e um plug-in para criar evictors customizados. O evictor de tempo de vida integrado utiliza um algoritmo baseado em tempo para decidir quando uma entrada no BackingMap deve ser despejada. Alguns aplicativos podem precisar usar um algoritmo diferente para decidir quando uma entrada de cache precisa ser despejada. O plug-in do Evictor disponibiliza um Evictor projetado customizado para ser utilizado pelo BackingMap. O plug-in Evictor é adicional ao evictor de tempo de vida integrado. É possível utilizar o plug-in Evictor customizado fornecido que implementa algoritmos bem conhecidos como "menos utilizado recentemente" ou "menos utilizado frequentemente". Os aplicativos podem conectar um dos plug-ins do Evictor fornecidos ou podem fornecer seu próprio plug-in do Evictor. Para obter informações adicionais, consulte Plug-ins para Despejar Objetos de Cache.
-  **ObjectTransformer**: Um plug-in ObjectTransformer permite serializar, desserializar e copiar objetos no cache. A interface ObjectTransformer foi substituída pelos plug-ins DataSerializer, que podem ser usados para armazenar dados arbitrários com eficiência no WebSphere eXtreme Scale para que as APIs

do produto existentes possam interagir eficientemente com seus dados. Para obter informações adicionais, consulte “Plug-in ObjectTransformer” na página 564.

-  **OptimisticCallback** - Utilize o plug-in OptimisticCallback para customizar as operações de versão e comparação dos objetos de cache ao utilizar a estratégia de bloqueio otimista. O plug-in OptimisticCallback foi substituído pela interface ValueDataSerializer.Versionable, que pode ser implementada quando o plug-in DataSerializer for usado com o modo de cópia COPY_TO_BYTES ou quando for usada a anotação @Version com a API do EntityManager. Para obter informações adicionais, consulte “Plug-ins para Versão e Comparação de Objetos de Cache” na página 555.
- **MapEventListener** - Um plug-in MapEventListener fornece notificações de retorno de chamada e alterações de estado de cache significativas que ocorrem para um BackingMap. Um aplicativo talvez queira saber sobre eventos de BackingMap tal como um despejo de entrada do mapa ou um pré-carregamento de uma conclusão de BackingMap. Um BackingMap chama métodos no plug-in MapEventListener para notificar um aplicativo sobre eventos do BackingMap. Um aplicativo pode receber notificação de vários eventos de BackingMap, utilizando o método setMapEventListener para fornecer um ou mais plug-ins MapEventListener projetados customizados para o BackingMap. O aplicativo pode modificar os objetos MapEventListener listados usando o método addMapEventListener ou o método removeMapEventListener. Para obter informações adicionais, consulte “Plug-in MapEventListener” na página 570.
- **BackingMapLifecycleListener**: Um plug-in BackingMapLifecycleListener fornece eventos de ciclo de vida BackingMap para a instância do BackingMap. O plug-in BackingMapLifecycleListener pode ser usado como uma interface combinada opcional para todos os outros plug-ins do BackingMap.
- **BackingMapPlugin**: Um BackingMapPlugin é uma interface combinada opcional que fornece eventos de gerenciamento de ciclo de vida estendida para todos os outros plug-ins do BackingMap.
- **Indexação** - Use o recurso de indexação, que é representado pelo plug-in MapIndexplug-in, para construir um ou mais índices em um mapa BackingMap para suportar acesso a dados sem chave.
- **Loader**: Um plug-in Loader em um mapa ObjectGrid atua como um cache de memória para os dados que são normalmente mantidos em um armazenamento persistente no mesmo sistema ou em outro sistema diferente. (Apenas lado do servidor) Por exemplo, um Carregador de Java Database Connectivity (JDBC) pode ser usado para mover dados para dentro e fora de um BackingMap e uma ou mais tabelas relacionais de um banco de dados relacional. Um banco de dados relacional não precisa ser utilizado como o armazenamento persistente para um BackingMap. O utilitário de carga também pode ser usado para dados movidos entre um BackingMap e um arquivo, entre um BackingMap e um mapa Hibernate, entre um BackingMap e um bean de entidade Java 2 Platform, Enterprise Edition (J2EE), entre um BackingMap e outro servidor de aplicativos, e assim por diante. O aplicativo deve fornecer um plug-in do Loader projetado customizado para mover dados entre o BackingMap e o armazenamento persistente para cada tecnologia utilizada. Se um Loader não for fornecido, o BackingMap se tornará um cache de memória simples. Para obter informações adicionais, consulte “Plug-ins para a Comunicação com os Bancos de Dados” na página 601.
- **MapSerializerPlugin**: Um MapSerializerPlugin permite que você serialize e encha objetos Java e dados não Java no cache. Ele é usado com as interfaces combinadas DataSerializer, permitindo opções robustas e flexíveis para aplicativos de alto desempenho.

Tarefas relacionadas:

"Executando os Contêineres do eXtreme Scale com Plug-ins Não Dinâmicos em um Ambiente do OSGi" na página 168
Se você não precisar usar o recurso dinâmico de um ambiente de OSGi, será possível ainda aproveitar o acoplamento mais fechado, o empacotamento declarativo e as dependências de serviço que a estrutura de OSGi oferece.

Visão Geral do Serviço de Dados REST

Java

O serviço de dados REST WebSphere eXtreme Scale é um serviço HTTP Java compatível com Microsoft WCF Data Services (formalmente, ADO.NET Data Services) e implementa o Open Data Protocol (OData). O Microsoft WCF Data Services é compatível com essa especificação quando utiliza Visual Studio 2008 SP1 e .NET Framework 3.5 SP1.

Requisitos de Compatibilidade

O serviço de dados REST permite que qualquer cliente HTTP acesse uma grade de dados. O serviço de dados REST é compatível com o suporte do WCF Data Services fornecido com o Microsoft .NET Framework 3.5 SP1. Aplicativos RESTful podem ser desenvolvidos com um rico conjunto de ferramentas fornecido pelo Microsoft Visual Studio 2008 SP1. A figura fornece uma visão geral de como o WCF Data Services interage com clientes e bancos de dados.

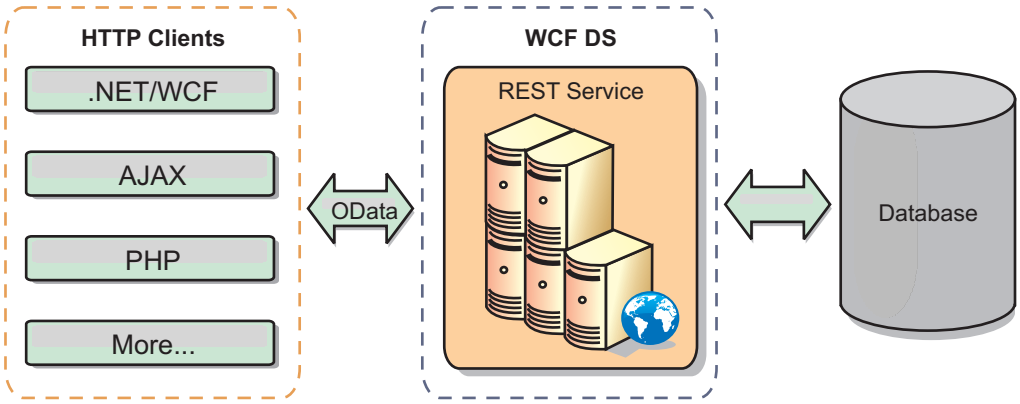


Figura 32. Microsoft WCF Data Services

O WebSphere eXtreme Scale inclui um conjunto de APIs com várias funções para clientes Java. Conforme mostrado na figura a seguir, o serviço de dados REST é um gateway entre clientes HTTP e a grade de dados do WebSphere eXtreme Scale, comunicando-se com a grade por meio de um cliente do WebSphere eXtreme Scale. O serviço de dados REST é um servlet Java, que permite implementações flexíveis para Plataforma Java comum, plataformas Enterprise Edition (JEE), como o WebSphere Application Server. O serviço de dados REST se comunica com a grade de dados WebSphere eXtreme Scale usando as APIs Java WebSphere eXtreme Scale. Ele permite clientes do WCF Data Services ou qualquer outro cliente que possa se comunicar com HTTP e XML.

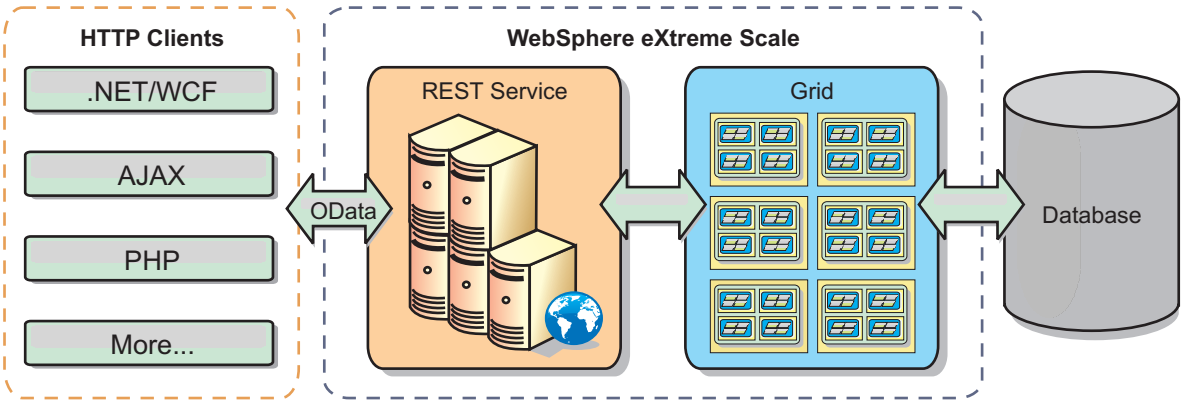


Figura 33. Serviço de Dados REST do WebSphere eXtreme Scale

Consulte o Configurando Serviços de Dados REST ou use os seguintes links para aprender mais sobre o WCF Data Services.

- Microsoft WCF Data Services Developer Center
- Visão geral do ADO.NET Data Services no MSDN
- White Paper: Utilizando ADO.NET Data Services
- Atom Publish Protocol: Data Services URI and Payload Extensions
- Conceptual Schema Definition File Format
- Entity Data Model for Data Services Packaging Format
- Open Data Protocol
- FAQ do Open Data Protocol

Características

Esta versão do serviço de dados REST do eXtreme Scale suporta os seguintes recursos:

- Modelagem automática de entidades de API EntityManager do eXtreme Scale como entidades do WCF Data Services, que inclui o seguinte suporte:
  - Tipo de dados Java para conversão de tipo do Entity Data Model
  - Suporte de associação de entidade
  - Suporte à raiz do esquema e à associação de chave, que é requerido para grades de dados particionadas

  Consulte o Modelo de Entidade para obter informações adicionais.
- Formato de carga útil de dados Atom Publish Protocol (AtomPub ou APP) XML e JavaScript Object Notation (JSON).
- Operações Create, Read, Update and Delete (CRUD) utilizando os respectivos métodos de pedido de HTTP: POST, GET, PUT e DELETE. Além disso, a extensão da Microsoft MERGE é suportada.

Nota: 8.6+ Os métodos upsert e upsertAll substituem os métodos put e putAll do ObjectMap. Use o método upsert para informar ao BackingMap e carregador que uma entrada na grade de dados precisa colocar a chave e o valor na grade. O BackingMap e carregador executam uma inserção ou uma atualização para colocar o valor na grade e no carregador. Se você executar a API upsert dentro de seus aplicativos, o carregador obterá um tipo UPSERT de LogElement, que permite que carregadores façam a mesclagem do banco de dados ou chamadas upsert em vez de usar insert ou update.

- Consultas simples, usando filtros
- Pedidos de recuperação de lote e do conjunto de mudanças
- Suporte de grade de dados particionada para alta disponibilidade
- Interoperabilidade com clientes de API EntityManager do eXtreme Scale
- Suporte para servidores da Web JEE padrão
- Simultaneidade otimista
- Autorização e autenticação de usuário entre o serviço de dados REST e a grade de dados do eXtreme Scale

Limitações e Problemas Conhecidos

- Pedidos em túnel não são suportados.

Tarefas relacionadas:

Configurando Serviços de Dados REST
É possível usar o serviço de dados REST do WebSphere eXtreme Scale com o WebSphere Application Server versão 7.0, o WebSphere Application Server Community Edition e o Apache Tomcat.

Java "Acessando Dados com o Serviço de Dados REST" na página 517
Desenvolva aplicativos que executam operações usando protocolos do serviço de dados REST.

Referências relacionadas:

Java "Simultaneidade Otimista no Serviço de Dados REST" na página 522
O serviço de dados REST do eXtreme Scale usa um modelo de bloqueio otimista ao usar cabeçalhos HTTP nativos: If-Match, If-None-Match e ETag. Esses cabeçalhos são enviados em mensagens de pedido e de resposta para retransmitir informações da versão da entidade do servidor para o cliente e do cliente para o servidor.

Java "Protocolos de Pedido para o Serviço de Dados REST" na página 523
No geral, os protocolos para interação com o serviço REST são os mesmos que os descritos no protocolo AtomPub de Serviços de Dados WCF. No entanto, o eXtreme Scale fornece detalhes adicionais, da perspectiva Modelo de Entidade do eXtreme Scale. Os usuários devem estar familiarizados com os protocolos WCF Data Services antes de lerem esta seção. Alternativamente, os usuários podem ler esta seção com a seção do protocolo WCF Data Services.

Java "Recuperar Pedidos com Serviço de Dados REST" na página 524
Um Pedido RetrieveEntity é usado por um cliente para recuperar uma entidade do eXtreme Scale. A carga útil da resposta contém os dados da entidade no formato AtomPub ou JSON. Além disso, o operador do sistema $expand pode ser utilizado para expandir as relações. As relações são representadas em sequência dentro da resposta do serviço de dados como um Atom Feed Document, que é uma relação para-muitos, ou um Atom Entry Document que é uma relação para-um.

Java "Recuperando Não Entidades com Serviços de Dados REST" na página 531
O serviço de dados REST permite recuperar mais que apenas entidades, como coletas e propriedades das entidades.

Java "Pedidos de Inserção com Serviço de Dados REST" na página 537
Um Pedido InsertEntity pode ser usado para inserir uma nova instância de entidade do eXtreme Scale, potencialmente com novas entidades relacionadas, no serviço de dados REST do eXtreme Scale.

Java "Pedidos de Atualização com Serviço de Dados REST" na página 541
O serviço de dados REST do WebSphere eXtreme Scale suporta pedidos de atualização para entidades, propriedades de primitivas de entidades e assim por diante.

Java "Pedidos de Exclusão com Serviços de Dados REST" na página 546
O serviço de dados REST do WebSphere eXtreme Scale pode excluir entidades, valores da propriedade e links.

Visão Geral da Estrutura Spring

Java

O Spring é uma estrutura para desenvolvimento de aplicativos Java. O WebSphere eXtreme Scale fornece suporte para permitir que o Spring gerencie as transações e configure clientes e servidores que compõem a grade de dados em memória implementada.

Provedor de Cache Spring

O Spring Framework Versão 3.1 introduziu uma nova abstração de cache. Com essa nova abstração, é possível incluir de modo transparente o armazenamento em cache em um aplicativo Spring existente. É possível usar o WebSphere eXtreme Scale como o provedor de cache para a abstração de cache. Para obter informações adicionais, consulte Configurando um Provedor de Cache Spring.

Transações Nativas Gerenciadas do Spring

O Spring fornece transações gerenciadas por contêiner que são similares a um servidor de aplicativos do Java Platform, Enterprise Edition. Porém, o mecanismo do Spring pode usar diferentes implementações. O WebSphere eXtreme Scale fornece a integração do gerenciador de transações que permite ao Spring para gerenciar os ciclos de vida da transação do ObjectGrid. Para obter informações adicionais, consulte “Gerenciando Transações com o Spring” na página 679.

Beans de Extensão Gerenciados do Spring e Suporte a Espaço de Nomes

Além disso, o eXtreme Scale se integra ao Spring para permitir que os beans de estilo do Spring definidos para pontos de extensão ou plug-ins. Este recurso fornece configurações mais sofisticadas e mais flexíveis para configuração dos pontos de extensão.

Além dos beans de extensão gerenciados do Spring, o eXtreme Scale fornece um espaço de nomes Spring chamado "objectgrid". Beans e implementações integradas são predefinidos neste espaço de nomes, o que facilita aos usuários configurar o eXtreme Scale. Consulte “Beans de Extensão Spring e Suporte a Espaço de Nomes” na página 684 para obter mais detalhes sobre esses tópicos e uma amostra de como iniciar um servidor de contêiner do eXtreme Scale usando configurações Spring.

Suporte ao Escopo Shard

Com a configuração do Spring estilo tradicional, um bean ObjectGrid pode se do tipo singleton ou prototype. O ObjectGrid também suporta um novo escopo chamado de escopo "shard". Se um bean for definido como escopo shard, então somente um bean será criado por shard. Todas as solicitações de beans com um ID ou IDs correspondentes a essa definição de bean no mesmo shard resulta nessa instância de bean específica sendo retornada pelo contêiner Spring.

O exemplo a seguir mostra que um bean com.ibm.ws.objectgrid.jpa.plugins.JPAPropFactoryImpl é definido com o escopo configurado para shard. Portanto, apenas uma instância da classe JPAPropFactoryImpl é criada por shard.

```
<bean id="jpaPropFactory" class="com.ibm.ws.objectgrid.jpa.plugins.JPAPropFactoryImpl" scope="shard" />
```

Fluxo da Web do Spring

O Fluxo da Web do Spring armazena seu estado de sessão em uma sessão HTTP por padrão. Se um aplicativo da web usar o eXtreme Scale para gerenciamento de

sessões, o Spring armazenará automaticamente o estado com o eXtreme Scale. Além disso, a tolerância a falhas é ativada da mesma forma que a sessão.

Para obter mais informações, consulte Gerenciando de Sessões HTTP.

compactando

As extensões Spring do eXtreme Scale estão no arquivo `ogspring.jar`. Este arquivo Java archive (JAR) deve estar no caminho de classe para o suporte ao Spring funcionar. Se um aplicativo Java EE que estiver em execução em um WebSphere Application Server Network Deployment aumentado pelo WebSphere Extended Deployment, coloque o arquivo `spring.jar` e seus arquivos associados nos módulos EAR (enterprise archive). Você também deve colocar o arquivo `ogspring.jar` no mesmo local.

Tarefas relacionadas:

Java "Desenvolvendo Aplicativos com a Estrutura Spring" na página 676
Aprenda como integrar seus aplicativos eXtreme Scale com o Spring Framework popular.

Java "Iniciando um Servidor de Contêiner com o Spring" na página 687
É possível iniciar um servidor de contêiner usando beans de extensão gerenciados pelo Spring e o suporte ao namespace.

Java "Gerenciando Transações com o Spring" na página 679
O Spring é uma estrutura popular para desenvolvimento de aplicativos Java. O WebSphere eXtreme Scale fornece suporte para permitir que o Spring gerencie transações do eXtreme Scale e configure clientes e servidores eXtreme Scale.

Referências relacionadas:

Java "Beans de Extensão Gerenciados pelo Spring" na página 682
É possível declarar que os POJOs sejam usados como pontos de extensão no arquivo `objectgrid.xml`. Se você nomear os beans e, em seguida, especificar o nome de classe, o eXtreme Scale normalmente cria instâncias da classe especificada e usa essas instâncias como o plug-in. O WebSphere eXtreme Scale pode delegar para que o Spring aja como o bean factory para obter instâncias desses objetos de plug-in.

Java Arquivo XML descritor do Spring
Use um arquivo XML descritor do Spring para configurar e integrar o eXtreme Scale com o Spring.

Java Arquivo `objectgrid.xsd` Spring
Use o arquivo `objectgrid.xsd` Spring para integrar o eXtreme Scale ao Spring para gerenciar as transações do eXtreme Scale e configurar os clientes e servidores.

Considerações sobre o Carregador de Classe Java e o Caminho de Classe

Java

Como o WebSphere eXtreme Scale armazena objetos Java no cache por padrão, você deve definir classes no caminho de classe sempre que os dados forem acessados.

Especificamente, os processos do cliente e de contêiner do WebSphere eXtreme Scale devem incluir as classes ou arquivos JAR no caminho de classe ao iniciar o processo. Quando você projeta um aplicativo para uso com o eXtreme Scale, separe qualquer lógica de negócios dos objetos de dados persistentes.

Consulte Carregamento de Classe no centro de informações do WebSphere Application Server para obter mais informações.

Para considerações dentro de uma configuração de Spring Framework, consulte a seção de empacotamento no “Visão Geral da Estrutura Spring” na página 330.

Para configurações relacionadas ao uso do agente de instrumentação doWebSphere eXtreme Scale, consulte “Agente de Instrumentação de Desempenho da Entidade” na página 762.

Para obter detalhes sobre a inclusão de suas classes ou arquivos JAR no caminho de classe do servidor de contêiner independente, consulte Script **startOgServer** (ORB) ou Script **startXsServer** (XIO).

Gerenciamento de Relacionamentos

Java

Linguagens orientadas a objetos como Java, e relacionamentos ou associações de suporte a bancos de dados relacionais. Os relacionamentos diminuem a quantidade de armazenamento através do uso de referências de objetos ou chaves estrangeiras.

Ao usar relacionamentos em uma grade de dados, os dados deverão ser organizados em uma árvore limitada. Um tipo de raiz deve existir na árvore e todos os filhos devem estar associados a apenas uma raiz. Por exemplo: Departamento pode ter muitos Funcionários e um Funcionário pode ter muitos Projetos. Porém um Projeto não pode ter muitos Funcionários pertencentes a diferentes departamentos. Depois de uma raiz ser definida, todo o acesso a este objeto raiz e seus descendentes será gerenciado através da raiz. O WebSphere eXtreme Scale usa o código hash da chave do objeto raiz para escolher uma partição. Por exemplo:

```
partition = (hashCode MOD numPartitions).
```

Quando todos os dados para um relacionamento estiverem ligados a um única instância do objeto, toda a árvore pode ser co-localizada em uma única partição e pode ser acessada muito eficientemente usando uma transação. Se os dados englobarem múltiplos relacionamentos, então múltiplas partições devem estar envolvidas que envolvem chamadas remotas adicionais, o que pode levar a gargalos no desempenho.

Dados de Referência

Alguns relacionamentos incluem dados de consulta ou de referência como: `CountryName`. Para dados de consulta ou de referência, os dados devem existir em cada partição. Os dados podem ser acessados por qualquer chave raiz e o mesmo resultado é retornado. Os dados de referência como estes devem ser usados apenas nos casos em que os dados forem razoavelmente estáticas. Atualizar esses dados pode ser dispendioso porque eles precisam ser atualizados em cada partição. A API DataGrid é uma técnica comum para manter os dados de referência atualizados.

Custos e Benefícios de Normalização

A normalização dos dados usando os relacionamentos pode ajudar a reduzir a quantidade de memória usada pela grade de dados pois a duplicação dos dados é diminuída. Porém, em geral, quanto mais dados relacionais forem incluídos, menos eles irão expandir. Quando os dados são agrupados juntos, torna-se mais caro manter os relacionamentos e manter os tamanhos gerenciáveis. Como os dados das

partições da grade baseiam-se na chave da raiz da árvore, o tamanho da árvore não é levado em consideração. Assim, se você tiver uma grande quantidade de relacionamentos para uma instância da árvore, a grade de dados poderá ficar desequilibrada, fazendo com que uma partição mantenha mais dados do que as outras.

Quando os dados forem não normalizados ou simplificados, os dados que normalmente seriam compartilhados entre os dois objetos são duplicados e cada tabela pode ser particionada de modo independente, oferecendo uma grade de dados muito mais equilibrada. Apesar disto aumentar a quantidade de memória usada, permite que o aplicativo escale pois uma única linha de dados pode ser acessada que pode ter todos os dados necessários. Isto é ideal para grades com maior quantidade de leituras pois a manutenção dos dados se torna mais cara.

Para obter informações adicionais, consulte Classificação de sistemas XTP e escalamento.

Gerenciamento de Relacionamentos Usando as APIs de Acesso a Dados

A API ObjectMap é a mais rápida, mais flexível e granular das APIs de acesso a dados, oferecendo uma abordagem transacional baseada em sessão no acesso aos dados na grade de mapas. A API ObjectMap permite que os clientes usem operações comuns, como create, read, update e delete (CRUD), para gerenciar pares de valores de chave de objetos na grade de dados distribuída.

Ao usar a API ObjectMap, os relacionamentos de objetos devem ser expressos pela incorporação da chave estrangeira para todos os relacionamentos no objeto-pai.

A seguir, está um exemplo.

```
public class Department {
 Collection<String> employeeIds;
}
```

A API EntityManager simplifica o gerenciamento de relacionamentos através da extração de dados persistentes a partir de objetos incluindo as chaves estrangeiras. Quando o objeto é posteriormente recuperado da grade de dados, o gráfico de relacionamentos é reconstruído, como no seguinte exemplo.

```
@Entity
public class Department {
 Collection<String> employees;
}
```

A API EntityManager é muito semelhante a outras tecnologias de persistência do objeto Java como JPA e Hibernate na qual ela sincroniza um gráfico de instâncias de objetos Java gerenciados com o armazenamento persistente. Nesse caso, o armazenamento persistente é uma grade de dados do eXtreme Scale, em que cada entidade é representada como um mapa e o mapa contém os dados da entidade em vez das instâncias do objeto.

Considerações-Chave sobre Cache

Java

O WebSphere eXtreme Scale usa mapas hash para armazenar dados na grade, na qual um objeto Java é usado para a chave.

Diretrizes

Ao escolher uma chave, considere os seguintes requisitos.

- As chaves nunca podem ser alteradas. Se uma parte da chave precisar ser alterada, a entrada do cache deverá ser removida e reinserida.
- As chaves devem ser pequenas. Como as chaves são utilizadas em toda operação de acesso a dados, é recomendável manter a chave pequena para que ela possa ser serializada eficientemente e utilize menos memória.
- Implementa um bom hash e algoritmo de igualdade. Os métodos hashCode e equals(Object o) devem ser sempre substituídos para cada objeto-chave.
- Armazene o hashCode da chave. Se possível, armazene em cache o código hash na instância do objeto-chave para acelerar os cálculos de hashCode(). Como a chave é imutável, o hashCode deve ser armazenável em cache.
- Evite duplicar a chave no valor. Ao usar a API ObjectMap, é conveniente armazenar a chave dentro do objeto do valor. Quando isso é feito, os dados-chave são duplicados na memória.

Dados para Diferentes Fusos Horários

Java

Ao inserir dados com os atributos calendar, java.util.Date e timestamp em um ObjectGrid, você deve garantir que esses atributos de data e hora sejam criados com base no mesmo fuso horário, principalmente quando implementados em vários servidores em vários fusos horários. Usar o mesmo objeto de data e hora baseado em fuso horário pode garantir que o aplicativo esteja protegido por fuso horário e que os dados possam ser consultados pelos predicados calendar, java.util.Date e timestamp.

Sem especificar explicitamente um fuso horário ao criar objetos de data e hora, o Java usa o fuso horário local e pode causar valores de data e hora inconsistentes nos clientes e servidores.

Considere um exemplo em uma implementação distribuída na qual o client1 está no fuso horário [GMT-0] e o client2 está no [GMT-6], e ambos querem criar um objeto java.util.Date com o valor '1999-12-31 06:00:00'. Então, o client1 criará o objeto java.util.Date com o valor '1999-12-31 06:00:00 [GMT-0]' e o client2 criará o objeto java.util.Date com o valor '1999-12-31 06:00:00 [GMT-6]'. Os objetos java.util.Date não são iguais porque o fuso horário é diferente. Um problema semelhante ocorre quando você pré-carrega os dados nas partições que residem em servidores em fusos horários diferentes se o fuso horário local for utilizado para criar objetos de data e hora.

Para evitar o problema descrito, o aplicativo pode escolher um fuso horário como [GMT-0] como fuso horário base para criar objetos calendar, java.util.Date e timestamp.

Capítulo 5. Desenvolvendo Aplicativos

8.6+ É possível desenvolver aplicativos clientes que usam a grade de dados em ambas as linguagens de programação, Java e .NET.

Desenvolvendo Aplicativos Java

É possível desenvolver aplicativos Java para acessar e inserir dados na grade de dados. É possível usar plug-ins para desenvolver funções específicas para componentes plugáveis. Seus aplicativos também podem se integrar com outras estruturas, incluindo OSGi, JPA e Spring.

Sobre Esta Tarefa

Desenvolva aplicativos Java que usam a grade de dados. As tarefas para desenvolver aplicativos incluem:

- Acessar Dados
- APIs e Plug-ins do Sistema
- Integração do OSGi
- Integração do JPA
- Integração do Spring

Configurando o Ambiente de Desenvolvimento Java

Java

Antes de iniciar o desenvolvimento de aplicativos Java, você deve configurar seu ambiente de desenvolvimento.

Antes de Iniciar

Consulte “Planejando para Desenvolver Aplicativos do WebSphere eXtreme Scale” na página 319 para obter informações adicionais sobre as interfaces de programação disponíveis e suas considerações.

Conceitos relacionados:

"Visão Geral da API Java" na página 321
O WebSphere eXtreme Scale fornece diversos recursos que são acessados programaticamente usando a linguagem de programação Java através de interfaces de programação de aplicativos (APIs) e interfaces de programação do sistema.

Java "Visão Geral da API Java" na página 321
O WebSphere eXtreme Scale fornece diversos recursos que são acessados programaticamente usando a linguagem de programação Java através de interfaces de programação de aplicativos (APIs) e interfaces de programação do sistema.

Informações relacionadas:

Documentação da API

Java Documentação da API

Acessando a Documentação da API Java

Java

É possível acessar a documentação da API Java para WebSphere eXtreme Scale fazendo download de um archive de arquivo zip, incorporando a documentação da API em seu ambiente de desenvolvimento ou visualizando a documentação da API no centro de informações.

Sobre Esta Tarefa

É possível acessar a documentação da API Java em um dos seguintes locais:

Centro de informações
Usar a documentação da API do centro de informações é útil para procurar junto com o resto das informações do produto WebSphere eXtreme Scale.

Archive zip
É possível fazer o download desse arquivo para cada liberação. É possível usar as ferramentas de comparação para verificar as mudanças das APIs de liberação a liberação. Também é possível ter um link direto para o arquivo compactado nos projetos do Eclipse quando está compilando com relação ao arquivo objectgrid.jar. Usar essa vinculação integra a documentação da API no IDE.

Formato online
O formato online é uma cópia publicada da documentação da API no website IBM. É possível ter um link direto para essa URL no Eclipse. O link da versão atual é sempre atualizado à última versão, de modo que seja possível consultar as correções e alterações da documentação.

Procedimento

- Visualize a documentação da API no centro de informações. Para obter informações adicionais, consulte

  Documentação da API.
- Faça o download de um archive zip da documentação da API.

  Se você deseja fazer o download da documentação da API para navegar offline, será possível fazer o download de um arquivo zip para a liberação apropriada da página a seguir: WebSphere eXtreme Scale wiki: Documentação da API.
- Visualize o formato online da documentação da API. É possível associar um marcador a um link que esteja sempre atualizado para a última versão ou ter

um link para uma versão específica. Para obter uma lista de links, consulte WebSphere eXtreme Scale wiki: Documentação da API.

O que Fazer Depois

Para obter informações adicionais sobre como acessar a documentação da API dentro do ambiente de desenvolvimento, consulte "Configurando um Ambiente de Desenvolvimento Independente no Eclipse".

Conceitos relacionados:

"Visão Geral da API Java" na página 321
O WebSphere eXtreme Scale fornece diversos recursos que são acessados programaticamente usando a linguagem de programação Java através de interfaces de programação de aplicativos (APIs) e interfaces de programação do sistema.

Java "Visão Geral da API Java" na página 321
O WebSphere eXtreme Scale fornece diversos recursos que são acessados programaticamente usando a linguagem de programação Java através de interfaces de programação de aplicativos (APIs) e interfaces de programação do sistema.

Informações relacionadas:

Documentação da API

Java Documentação da API

Configurando um Ambiente de Desenvolvimento Independente no Eclipse

Java

Configure um ambiente de desenvolvimento integrado baseado no Eclipse para construir e executar um aplicativo Java SE com a versão independente do WebSphere eXtreme Scale.

Antes de Iniciar

Instale o produto WebSphere eXtreme Scale em um diretório novo ou vazio e aplique o fix pack acumulativo mais recente do WebSphere eXtreme Scale. Também é possível usar a versão de teste do WebSphere eXtreme Scale ao descompactar o arquivo zip. Para obter mais informações sobre a instalação, consulte o .

Procedimento

- Configure o Eclipse para construir e executar um aplicativo SE Java com o WebSphere eXtreme Scale.
  1. Defina uma biblioteca de usuário para permitir que seu aplicativo faça referência a interfaces de programação de aplicativo do WebSphere eXtreme Scale.
     a. No Eclipse ou no ambiente do IBM Rational Application Developer, clique em **Janela** > **Preferências**.
     b. Expanda a ramificação **Java** > **Caminho de Construção** e selecione **Bibliotecas de Usuário**. Clique em **Novo**.
     c. Selecione a biblioteca de usuário do eXtreme Scale. Clique em **Incluir JARs**.
        1) Procure por e selecione o arquivo `objectgrid.jar` ou `ogclient.jar` a partir do diretório *wxs_root*`/lib`. Clique em **OK**. Selecione o arquivo `ogclient.jar` se estiver desenvolvendo caches de aplicativos clientes

ou locais em memória. Se estiver desenvolvendo e testando servidores eXtreme Scale, use o arquivo `objectgrid.jar`.

2) Para incluir Javadoc nas APIs do ObjectGrid, selecione o local do Javadoc para o arquivo `objectgrid.jar` ou `ogclient.jar` incluído na etapa anterior. Clique em **Editar**. Na caixa do caminho do local do Javadoc, digite o seguinte endereço da Web:

   ```
   http://www.ibm.com/developerworks/wikis/extremescale/docs/api/
   ```

d. Clique em **OK** para aplicar as configurações e fechar a janela Preferências.

As bibliotecas do eXtreme Scale estão agora no caminho de construção para o projeto.

2. Inclua a biblioteca de usuário em seu projeto Java.
   a. No Package Explorer, clique com o botão direito do mouse no projeto e selecione **Propriedades**.
   b. Selecione a guia **Bibliotecas**.
   c. Clique em **Incluir Biblioteca**.
   d. Selecione **Biblioteca de Usuário**. Clique em **Next**.
   e. Selecione a biblioteca de usuário do eXtreme Scale configurada anteriormente.
   f. Clique em **OK** para aplicar as mudanças e fechar a janela Propriedades.

- Execute um aplicativo SE Java com o eXtreme Scale com Eclipse. Crie uma configuração de execução para executar seu aplicativo.
  1. Configure o Eclipse para construir e executar um aplicativo SE Java com o eXtreme Scale. No menu **Executar**, selecione **Executar Configurações**.
  2. Clique com o botão direito do mouse na categoria Aplicativo Java e selecione **Novo**.
  3. Selecione a nova configuração de execução, denominada *New_Configuration*.
  4. Configure o perfil.
     – **Projeto** (na página tabulada principal): *your_project_name*
     – **Classe Principal** (na página tabulada principal): *your_main_class*
     – **Argumentos VM** (na página tabulada de argumentos): -Djava.endorsed.dirs=`wxs_root`/lib/endorsed

     Problemas com os **Argumentos VM** ocorrem com frequência porque o caminho para `java.endorsed.dirs` deve ser um caminho absoluto sem variáveis ou atalhos.

     Outros problemas comuns de configuração envolvem o Object Request Broker (ORB). Você deve ver o seguinte erro. Consulte o Configurando um Object Request Broker Customizado para obter mais informações.

     ```
     Caused by: java.lang.RuntimeException: The ORB that comes
     with the Sun Java implementation does not work with
     ObjectGrid at this time.
     ```

     Se você não tiver `objectGrid.xml` ou `deployment.xml` acessível ao aplicativo, poderá ver o seguinte erro:

     ```
     Exception in thread "P=211046:O=0:CT" com.ibm.websphere.objectgrid.
         ObjectGridRuntimeException: Cannot start OG container at
         Client.startTestServer(Client.java:161) at Client.
         main(Client.java:82) Caused by: java.lang.IllegalArgumentException:
         The objectGridXML must not be null at com.ibm.websphere.objectgrid.
         deployment.DeploymentPolicyFactory.createDeploymentPolicy
          (DeploymentPolicyFactory.java:55) at Client.startTestServer(Client.
         java:154) .. 1 more
     ```

5. Clique em **Aplicar** e feche a janela ou clique em **Executar**.

Conceitos relacionados:

"Visão Geral da API Java" na página 321
O WebSphere eXtreme Scale fornece diversos recursos que são acessados programaticamente usando a linguagem de programação Java através de interfaces de programação de aplicativos (APIs) e interfaces de programação do sistema.

Java "Visão Geral da API Java" na página 321
O WebSphere eXtreme Scale fornece diversos recursos que são acessados programaticamente usando a linguagem de programação Java através de interfaces de programação de aplicativos (APIs) e interfaces de programação do sistema.

Informações relacionadas:

Documentação da API

Java Documentação da API

Executando um Aplicativo Cliente ou do Servidor do WebSphere eXtreme Scale com o Apache Tomcat no Rational Application Developer

Java

Independente se você tiver um aplicativo cliente ou do servidor, use as mesmas etapas básicas para executar o aplicativo no Apache Tomcat no Rational Application Developer. Para um aplicativo cliente, você deseja configurar e executar um aplicativo da web para usar um cliente do WebSphere eXtreme Scale no Rational Application Developer. Siga estas instruções para criar um projeto da Web para executar um contêiner ou serviço de catálogo do WebSphere eXtreme Scale. Para um aplicativo do servidor, você deseja ativar um aplicativo Java EE na interface do Rational Application Developer com uma instalação independente do WebSphere eXtreme Scale. Siga estas instruções para configurar um projeto do aplicativo Java EE para usar a biblioteca do cliente do WebSphere eXtreme Scale.

Antes de Iniciar

Instale o Teste do WebSphere eXtreme Scale ou o produto integral.

- Instale a versão independente do produto WebSphere eXtreme Scale.
- Faça download e extraia a versão de teste do WebSphere eXtreme Scale.
- Instale o Apache Tomcat Versão 6.0 ou posterior.
- Instale o Rational Application Developer e crie um aplicativo da web Java EE.

Procedimento

1. Inclua a biblioteca de tempo de execução do WebSphere eXtreme Scale no caminho de construção do Java EE.

   Aplicativo cliente Neste cenário, você deseja configurar e executar um aplicativo da web para usar um cliente do WebSphere eXtreme Scale no Rational Application Developer.

   a. **Janela** > **Preferências** > **Java** > **Caminho de Construção** > **Bibliotecas de Usuário**. Clique em **Novo**.

   b. Digite um **Nome da biblioteca de usuário** de `eXtremeScaleClient` e clique em **OK**.

   c. Clique em **Incluir Jars...**, navegue para o arquivo `wxs_home/lib/ogclient.jar` e selecione-o. Clique em **Abrir**.

d. Opcional: (Opcional) Para incluir Javadoc, selecione o local Javadoc e clique em **Editar....** No caminho do local Javadoc, é possível digitar a URL da documentação da API ou pode fazer download da documentação da API.
   - Para usar a documentação da API on-line, digite `http://www.ibm.com/developerworks/wikis/extremescale/docs/api/` no caminho do local Javadoc.
   - Para fazer download da documentação da API, vá para a WebSphere eXtreme Scale Página de download de documentação da API. Para o caminho do local Javadoc, digite seu local de download local.

e. Clique em **OK**.

f. Clique em **OK** para fechar o diálogo Bibliotecas de Usuário.

g. Clique em **Projeto** > **Propriedades**.

h. Clique em **Caminho de Construção Java**.

i. Clique em **Incluir Biblioteca**.

j. Selecione **Biblioteca de Usuário**. Clique em **Avançar**.

k. Marque a biblioteca **eXtremeScaleClient** e clique em **Concluir**.

l. Clique em **OK** para fechar o diálogo **Propriedades do Projeto**.

Aplicativo do servidor Neste cenário, você deseja configurar e executar um aplicativo da web para executar um servidor WebSphere eXtreme Scale integrado no Rational Application Developer.

a. Clique em **Janela** > **Preferências** > **Java** > **Caminho de Construção** > **Bibliotecas de Usuário**. Clique em **Novo**.

b. Digite um **Nome de biblioteca de usuário** de `eXtremeScale` e clique em **OK**.

c. Clique em **Incluir Jars...** e selecione *wxs_home*`/lib/objectgrid.jar`. Clique em Abrir.

d. (Opcional) Para incluir Javadoc, selecione o local Javadoc e clique em **Editar....** No caminho do local Javadoc, digite `http://www.ibm.com/developerworks/wikis/extremescale/docs/api/`.

e. Clique em **OK**.

f. Clique em **OK** para fechar o diálogo Bibliotecas de Usuário.

g. Clique em **Projeto** > **Propriedades**.

h. Clique em **Caminho de Construção Java**.

i. Clique em **Incluir Biblioteca**.

j. Selecione **Biblioteca de Usuário**. Clique em **Avançar**.

k. Marque a biblioteca **eXtremeScaleClient** e clique em **Concluir**.

l. Clique em **OK** para fechar o diálogo **Propriedades do Projeto**.

2. Defina Tomcat Server para nosso projeto.

a. Certifique-se de estar na perspectiva J2EE e clique na guia **Servidores** na área de janela inferior. Você também pode clicar em **Janela** > **Mostrar Visualização** > **Servidores**.

b. Clique com o botão direito do mouse na área de janela Servidores e escolha **Novo** > **Servidor**.

c. Escolha **Apache, Tomcat v6.0 Server**. Clique em **Avançar**.

d. Clique em **Procurar** e selecione *tomcat_root*. Clique em **OK**.

e. Clique em **Avançar**.

f. Selecione seu aplicativo Java EE na área de janela Disponível à esquerda, clique em **Incluir >** para movê-lo para a área de janela Configurado à direita no servidor e clique em **Concluir**.

3. Resolva quaisquer erros restantes para o Projeto. Use as seguintes etapas para eliminar erros na área de janela Problemas:
   a. Clique em **Projeto** > **Limpar** > *project_name*. Clique em **OK**. Construa o projeto.
   b. Clique com o botão direito no projeto Java EE e escolha **Caminho de Construção** > **Configurar Caminho de Construção**.
   c. Clique na guia **Bibliotecas**. Certifique-se de que o caminho seja configurado adequadamente:
      - **Para aplicativos clientes:** Assegure que o Apache Tomcat, eXtremeScaleClient, e JavaJRE estejam no caminho.
      - **Para aplicativos do servidor:** Assegure que o Apache Tomcat, eXtremeScale, e Java JRE estejam no caminho.
4. Crie uma configuração de execução para executar seu aplicativo.
   a. No menu **Executar**, selecione **Executar Configurações**.
   b. Clique com o botão direito do mouse na categoria Aplicativo Java e selecione **Novo**.
   c. Selecione a nova configuração de execução, denominada *New_Configuration*.
   d. Configure o perfil.
      - **Projeto** (na página tabulada principal): *your_project_name*
      - **Classe Principal** (na página tabulada principal): *your_main_class*
      - **Argumentos VM** (na página tabulada de argumentos): `-Djava.endorsed.dirs=wxs_root/lib/endorsed`

      Problemas com os **Argumentos VM** ocorrem com frequência porque o caminho para `java.endorsed.dirs` deve ser um caminho absoluto sem variáveis ou atalhos.

      Outros problemas comuns de configuração envolvem o Object Request Broker (ORB). Você deve ver o seguinte erro. Consulte o Configurando um Object Request Broker Customizado para obter mais informações:

      ```
      Caused by: java.lang.RuntimeException: The ORB that comes with the
      Java implementation does not work with ObjectGrid at this time.
      ```

      Se você não tiver os arquivos `objectGrid.xml` ou `deployment.xml` acessíveis ao aplicativo, poderá ver o seguinte erro:

```
Exception in thread "P=211046:O=0:CT" com.ibm.websphere.objectgrid.ObjectGridRuntimeException:
Cannot start OG container
 at Client.startTestServer(Client.java:161)
 at Client.main(Client.java:82)
Caused by: java.lang.IllegalArgumentException: The objectGridXML must not be null
 at com.ibm.websphere.objectgrid.deployment.DeploymentPolicyFactory.createDeploymentPolicy
  (DeploymentPolicyFactory.java:55)
 at Client.startTestServer(Client.java:154)
 ... 1 more
```

5. Clique em **Aplicar** e feche a janela ou clique em **Executar**.

O que Fazer Depois

Depois de configurar e de executar um aplicativo da web com o cliente do WebSphere eXtreme Scale no Rational Application Developer, será possível desenvolver um servlet. Esse servlet usa as APIs do WebSphere eXtreme Scale para armazenar e recuperar dados de uma grade de dados remota.

Depois de ativar um aplicativo Java EE na interface do Rational Application Developer com uma instalação independente do WebSphere eXtreme Scale, será possível desenvolver um servlet que use as APIs de sistema do WebSphere eXtreme Scale para iniciar e parar serviços de catálogo.

Conceitos relacionados:

"Visão Geral da API Java" na página 321
O WebSphere eXtreme Scale fornece diversos recursos que são acessados programaticamente usando a linguagem de programação Java através de interfaces de programação de aplicativos (APIs) e interfaces de programação do sistema.

Java "Visão Geral da API Java" na página 321
O WebSphere eXtreme Scale fornece diversos recursos que são acessados programaticamente usando a linguagem de programação Java através de interfaces de programação de aplicativos (APIs) e interfaces de programação do sistema.

Informações relacionadas:

Documentação da API

Java Documentação da API

Executando um Cliente ou um Servidor de Aplicativos Integrado com o WebSphere Application Server no Rational Application Developer

Java

Configure e execute um aplicativo Java EE com um cliente ou servidor WebSphere eXtreme Scale com o tempo de execução integrado do WebSphere Application Server no Rational Application Developer. Se estiver configurando um servidor, iniciar o WebSphere Application Server inicia automaticamente o WebSphere eXtreme Scale.

Antes de Iniciar

As etapas a seguir são para o WebSphere Application Server Versão 7.0 com Rational Application Developer Versão 7.5. As etapas a seguir poderão variar se você estiver usando versões diferentes desses produtos.

Instale o Rational Application Developer com as extensões do Ambiente de Teste do WebSphere Application Server.

Instale o cliente ou servidor do WebSphere eXtreme Scale no Ambiente de Teste do WebSphere Application Server Versão 7.0 no diretório *rad_home*\runtimes\base_v7. Consulte Instalando o WebSphere eXtreme Scale ou o WebSphere eXtreme Scale Client com WebSphere Application Server para obter informações adicionais.

Procedimento

1. Defina o servidor eXtreme Scale que está integrado ao WebSphere Application Server para seu projeto.
   a. Na perspectiva J2EE, clique em **Janela > Mostrar Visualização > Servidores.**
   b. Clique com o botão direito do mouse na área de janela **Servidores**. Escolha **Novo > Servidor**.
   c. Escolha **IBM WebSphere Application Server v7.0**. Clique em Avançar.
   d. Selecione um perfil para usar. O padrão é was70profile1.
   e. Digite o nome do servidor. O padrão é server1.

f. Clique em **Next**.

g. Selecione seu aplicativo Java EE na área de janela **Disponível**. Clique em **Incluir >** para movê-lo para a área de janela **Configurado** no servidor. Clique em **Terminar**.

2. Para executar o aplicativo Java EE, inicie o servidor de aplicativos. Clique com o botão direito do mouse no **WebSphere Application Server v7.0** e selecione **Iniciar**.

Conceitos relacionados:

"Visão Geral da API Java" na página 321
O WebSphere eXtreme Scale fornece diversos recursos que são acessados programaticamente usando a linguagem de programação Java através de interfaces de programação de aplicativos (APIs) e interfaces de programação do sistema.

Java "Visão Geral da API Java" na página 321
O WebSphere eXtreme Scale fornece diversos recursos que são acessados programaticamente usando a linguagem de programação Java através de interfaces de programação de aplicativos (APIs) e interfaces de programação do sistema.

Informações relacionadas:

Documentação da API

Java Documentação da API

Acessando Dados com Aplicativos Cliente

Java

Após configurar seu ambiente de desenvolvimento, é possível começar a desenvolver aplicativos que criam, acessam e gerenciam os dados em sua grade de dados.

Sobre Esta Tarefa

Da perspectiva de um aplicativo cliente, usar o WebSphere eXtreme Scale envolve as seguintes etapas principais:

- Conexão com o serviço de catálogo por meio da obtenção de uma instância de ClientClusterContext.
- Obtenção de uma instância do ObjectGrid do cliente.
- Obtenção de uma instância da Sessão.
- Obtenção de uma instância do ObjectMap.
- Uso de métodos ObjectMap.

Conectando-se às Instâncias do ObjectGrid Distribuído Programaticamente

Java

É possível conectar a um ObjectGrid distribuído aos terminais de conexão para o domínio de serviço do catálogo. É necessário ter o nome do host e a porta do listener de cada servidor de catálogos no domínio de serviço de catálogo com o qual deseja se conectar.

Antes de Iniciar

- Para se conectar a uma grade de dados distribuída, você deve configurar o ambiente do lado do servidor com um serviço de catálogo e com os servidores de contêiner.

- Você deve ter a porta de listener para cada serviço de catálogo. Para obter informações adicionais, consulte “Planejamento para Portas de Rede” na página 300.
- Se o aplicativo cliente estiver em execução no WebSphere Application Server aumentado com eXtreme Scale, configure o domínio de serviço de catálogo usando o console administrativo WebSphere Application Server ou wsadmin.

Sobre Esta Tarefa

Ao executar em um aplicativo Java EE, considere usar o adaptador de recursos eXtreme Scale. O adaptador de recursos permite que o aplicativo consulte uma conexão ObjectGrid no Java Naming Directory Interface (JNDI) usando um connection factory do Java Connector Architecture (JCA), que simplifica significativamente o acesso à grade de dados e permite a integração com transações Java Transaction API (JTA). Para obter informações adicionais, consulte “Cenário: Usando JCA para Conectar Aplicativos Transacionais aos Clientes do eXtreme Scale” na página 189.

Os métodos ObjectGridManager.connect() se conectam a um domínio de serviço de catálogo usando os terminais de conexão fornecidos e retorna um objeto ClientClusterContext que é usado para recuperar as instâncias ObjectGrid para o domínio. Os terminais de conexão são uma lista delimitada por vírgula de combinações de host e de porta para cada servidor de catálogos no domínio de serviço de catálogo. Consulte o formato a seguir de terminais de serviço de catálogo:

```
catalogServiceEndpoints ::= <catalogServiceEndpoint> [,<catalogServiceEndpoint>]
catalogServiceEndpoint  ::= <hostName> : <listenerPort>
hostName                ::= The IP address or host name of a catalog service.
listenerPort            ::= The listener port that the catalog service is configured to use.
```

Depois de se conectar ao domínio de serviço de catálogo, use o método ObjectGridManagerFactory.getObjectGrid(ClientClusterContext ccc, String objectGridName) para recuperar uma instância de cliente ObjectGrid nomeada. Essa instância do ObjectGrid é um proxy para a grade de dados nomeada e é armazenada em cache no aplicativo cliente. A instância ObjectGrid representa uma conexão lógica para a grade de dados remota e tem encadeamento seguro. Todas as conexões físicas subjacentes para a grade de dados são gerenciadas automaticamente e podem tolerar eventos de falha.

As etapas de conexão variam dependendo de você estar usando uma configuração independente ou WebSphere Application Server.

Procedimento

- Conecte-se a uma grade de dados distribuída independente usando terminais de serviço de catálogo explícitos.

```
// Retrieve an ObjectGridManager instance.
ObjectGridManager ogm = ObjectGridManagerFactory.getObjectGridManager();

// Obtain a ClientClusterContext by connecting to a catalog
// service domain, manually suppling the catalog service endpoints,
// and optionally specifying the ClientSecurityConfiguration and
// client ObjectGrid override XML file URL.
String catalogServiceEndpoints = "host1:2809,host2:2809";
ClientClusterContext ccc = ogm.connect(catalogServiceEndpoints,
  (ClientSecurityConfiguration) null, (URL) null);
```

```
// Obtain a distributed ObjectGrid using ObjectGridManager and providing
// the ClientClusterContext.
ObjectGrid og = ogm.getObjectGrid(ccc, "Mygrid");
```

- Conecte-se a um domínio de serviço de catálogo a partir de um aplicativo cliente hospedado em WebSphere Application Server, em que o domínio de serviço de catálogo foi configurado usando o console administrativo ou a tarefa admin. Os terminais de serviço de catálogo podem ser recuperados de um identificador de domínio nomeado ou para o domínio padrão usando o ObjectGridManager.

```
// Retrieve an ObjectGridManager instance.
ObjectGridManager ogm = ObjectGridManagerFactory.getObjectGridManager();

// Retrieve the domain by its ID (the name given to it in the admin console or wsadmin)
// The CatalogDomainManager also includes methods to retrieve all domains and the default domain.
CatalogDomainInfo di = ogm.getCatalogDomainManager().getDomainInfo("ProductionDomain");
if(di == null) throw new IllegalStateException("Domain not configured");

// Connect to the domain using the catalog service endpoints and the security configuration
// in the CatalogDomainInfo object.  The client override ObjectGrid XML is optional
// and is manually supplied.
ClientClusterContext ccc = ogm.connect(di.getClientCatalogServiceEndpoints(),
  di.getClientSecurityConfiguration(), (URL) null);

// Obtain a distributed ObjectGrid using ObjectGridManager and by providing
// the ClientClusterContext.
ObjectGrid og = ogm.getObjectGrid(ccc, "MyGrid");
```

O que Fazer Depois

Se o domínio de serviço de catálogo estiver hospedado em um gerenciador de implementação WebSphere Application Server, os clientes fora da célula, incluindo os clientes Java Platform, Enterprise Edition, devem se conectar ao serviço de catálogo usando o nome do host do gerenciador de implementação e a porta de autoinicialização IIOP. Quando o serviço de catálogo for executado nas células do WebSphere Application Server e os clientes forem executados fora das células, consulte as páginas de configuração de domínio do eXtreme Scale no console administrativo WebSphere Application Server para obter as informações que você precisa para apontar um cliente para o serviço do catálogo.

Rastreando Atualizações de Mapas por um Aplicativo

Java

Quando um aplicativo está fazendo alterações em um Mapa durante uma transação, um objeto LogSequence rastreia estas alterações. Se o aplicativo alterar uma entrada no mapa, um objeto LogElement correspondente fornecerá os detalhes da mudança.

Os Loaders recebem um objeto LogSequence para um mapa específico sempre que um aplicativo solicita uma limpeza ou confirmação da transação. O Utilitário de Carga é repetido pelos objetos LogElement, no objeto LogSequence, e aplica cada objeto LogElement ao backend.

Os listeners ObjectGridEventListener registrados com um ObjectGrid também utilizam os objetos LogSequence. Estes listeners recebem um objeto LogSequence para cada mapa em uma transação confirmada. Os aplicativos podem utilizar estes listeners para esperar alterações de algumas entradas, como um acionador em um banco de dados convencional.

As seguintes interfaces ou classes relacionadas ao log são fornecidas pela estrutura do eXtreme Scale:

- com.ibm.websphere.objectgrid.plugins.LogElement
- com.ibm.websphere.objectgrid.plugins.LogSequence

- com.ibm.websphere.objectgrid.plugins.LogSequenceFilter
- com.ibm.websphere.objectgrid.plugins.LogSequenceTransformer

Interface LogElement

Um LogElement representa uma operação em uma entrada durante uma transação. Um objeto LogElement possui vários métodos para obter os vários atributos. Os atributos mais usados são de tipo e os atributos de valor atual procurados por getType() e getCurrentValue().

8.6+ O tipo é representado por uma das constantes definidas na interface LogElement: INSERT, UPDATE, DELETE, EVICT, FETCH, TOUCH ou UPSERT.

O valor atual representa o novo valor para a operação se ela é INSERT, UPDATE, FETCH ou UPSERT. Se a operação for TOUCH, DELETE ou EVICT, o valor atual será nulo. Este valor pode ser lançado no ValueProxyInfo quando um ValueInterface estiver sendo utilizado.

Consulte a documentação da API para obter mais detalhes sobre a interface LogElement.

Interface LogSequence

Na maioria das transações, ocorrem operações em mais de uma entrada em um mapa, portanto, são criados vários objetos LogElement. É necessário criar um objeto que atue como uma composição de vários objetos LogElement. A interface LogSequence atende esta finalidade contendo uma lista de objetos LogElement.

Consulte a documentação da API para obter mais detalhes sobre a interface LogSequence.

Usando o LogElement e o LogSequence

O LogElement e o LogSequence são amplamente utilizados no eXtreme Scale e por plug-ins do ObjectGrid que são gravados por usuários quando operações são propagadas de um componente ou servidor para outro componente ou servidor. Por exemplo, um objeto LogSequence pode ser utilizado pela função de propagação de transação do ObjectGrid distribuído para propagar as alterações para outros servidores ou pode ser aplicado ao armazenamento de persistência pelo loader. LogSequence é utilizado principalmente pelas seguintes interfaces.

- com.ibm.websphere.objectgrid.plugins.ObjectGridEventListener
- com.ibm.websphere.objectgrid.plugins.Loader
- com.ibm.websphere.objectgrid.plugins.Evictor
- com.ibm.websphere.objectgrid.Session

Exemplo de Utilitário de Carga

Esta seção demonstra como os objetos LogSequence e LogElement são utilizados em um Utilitário de Carga. Um Utilitário de Carga é utilizado para fins de carregamento ou persistência de dados num armazenamento persistente. O método batchUpdate da interface do Utilitário de Carga utiliza o objeto LogSequence:

```
void batchUpdate(TxID txid, LogSequence sequence) throws LoaderException,
OptimisticCollisionException;
```

O método batchUpdate é chamado quando um ObjectGrid precisa aplicar todas as alterações atuais no Utilitário de Carga. O Utilitário de Carga recebe uma lista de objetos LogElement para o mapa, encapsulados em um objeto LogSequence. A implementação do método batchUpdate deve ser repetida nas alterações e aplicada ao backend. O trecho de código a seguir demonstra como um Utilitário de Carga utiliza um objeto LogSequence. O fragmento é repetido no conjunto de mudanças e constrói três instruções de Java Database Connectivity (JDBC) em lote: inserts, updates e deletes:

```
public void batchUpdate(TxID tx, LogSequence sequence) throws LoaderException {
    // Obter uma conexão SQL para utilizar.
    Connection conn = getConnection(tx);
    try
    {
    // Processar a lista de alterações e construir um conjunto de instruções preparadas
    // para executar uma operação SQL update, insert ou delete
    // . As instruções são armazenadas em cache em stmtCache.
    Iterator iter = sequence.getPendingChanges();
    while(iter.hasNext())
    {
        LogElement logElement = (LogElement)iter.next();
        Object key = logElement.getCacheEntry().getKey();
        Object value = logElement.getCurrentValue();
        switch ( logElement.getType().getCode() )
        {
            case LogElement.CODE_INSERT:
                buildBatchSQLInsert( key, value, conn );
                break;
            case LogElement.CODE_UPDATE:
                buildBatchSQLUpdate( key, value, conn );
                break;
            case LogElement.CODE_DELETE:
                buildBatchSQLDelete( key, conn );
                break;
        }
    }
    // Executar as instruções de lote que foram construídas pelo loop acima.
    Collection statements = getPreparedStatementCollection( tx, conn );
    iter = statements.iterator();
    while(iter.hasNext())
    {
        PreparedStatement pstmt = (PreparedStatement) iter.next();
        pstmt.executeBatch();
    }
} catch (SQLException e) {
    LoaderException ex = new LoaderException(e);
    throw ex;
}
}
```

O exemplo anterior mostra a lógica de alto nível de processamento do argumento LogSequence. Entretanto, o exemplo não mostra os detalhes de como construir uma instrução SQL insert, update ou delete. O método getPendingChanges é chamado no argumento LogSequence para obter um iterador dos objetos LogElement que o Utilitário de Carga precisa para processar e o método LogElement.getType().getCode() é usado para determinar se um LogElement destina-se para uma operação SQL insert, update ou delete.

Amostra de Evictor

Também é possível usar os objetos LogSequence e LogElement com um Evictor. Um Evictor é utilizado para liberar as entradas do mapa de suporte com base em alguns critérios. O método apply da interface do Evictor utiliza LogSequence.

```
/**
* É chamado durante a confirmação de cache para permitir que o evictor
rastreie o uso de objetos
* em um mapa de apoio. Também relatará as entradas que foram liberadas com
* êxito.
*
* Sequência @param LogSequence de alterações no mapa
*/
void apply(LogSequence sequence);
```

Para obter informações sobre como o método apply utiliza o objeto LogSequence, consulte a amostra de código no tópico Gravando um Evictor Customizado.

Interfaces LogSequenceFilter e LogSequenceTransformer

Às vezes, é necessário filtrar os objetos LogElement para que apenas os objetos LogElement com alguns critérios sejam aceitos e rejeitar outros objetos. Por exemplo, é possível serializar um determinado LogElement com base em algum critério.

LogSequenceFilter resolve este problema com o seguinte método:

```
public boolean accept (LogElement logElement);
```

Este método retorna true se o LogElement especificado tiver que ser utilizado na operação e retorna false se o LogElement especificado não tiver que ser utilizado.

LogSequenceTransformer é uma classe que utiliza a função LogSequenceFilter. Utiliza LogSequenceFilter para filtrar alguns objetos LogElement e, em seguida, serializar os objetos LogElement aceitos. Esta classe possui dois métodos. O primeiro método é o seguinte:

```
public static void serialize(Collection logSequences, ObjectOutputStream stream,
   LogSequenceFilter filter, DistributionMode mode) throws IOException
```

Este método permite que o responsável pela chamada forneça um filtro para determinar quais LogElements incluir no processo de serialização. O parâmetro DistributionMode permite que o responsável pela chamada controle o processo de serialização. Por exemplo, se o modo de distribuição for apenas de invalidação, não será necessário serializar o valor. O segundo método desta classe é o método inflate, da seguinte forma:

```
public static Collection inflate(ObjectInputStream stream, ObjectGrid
   objectGrid) throws IOException, ClassNotFoundException
```

Esse método lê o formulário serializado de sequência de log, que foi criado pelo método serialize a partir do fluxo de entrada de objetos fornecido.

Interagindo com um ObjectGrid Usando a Interface ObjectGridManager

Java

A classe ObjectGridManagerFactory e a interface ObjectGridManager fornecem um mecanismo para criar, acessar e incluir dados para instâncias do ObjectGrid. A classe ObjectGridManagerFactory é uma classe auxiliar estática para acessar a interface ObjectGridManager, que é um singleton. A interface ObjectGridManager inclui vários métodos de conveniência para criar instâncias de um objeto do ObjectGrid. A interface ObjectGridManager também facilita a criação e armazenamento em cache de instâncias do ObjectGrid que podem ser acessadas por vários usuários.

Criando Instâncias do ObjectGrid com a Interface ObjectGridManager:

Java

Cada um desses métodos cria uma instância local de um ObjectGrid.

Instância na Memória Local

O trecho de código a seguir ilustra como obter e configurar uma instância de ObjectGrid local com o eXtreme Scale.

```
// Obtain a local ObjectGrid reference
        // you can create a new ObjectGrid, or get configured ObjectGrid
        // defined in ObjectGrid xml file
        ObjectGridManager objectGridManager =
     ObjectGridManagerFactory.getObjectGridManager();
        ObjectGrid ivObjectGrid =
     objectGridManager.createObjectGrid("objectgridName");

        // Add a TransactionCallback into ObjectGrid
        HeapTransactionCallback tcb = new HeapTransactionCallback();
        ivObjectGrid.setTransactionCallback(tcb);

        // Define a BackingMap
        // if the BackingMap is configured in ObjectGrid xml
        // file, you can just get it.
        BackingMap ivBackingMap = ivObjectGrid.defineMap("myMap");

        // Add a Loader into BackingMap
        Loader ivLoader = new HeapCacheLoader();
        ivBackingMap.setLoader(ivLoader);

        // initialize ObjectGrid
        ivObjectGrid.initialize();

        // Obtain a session to be used by the current thread.
        // Session can not be shared by multiple threads
        Session ivSession = ivObjectGrid.getSession();

        // Obtaining ObjectMap from ObjectGrid Session
        ObjectMap objectMap = ivSession.getMap("myMap");
```

Configuração Compartilhada Padrão

O código a seguir é um caso simples de como criar um ObjectGrid para compartilhar entre muitos usuários.

```
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.ObjectGridException;
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
import com.ibm.websphere.objectgrid.ObjectGridManager;
final ObjectGridManager oGridManager=
  ObjectGridManagerFactory.getObjectGridManager();
ObjectGrid employees =
 oGridManager.createObjectGrid("Employees",true);
employees.initialize();
employees.
/*sample continues..*/
```

O trecho de código Java precedente cria e armazena em cache o Employees ObjectGrid. O Employees ObjectGrid é inicializado com a configuração padrão e já está pronto para uso. O segundo parâmetro no método createObjectGrid é configurado como true, o que instrui o ObjectGridManager a armazenar em cache a instância do ObjectGrid que ele cria. Se este parâmetro for configurado como

false, a instância não é armazenada em cache. Cada instância do ObjectGrid possui um nome e a instância pode ser compartilhada entre vários clientes ou usuários com base em tal nome.

Se a instância do objectGrid for utilizada no compartilhamento ponto a ponto, o armazenamento em cache deve ser configurado como true. Para obter informações adicionais sobre o compartilhamento ponto a ponto, consulte Distribuição de alterações entre as Java Virtual Machines de peer.

Configuração XML

O WebSphere eXtreme Scale é altamente configurável. O exemplo anterior demonstra como criar um ObjectGrid simples sem nenhuma configuração. Este exemplo mostra como criar uma instância do ObjectdGrid pré-configurada que é baseada em um arquivo de configuração XML. É possível configurar uma instância do ObjectGrid programaticamente ou utilizando um arquivo de configuração baseado em XML. Também é possível configurar o ObjectGrid utilizando uma combinação de duas abordagens. A interface ObjectGridManager permite a criação de uma instância do ObjectGrid baseada na configuração XML. A interface ObjectGridManager possui vários métodos que utilizam uma URL como argumento. Cada arquivo XML transmitido para o ObjectGridManager deve ser validado no esquema. A validação XML pode ser desativada apenas quando o arquivo está previamente validado e nenhuma alteração foi feita no arquivo desde sua última validação. A desativação da validação poupa uma pequena quantidade de sobrecarga, mas introduz a possibilidade de utilizar um arquivo XML inválido. O IBM Java Developer Kit (JDK)Versão 6 ou posterior possui suporte para validação de XML. Ao utilizar um JDK que não tem este suporte, o Apache Xerces pode ser requerido para validar o XML.

O trecho de código Java a seguir demonstra como transmitir um arquivo de configuração XML para criar um ObjectGrid.

```
import java.net.MalformedURLException;
import java.net.URL;
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.ObjectGridException;
import com.ibm.websphere.objectgrid.ObjectGridManager;
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
boolean validateXML = true; // ativar a validação XML
boolean cacheInstance = true; // Armazenar a instância em cache
String objectGridName="Employees"; // Nome da URL do Object Grid
allObjectGrids = new URL("file:test/myObjectGrid.xml");
final ObjectGridManager oGridManager=
 ObjectGridManagerFactory.getObjectGridManager();
 ObjectGrid employees =
 oGridManager.createObjectGrid(objectGridName, allObjectGrids,
  bvalidateXML, cacheInstance);
```

O arquivo XML pode conter informações de configuração para vários ObjectGrids. O trecho de código anterior retorna especificamente o ObjectGrid Employees, supondo que a configuração de Employees esteja definida no arquivo.

Métodos createObjectGrid

```
.
/**
 * Um método de depósito de informações do provedor simples
 para retornar uma instância de um
 * Object Grid. É designado um nome exclusivo.
 * A instância do ObjectGrid não é armazenada em cache.
```

```
 * Os usuários podem então utilizar
 {@link ObjectGrid#setName(String)} para alterar o
 * nome do ObjectGrid.
 *
 * @return ObjectGrid uma instância do ObjectGrid
 com um nome exclusivo designado
 * @throws ObjectGridException qualquer erro
 encontrado durante a
 * criação do ObjectGrid
 */
public ObjectGrid createObjectGrid() throws ObjectGridException;

/**
 * Um método de depósito de informações do provedor simples para
 retornar uma instância de um ObjectGrid com
 * o nome especificado. As instâncias do ObjectGrid podem ser
 armazenadas em cache. Se um ObjectGrid
 * com este nome já tiver sido armazenado em cache, será emitida uma
 * ObjectGridException.
 *
 * @param objectGridName o nome do ObjectGrid a ser criado.
 * @param cacheInstance true, se a instância do ObjectGrid tiver
 que ser armazenada em cache
 * @return an ObjectGrid instance
 * @this o nome já foi armazenado em cache ou
 * qualquer erro durante a criação do ObjectGrid.
 */
public ObjectGrid createObjectGrid(String objectGridName,
boolean cacheInstance)
  throws ObjectGridException;

/**
 * Crie uma instância do ObjectGrid com o nome do ObjectGrid
 especificado. The
 * instância do ObjectGrid criada será armazenada em cache.
 * @param objectGridName o Nome da instância do ObjectGrid
 a ser criada.
 * @return an ObjectGrid instance
 * @throws ObjectGridException se um ObjectGrid com este
 nome já tiver sido
 * armazenado em cache ou algum erro encontrado durante
 a criação do ObjectGrid
 */
public ObjectGrid createObjectGrid(String objectGridName)
  throws ObjectGridException;

/**
 * Crie uma instância do ObjectGrid com base no nome do
 ObjectGrid e no
 * XML do cluster. A instância do ObjectGrid definida
 no arquivo XML com o nome do
 * ObjectGrid especificado será criada e retornada.
 Se tal ObjectGrid
 * não puder ser localizado no arquivo xml, será
 emitida uma exceção.
 *
 * Esta instância do ObjecGrid não pode ser armazenada
 em cache.
 *
 * Se a URL for nula, ela simplesmente será ignorada.
 Neste caso, este método se comportará
 * igual a {@link #createObjectGrid(String, boolean)}.
 *
 * @param objectGridName o Nome da instância do ObjectGrid
 a ser retornada. Ela
 * não deve ser nula.
 * @param xmlFile uma URL para um arquivo xml bem formado
```

```
 baseado no esquema do ObjectGrid.
 * @param enableXmlValidation se true o XML será validado
 * @param cacheInstance um valor booleano que indica se a(s)
 instância(s) do
 * ObjectGrid
 * definida(s) no arquivo XML será(ão) ou não armazenada(s)
 em cache. Se true, a(s) instância(s) será(ão)
 * armazenada(s) em cache.
 *
 * @throws ObjectGridException se um ObjectGrid com o mesmo nome
 * tiver sido armazenado em cache anteriormente, nenhum nome do
 ObjectGrid poderá ser localizado no arquivo xml
 * ou qualquer outro erro durante a criação do ObjectGrid.
 * @return an ObjectGrid instance
 * @see ObjectGrid
 */
public ObjectGrid createObjectGrid(String objectGridName,
final URL xmlFile,
final boolean enableXmlValidation, boolean cacheInstance)
 throws ObjectGridException;

/**
 * Processar um arquivo XML e criar uma Lista de objetos do
 ObjectGrid com base
 * no arquivo.
 * Estas instâncias do ObjecGrid podem ser armazenadas em cache.
 * Será emitida uma ObjectGridException ao tentar armazenar em cache
 * um ObjectGrid recém-criado que
 * tenha o mesmo nome que um ObjectGrid já armazenado em cache.
 *
 * @param xmlFile o arquivo que define um ObjectGrid ou vários
 * ObjectGrids
 * @param enableXmlValidation a configuração como true validará o
 arquivo XML
 * no esquema
 * @param cacheInstances configurado como true para armazenar em
 cache todas as instâncias do ObjectGrid
 * criadas com base no arquivo
 * @return an ObjectGrid instance
 * @throws ObjectGridException ao tentar criar e armazenar em cache um
 * ObjectGrid com o mesmo nome que um
 * ObjectGrid já armazenado em cache ou qualquer outro erro
 * ocorrido durante a
 * criação do ObjectGrid
 */
public List createObjectGrids(final URL xmlFile, final boolean
enableXmlValidation,
boolean cacheInstances) throws ObjectGridException;

/** Criar todos os ObjectGrids localizados no arquivo XML.
O arquivo XML será validado
 * no esquema. Cada instância do ObjectGrid criada será
 * armazenada(s) em cache. Será emitida uma ObjectGridException
 ao tentar armazenar em cache um
 * ObjectGrid recém-criado com o mesmo nome que um ObjectGrid
 * já armazenado em cache.
 * @param xmlFile O arquivo XML a ser processado. Os ObjectGrids
 serão criados com base
 * no conteúdo do arquivo.
 * @return Uma Lista de instâncias do ObjectGrid que foram criadas.
 * @throws ObjectGridException se um ObjectGrid que tenha o mesmo
 nome que qualquer um dos
 * localizados no XML já tiver sido armazenado em cache ou
 * qualquer outro erro encontrado durante a criação do ObjectGrid.
 */
public List createObjectGrids(final URL xmlFile) throws ObjectGridException;
```

```
/**
 * Processar o arquivo XML e criar uma única instância do
 ObjectGrid com o
 * objectGridName especificado apenas se um ObjectGrid
 com esse nome for localizado
 * no arquivo. Se não houver nenhum ObjectGrid com este
 nome definido no arquivo XML,
 * será emitida uma
 * ObjectGridException. A instância do ObjectGrid criada
 será armazenada em cache.
 * @param objectGridName nome do ObjectGrid a ser criado.
 Este ObjectGrid
 * deve ser definido no arquivo XML.
 * @param xmlFile o arquivo XML a ser processado
 * @return Um ObjectGrid recém-criado
 * @throws ObjectGridException se um ObjectGrid com o mesmo
 nome tiver sido
 * armazenado em cache anteriormente, nenhum nome do ObjectGrid
 poderá ser localizado no arquivo xml
 * ou qualquer outro erro durante a criação do ObjectGrid.
 */
public ObjectGrid createObjectGrid(String objectGridName, URL xmlFile)
  throws ObjectGridException;
```

Tarefas relacionadas:

Java "Resolução de Problemas de Conectividade do Cliente" na página 872
Há vários problemas comuns específicos para clientes e de conectividade do cliente que podem ser resolvidos conforme descrito nas seções a seguir.

Recuperando uma Instância ObjectGrid com a Interface ObjectGridManager:

Java

Use os métodos ObjectGridManager.getObjectGrid para recuperar as instâncias em cache.

Recuperando uma Instância de Cache

Como a instância Employees ObjectGrid foi armazenada em cache pela interface ObjectGridManager, outro usuário pode acessá-la com o fragmento de código a seguir:

```
ObjectGrid myEmployees = oGridManager.getObjectGrid("Employees");
```

Os dois métodos getObjectGrid a seguir retornam instâncias do ObjectGrid em cache:

- **Recuperando Todas as Instâncias em Cache**

  Para obter todas as instâncias do ObjectGrid que foram previamente armazenadas em cache, use o método getObjectGrids, que retorna uma lista de cada instância. Se nenhuma instância em cache existir, o método retornará null.

- **Recuperando uma Instância em Cache por Nome**

  Para obter uma instância em cache única de um ObjectGrid, use getObjectGrid(StringobjectGridName), passando o nome da instância em cache para o método. O método retorna a instância de ObjectGrid com o nome especificado ou retorna nulo se não houver nenhuma instância de ObjectGrid com esse nome.

Nota: Também é possível usar o método getObjectGrid para se conectar a uma grade distribuída. Consulte o "Conectando-se às Instâncias do ObjectGrid Distribuído Programaticamente" na página 345 para obter informações adicionais.

Removendo Instâncias do ObjectGrid com a Interface ObjectGridManager:

Java

Você pode usar dois métodos removeObjectGrid diferentes para remover as instâncias do ObjectGrid do cache.

Remover uma Instância do ObjectGrid

Para remover instâncias do ObjectGrid do cache, utilize um dos métodos removeObjectGrid. A interface do ObjectGridManager não mantém uma referência das instâncias que são removidas. Existem dois métodos remove. Um método utiliza um parâmetro booleano. Se o parâmetro booleano for configurado como `true`, o método destroy é chamado no ObjectGrid. A chamada para o método destroy no ObjectGrid encerra o ObjectGrid e libera todos os recursos que o ObjectGrid está usando. Uma descrição de como usar os dois métodos removeObjectGrid a seguir:

```
/**
 * Remover um ObjectGrid do cache de instâncias do ObjectGrid
 *
 * @param objectGridName o nome da instância do ObjectGrid a ser removida
 * do cache
 *
 * @throws ObjectGridException se um ObjectGrid com o objectGridName
 * não tiver sido localizado no cache
 */
public void removeObjectGrid(String objectGridName) throws ObjectGridException;

/**
 * Remover um ObjectGrid do cache de instâncias do ObjectGrid e
 * destruir seus recursos associados
 *
 * @param objectGridName o nome da instância do ObjectGrid a ser removida
 * do cache
 *
 * @param destroy destruir a instância do objectgrid e seus
 * recursos associados
 *
 * @throws ObjectGridException se um ObjectGrid com o objectGridName
 * não tiver sido localizado no cache
 */
public void removeObjectGrid(String objectGridName, boolean destroy)
 throws ObjectGridException;
```

Controlando o Ciclo de Vida e um ObjectGrid com a Interface ObjectGridManager:

Java

É possível usar a interface ObjectGridManager para controlar o ciclo de vida de uma instância ObjectGrid usando um bean ou um servlet de inicialização.

Gerenciando o Ciclo de Vida com um Bean de Inicialização

Um bean de inicialização é usado para controlar o ciclo de vida de uma instância ObjectGrid. Um bean de inicialização é carregado quando um aplicativo é iniciado. Com um bean de inicialização, o código pode ser executado sempre que um aplicativo for iniciado ou parado conforme o esperado. Para criar um bean de inicialização, utilize a interface home com.ibm.websphere.startupservice.AppStartUpHome e a interface remota com.ibm.websphere.startupservice.AppStartUp. Implemente os métodos start e stop no bean. O método start é chamado sempre que o aplicativo é inicializado. O método stop é chamado quando o aplicativo é encerrado. O método start é usado

para criar instâncias do ObjectGrid. O método stop é usado para remover as instâncias do ObjectGrid. A seguir há um fragmento de código que demonstra esse gerenciamento do ciclo de vida do ObjectGrid em um bean de inicialização:

```
public class MyStartupBean implements javax.ejb.SessionBean {
    private ObjectGridManager objectGridManager;

    /* The methods on the SessionBean interface have been
     * left out of this example for the sake of brevity */

    public boolean start(){
        // Iniciando o bean de inicialização
        // Este método é chamado quando o aplicativo é iniciado
        objectGridManager = ObjectGridManagerFactory.getObjectGridManager();
        try {
            // criar 2 ObjectGrids e armazenar estas instâncias em cache
            ObjectGrid bookstoreGrid = objectGridManager.createObjectGrid("bookstore", true);
            bookstoreGrid.defineMap("book");
            ObjectGrid videostoreGrid = objectGridManager.createObjectGrid("videostore", true);
            // na JVM,
            // estes ObjectGrids agora podem ser recuperados do
            //ObjectGridManager utilizando o método getObjectGrid(String)
        } catch (ObjectGridException e) {
            e.printStackTrace();
            return false;
        }

        return true;
    }

    public void stop()  {
        // Parando o bean de inicialização
        // Este método é chamado quando o aplicativo é parado
        try {
            // remover os ObjectGrids armazenados em cache e destruí-los
            objectGridManager.removeObjectGrid("bookstore", true);
            objectGridManager.removeObjectGrid("videostore", true);
        } catch (ObjectGridException e) {
            e.printStackTrace();
        }
    }
}
```

Depois que o método start for chamado, as instâncias recém criadas do ObjectGrid serão recuperadas a partir da interface do ObjectGridManager. Por exemplo, se um servlet está incluído no aplicativo, o servlet acessa o eXtreme Scale utilizando o seguinte trecho de código:

```
ObjectGridManager objectGridManager =
 ObjectGridManagerFactory.getObjectGridManager();
ObjectGrid bookstoreGrid = objectGridManager.getObjectGrid("bookstore");
ObjectGrid videostoreGrid = objectGridManager.getObjectGrid("videostore");
```

Gerenciando o Ciclo de Vida com um Servlet

Para gerenciar o ciclo de vida de um ObjectGrid em um servlet, será possível usar o método init para criar uma instância ObjectGrid e o método destroy para remover a instância ObjectGrid. Se a instância do ObjectGrid estiver em cache, ela será recuperada e manipulada no código de servlet. A seguir há um código que mostra a criação, a manipulação e a destruição de um ObjectGrid em um servlet:

```
public class MyObjectGridServlet extends HttpServlet implements Servlet {
    private ObjectGridManager objectGridManager;

    public MyObjectGridServlet() {
        super();
    }

    public void init(ServletConfig arg0) throws ServletException {
        super.init();
        objectGridManager = ObjectGridManagerFactory.getObjectGridManager();
        try {
            // criar e armazenar em cache um ObjectGrid denominado bookstore
            ObjectGrid bookstoreGrid =
      objectGridManager.createObjectGrid("bookstore", true);
            bookstoreGrid.defineMap("book");
```

```
        } catch (ObjectGridException e) {
            e.printStackTrace();
        }
    }

    protected void doGet(HttpServletRequest req, HttpServletResponse res)
        throws ServletException, IOException {
        ObjectGrid bookstoreGrid = objectGridManager.getObjectGrid("bookstore");
        Session session = bookstoreGrid.getSession();
        ObjectMap bookMap = session.getMap("book");
        // desempenhar operações no ObjectGrid armazenado em cache
        // ...
 // Close the session (optional in Version 7.1.1 and later) for improved performance
 session.close();
  }
    public void destroy() {
        super.destroy();
        try {
            // remover e destruir o ObjectGrid bookstore armazenado em cache
            objectGridManager.removeObjectGrid("bookstore", true);
        } catch (ObjectGridException e) {
            e.printStackTrace();
        }
    }
}
```

Acesso ao Shard ObjectGrid: Java

O WebSphere eXtreme Scale atinge altas taxas de processamento movendo a lógica para onde os dados estão e retornando apenas resultados ao cliente.

A lógica de aplicativo em uma Java Virtual Machine (JVM) cliente precisa executar o pull de dados do servidor JVM que contém os dados e executar o push back quando ocorre o commit da transação. Esse processo reduz a taxa em que os dados podem ser processados. Se a lógica de aplicativo estivesse no mesmo JVM que o shard que está hospedando os dados, então a latência de rede e o custo de delegação seriam eliminados e poderia fornecer um significativo impulso no desempenho.

Referência Local para Dados do Shard

As APIs do ObjectGrid fornecem uma Session para o método do lado do servidor. Tal objeto Session é uma referência direta aos dados do shard. Não há nenhuma lógica de roteamento nesse caminho. A lógica de aplicativo pode trabalhar com os dados desse shard diretamente. O Session não pode ser utilizado para acessar os dados em outra partição porque não há nenhuma lógica de roteamento.

Um plug-in do Utilitário de Carga também fornece um meio para receber um evento quando um shard assume a função de partição primária. Um aplicativo pode implementar um Utilitário de Carga e implementar a interface do ReplicaPreloadController. O método check preload status é chamado apenas quando o shard assume a função de primário. O objeto Session fornecido a esse método é uma referência local aos dados dos shards. Essa abordagem é utilizada normalmente se o shard primário de uma partição precisar iniciar alguns encadeamentos ou assinar uma malha de mensagens para o tráfego relacionado à partição. Ele pode iniciar um encadeamento para escutar mensagens num Mapa local, por meio da API getNextKey.

Otimização Colocada do Cliente-Servidor

Se um aplicativo utiliza as APIs do cliente para acessar uma partição que pode ter sido colocada com a JVM que contém o cliente, a rede será evitada mas ainda ocorrerá alguma delegação devido a problemas de implementação atuais. Se uma grade particionada é utilizada, então não há impacto no desempenho do aplicativo porque (N-1)/número N de chamadas são roteadas para uma JVM diferente. Se você sempre precisar de acesso local com um shard, então, utilize o Utilitário de Cargo ou as APIs do ObjectGrid para chamar est lógica.

Acessando Dados com Índices (API de Índice)

Java

Use indexação para acesso a dados mais eficiente.

Sobre Esta Tarefa

A classe HashIndex é a implementação de plug-in de índice integrada que pode suportar ambas as interfaces integradas de índice a seguir: MapIndex e MapRangeIndex. Também é possível criar seus próprios índices. É possível incluir HashIndex como um índice estático ou dinâmico no mapa de apoio, obter um objeto proxy do índice MapIndex ou MapRangeIndex e usar o objeto proxy do índice para localizar objetos em cache.

Se desejar iterar por meio das chaves em um mapa local, o índice padrão poderá ser usado. Este índice não requer nenhuma configuração, porém ele deve ser usado com relação ao shard, usando um agente ou uma instância do ObjectGrid recuperados a partir do método ShardEvents.shardActivated(shard do ObjectGrid).

Nota: Em um ambiente distribuído, se o objeto do índice for obtido de um cliente do ObjectGrid, o índice possuirá um objeto de índice do tipo cliente e todas as operações de índice executadas em um ObjectGrid do servidor remoto. Se o mapa for particionado, as operações de índice executarão em cada partição remotamente. Os resultados de cada partição são mesclados antes de retornar os resultados para o aplicativo. O desempenho é determinado pelo número de partições e pelo tamanho do resultado retornado por cada partição. Um desempenho insuficiente poderá ocorrer se ambos os fatores forem altos.

Procedimento

1. Se desejar usar índices diferente do índice local padrão, inclua plug-ins de índice no mapa de apoio.
   - **Configuração XML**:

```
<backingMapPluginCollection id="person">
     <bean id="MapIndexplugin"
   className="com.ibm.websphere.objectgrid.plugins.index.HashIndex">
         <property name="Name"
type="java.lang.String" value="CODE"
      description="index name" />
         <property name="RangeIndex" type="boolean" value="true"
      description="true for MapRangeIndex" />
         <property name="AttributeName"
type="java.lang.String" value="employeeCode" description="attribute name" />
     </bean>
</backingMapPluginCollection>
```

     Neste exemplo de configuração XML, a classe HashIndex integrada é usada como o plug-in de índice. A classe HashIndex suporta propriedades que os usuários podem configurar, como Name, RangeIndex e AttributeName no exemplo anterior.

     – A propriedade **Name** é configurada como `CODE`, uma sequência que identifica este plug-in de índice. O valor da propriedade Name deve ser

único dentro do escopo do BackingMap, e pode ser usado para recuperar o objeto do índice pelo nome a partir da instância de ObjectMap para o BackingMap.

– A propriedade **RangeIndex** é configurada como `true`, o que significa que o aplicativo pode efetuar cast do objeto do índice recuperado para a interface MapRangeIndex. Se a propriedade RangeIndex for configurada como `false`, o aplicativo poderá apenas efetuar cast do objeto do índice recuperado para a interface MapIndex. Um MapRangeIndex suporta funções para localizar dados usando funções de intervalo, como maior que, menor que, ou ambas, enquanto um MapIndex suporta apenas funções iguais. Se o índice for usado por consulta, a propriedade **RangeIndex** deverá ser configurada para `true` em índices de atributo único. Para um índice de relacionamento e um índice composto, a propriedade RangeIndex deve ser configurada para `false`.

– A propriedade **AttributeName** é configurada como `employeeCode`, o que significa que o atributo **employeeCode** do objeto em cache é usado para construir um índice de atributo único. Se um aplicativo precisar procurar por objetos em cache com diversos atributos, a propriedade **AttributeName** poderá ser configurada para uma lista de atributos delimitados por vírgula, rendendo um índice composto.

- **Configuração programática:**

  A interface BackingMap tem dois métodos que podem ser usados para incluir plug-ins de índice estático: addMapIndexplugin e setMapIndexplugins. Para obter mais informações, consulte API do BackingMap . O exemplo a seguir cria a mesma configuração que o exemplo de configuração XML :

```
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
import com.ibm.websphere.objectgrid.ObjectGridManager;
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.BackingMap;

    ObjectGridManager ogManager = ObjectGridManagerFactory.getObjectGridManager();
    ObjectGrid ivObjectGrid = ogManager.createObjectGrid( "grid" );
    BackingMap personBackingMap = ivObjectGrid.getMap("person");

    //utilize a classe HashIndex interna como a classe de plugin do índice.
    HashIndex mapIndexplugin = new HashIndex();
    mapIndexplugin.setName("CODE");
    mapIndexplugin.setAttributeName("EmployeeCode");
    mapIndexplugin.setRangeIndex(true);
    personBackingMap.addMapIndexplugin(mapIndexplugin);
```

2. Acesse as chaves e valores de mapa com índices.

   - **Índice de local:**

     Para iterar por meio das chaves e valores em um mapa local, o índice padrão poderá ser usado. O índice padrão funciona apenas com relação ao shard, usando um agente ou usando a instância do ObjectGrid recuperados com o método ShardEvents.shardActivated(shard do ObjectGrid). Consulte o seguinte exemplo:

```
MapIndex keyIndex = (MapIndex)
objMap.getIndex(MapIndexPlugin.SYSTEM_KEY_INDEX_NAME);
Iterator keyIterator = keyIndex.findAll();
```

   - **Índices estáticos:**

     Após um plug-in de índice estático ser incluído em uma configuração de BackingMap e a instância de ObjectGrid de abrangência ser inicializada, os aplicativos podem recuperar o objeto do índice por nome a partir da instância do ObjectMap para o BackingMap. Lance o objeto de índice para a interface de índice do aplicativo. As operações que a interface do índice do aplicativo suporta podem executar agora.

```
Session session = ivObjectGrid.getSession();
ObjectMap map = session.getMap("person");
MapRangeIndex codeIndex = (MapRangeIndex) m.getIndex("CODE");
Iterator iter = codeIndex.findLessEqual(new Integer(15));
while (iter.hasNext()) {
  Object key = iter.next();
  Object value = map.get(key);
}
// Close the session (optional in Version 7.1.1 and later) for improved performance
session.close();
```

- **Índices dinâmicos:**

  É possível criar e remover índices dinâmicos a partir de uma instância do BackingMap programaticamente a qualquer momento. Um índice dinâmico se difere de um índice estático porque o índice dinâmico pode ser criado mesmo depois que a instância do ObjectGrid de abrangência tiver sido inicializada. Diferentemente da indexação estática, a indexação dinâmica é um processo assíncrono e precisa estar em estado de pronto antes de ser usada. Este método utiliza a mesma abordagem para recuperação e utilização de índices dinâmicos como índices estáticos. É possível remover um índice dinâmico se ele não for mais necessário. A interface BackingMap possui métodos para criar e remover índices dinâmicos.

  Consulte a API BackingMap para obter mais informações sobre os métodos createDynamicIndex e removeDynamicIndex.

```
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
import com.ibm.websphere.objectgrid.ObjectGridManager;
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.BackingMap;

        ObjectGridManager ogManager = ObjectGridManagerFactory.getObjectGridManager();
        ObjectGrid og = ogManager.createObjectGrid("grid");
        BackingMap bm = og.getMap("person");
        og.initialize();

        // create index after ObjectGrid initialization without DynamicIndexCallback.
        bm.createDynamicIndex("CODE", true, "employeeCode", null);

        try {
            //Se não estiver utilizando DynamicIndexCallback, será necessário aguardar que o Índice esteja pronto.
            //O tempo de espera depende do tamanho atual do mapa
            Thread.sleep(3000);
        } catch (Throwable t) {
            // ...
        }

        // When the index is ready, applications can try to get application index
        // interface instance.
        // Applications have to find a way to ensure that the index is ready to use,
        // if not using DynamicIndexCallback interface.
        // The following example demonstrates the way to wait for the index to be ready
        // Consider the size of the map in the total waiting time.

        Session session = og.getSession();
        ObjectMap m = session.getMap("person");
        MapRangeIndex codeIndex = null;

        int counter = 0;
        int maxCounter = 10;
        boolean ready = false;
        while(!ready && counter < maxCounter){
            try {
                counter++;
                codeIndex = (MapRangeIndex) m.getIndex("CODE");
                ready = true;
            } catch (IndexNotReadyException e) {
                // implies index is not ready, ...
                System.out.println("Index is not ready. continue to wait.");
                try {
                    Thread.sleep(3000);
                } catch (Throwable tt) {
                    // ...
                }
            } catch (Throwable t) {
                // unexpected exception
                t.printStackTrace();
            }
        }

        if(!ready){
            System.out.println("Index is not ready.  Need to handle this situation.");
        }

        // Use the index to peform queries
        // Refer to the MapIndex or MapRangeIndex interface for supported operations.
        // The object attribute on which the index is created is the EmployeeCode.
        // Assume that the EmployeeCode attribute is Integer type: the
        // parameter that is passed into index operations has this data type.

        Iterator iter = codeIndex.findLessEqual(new Integer(15));

        // remove the dynamic index when no longer needed
```

```
        bm.removeDynamicIndex("CODE");
// Close the session (optional in Version 7.1.1 and later) for improved performance
session.close();
```

O que Fazer Depois

É possível usar a interface DynamicIndexCallback para obter notificações nos eventos de indexação. Consulte o “Interface DynamicIndexCallback” na página 364 para obter informações adicionais.

Conceitos relacionados:

Java "Plug-ins para Indexar Dados" na página 580
Dependendo do tipo de índices que você deseja construir, o WebSphere eXtreme Scale fornece plug-ins integrados que podem ser incluídos no BackingMap para construir um índice.

Java "Plug-ins para Indexação Customizada de Objetos de Cache" na página 593
Com um plug-in MapIndexPlugin, ou índice, é possível gravar estratégias de indexação customizadas que vão além de índices integrados fornecidos pelo eXtreme Scale.

Java "Usando um Índice Composto" na página 596
O HashIndex composto aprimora o desempenho da consulta e evita a custosa varredura de mapa. O recurso também fornece uma maneira conveniente para a API HashIndex localizar objetos em cache quando os critérios de busca envolvem muitos atributos.

Java "Indexação" na página 280
Use o plug-in MapIndexPlugin para construir um índice ou vários índices em um BackingMap para suportar acesso a dados sem chave.

Java "Utilizando o Índice Global" na página 599
O índice global pode melhorar o desempenho da procura de dados em ambiente particionado grande, por exemplo 100 partições.

"Utilizando o Índice Global" na página 599
O índice global pode melhorar o desempenho da procura de dados em ambiente particionado grande, por exemplo 100 partições.

"Otimização de Consulta do Cliente Utilizando Índices Globais" na página 759
Ao executar consultas a partir do ObjectGrid do cliente, é necessário configurar a partição se os mapas envolvidos são particionados. Em um grande ambiente do ObjectGrid particionado, o aplicativo geralmente precisa executar consultas paralelas simultaneamente em todas as partições para obter o resultado da consulta completo. Por exemplo, se houver 100 partições, o aplicativo deverá executar a mesma consulta em todas as 100 partições e mesclar os resultados da consulta para obter o resultado da consulta completo. Isto geralmente consome grandes quantidades de recurso do sistema.

"Ajustando o Desempenho de Consulta" na página 746
Para ajustar o desempenho de suas consultas, utilize as técnicas e dicas a seguir.

Referências relacionadas:

Java "Interface DynamicIndexCallback" na página 364
A interface DynamicIndexCallback foi projetada para aplicativos que desejam obter notificações nos eventos de indexação de ready, error ou destroy. O DynamicIndexCallback é um parâmetro opcional para o método createDynamicIndex do BackingMap. Com uma instância DynamicIndexCallback registrada, os aplicativos podem executar a lógica de negócios ao receber notificação de um evento de indexação.

Java "Atributos do Plug-in HashIndex" na página 589
É possível usar os seguintes atributos para configurar o plug-in HashIndex. Esses atributos definem propriedades, como se você estiver usando um atributo ou HashIndex composto ou se a indexação do intervalo estiver ativada.

Java "Atributos do Plug-in InverseRangeIndex" na página 583
É possível usar os seguintes atributos para configurar o plug-in InverseRangeIndex. Esses atributos definem propriedades sobre como o índice é construído.

Java Interface GlobalIndex

Informações relacionadas:

Java API DynamicIndexCallback

Interface DynamicIndexCallback: Java

A interface DynamicIndexCallback foi projetada para aplicativos que desejam obter notificações nos eventos de indexação de ready, error ou destroy. O DynamicIndexCallback é um parâmetro opcional para o método createDynamicIndex do BackingMap. Com uma instância DynamicIndexCallback registrada, os aplicativos podem executar a lógica de negócios ao receber notificação de um evento de indexação.

Eventos de Indexação

Por exemplo, o evento ready significa que o índice está pronto para utilização. Quando uma notificação para este evento for recebida, um aplicativo poderá tentar recuperar a instância da interface do índice do aplicativo e utilizá-la.

Exemplo: Usando a Interface EntityIndexCallback

```
BackingMap personBackingMap = ivObjectGrid.getMap("person");
    DynamicIndexCallback callback = new DynamicIndexCallbackImpl();
    personBackingMap.createDynamicIndex("CODE", true, "employeeCode", callback);


    class DynamicIndexCallbackImpl implements DynamicIndexCallback {
        public DynamicIndexCallbackImpl() {
        }

        public void ready(String indexName) {
            System.out.println("DynamicIndexCallbackImpl.ready() -> indexName = " + indexName);

            // Simulate what an application would do when notified that the index is ready.
            // Normally, the application would wait until the ready state is reached and then proceed
            // with any index usage logic.
            if("CODE".equals(indexName)) {
                ObjectGridManager ogManager = ObjectGridManagerFactory.getObjectGridManager();
                ObjectGrid og = ogManager.createObjectGrid("grid");
                Session session = og.getSession();
                ObjectMap map = session.getMap("person");
                MapIndex codeIndex = (MapIndex) map.getIndex("CODE");
                Iterator iter = codeIndex.findAll(codeValue);
  // Close the session (optional in Version 7.1.1 and later) for improved performance
  session.close();
    }
        }

        public void error(String indexName, Throwable t) {
            System.out.println("DynamicIndexCallbackImpl.error() -> indexName = " + indexName);
            t.printStackTrace();
        }

        public void destroy(String indexName) {
            System.out.println("DynamicIndexCallbackImpl.destroy() -> indexName = " + indexName);
        }
    }
```

Tarefas relacionadas:

Java "Acessando Dados com Índices (API de Índice)" na página 359
Use indexação para acesso a dados mais eficiente.

Informações relacionadas:

Java API DynamicIndexCallback

Uso de Sessões para Acessar Dados na Grade

Java

Os aplicativos podem iniciar e terminar transações através da interface Session. A interface Session também fornece acesso ao aplicativo com base nas interfaces ObjectMap e JavaMap.

Cada instância de ObjectMap ou de JavaMap está diretamente ligada a um objeto de Sessão específico. Cada encadeamento que desejar acesso a um eXtreme Scale deve primeiro obter uma Sessão do objeto ObjectGrid. Uma instância de Sessão não pode ser compartilhada simultaneamente entre encadeamentos. O WebSphere eXtreme Scale não usa qualquer armazenamento local do encadeamento, mas restrições de plataforma podem limitar a oportunidade de passar uma Sessão de um encadeamento para outro.

Métodos

Método Get

Um aplicativo obtém uma instância da Sessão a partir de um objeto ObjectGrid usando o método ObjectGrid.getSession. O exemplo a seguir demonstra como obter uma instância de Session:

```
ObjectGrid objectGrid = ...; Session sess = objectGrid.getSession();
```

Após uma Sessão ter sido obtida, o encadeamento mantém uma referência à sessão para sua própria utilização. Chamar o método getSession várias vezes sempre retorna, cada vez, um novo objeto de Sessão.

Métodos de Transações e Sessão

Uma Sessão pode ser utilizada para iniciar, confirmar ou efetuar rollback de transações. As operações em BackingMaps que utilizam ObjectMaps e JavaMaps são desempenhadas de maneira mais eficiente em uma transação de Sessão. Quando uma transação é iniciada, as alterações em um ou mais BackingMaps nesse escopo de transação são armazenadas em um cache de transações especiais até que a transação seja confirmada. Quando uma transação é confirmada, as alterações pendentes são aplicadas aos BackingMaps e Loaders e se tornam visíveis a outros clientes desse ObjectGrid.

O WebSphere eXtreme Scale também suporta a habilidade de automaticamente consolidar transações, também conhecida como auto-consolidação. Se quaisquer operações do ObjectMap forem desempenhadas fora do contexto de uma transação ativa, uma transação implícita será iniciada antes da operação e a transação será automaticamente confirmada antes de retornar o controle ao aplicativo.

```
Session session = objectGrid.getSession();
ObjectMap objectMap = session.getMap("someMap");
session.begin();
objectMap.insert("key1", "value1");
objectMap.insert("key2", "value2");
session.commit();
objectMap.insert("key3", "value3"); // auto-commit
```

Método Session.flush

O método Session.flush faz sentido apenas quando um Loader está associado a um BackingMap. O método flush chama o Loader com o conjunto atual de alterações no cache de transações. O Loader aplica as alterações ao backend. Estas alterações não são confirmadas quando o flush é chamado. Se uma transação de Sessão for confirmada após uma chamada de flush, apenas as atualizações que ocorrem após a chamada do flush serão aplicadas ao Loader. Se uma transação de Sessão receber rollback após uma chamada de flush, as alterações limpas serão descartadas com todas as demais alterações pendentes na transação. Utilize o método Flush com moderação, pois ele limita a oportunidade de operações de batch em um Loader. A seguir está um exemplo do uso do método Session.flush:

```
Session session = objectGrid.getSession();
session.begin();
// fazer algumas alterações
...
session.flush(); // enviar estas alterações para o Loader, mas ainda não confirmar
// fazer mais algumas alterações
...
session.commit();
```

Método NoWriteThrough

Alguns mapas são suportados por um Loader, que fornece armazenamento persistente aos dados no mapa. Algumas vezes, é útil consolidar dados apenas no mapa do eXtreme Scale e não executar o push de dados para fora do Utilitário de Carga. A interface Session fornece o método beginNoWriteThough para esta finalidade. O método beginNoWriteThrough inicia uma transação como o método begin. Com o método beginNoWriteThrough, quando a transação é confirmada, os dados são confirmados apenas para o mapa na memória e não são confirmados para o armazenamento persistente que é fornecido pelo Loader. Este método é muito útil ao desempenhar o pré-carregamento de dados no mapa.

Ao utilizar uma instância do ObjectGrid distribuído, o método beginNoWriteThrough é útil para fazer alterações apenas no near cache, sem modificar o far cache no servidor. Se os dados forem considerados stale no near cache, a utilização do método beginNoWriteThrough pode permitir que entradas sejam invalidadas no near cache sem invalidá-las também no servidor.

A interface Session também fornece o método isWriteThroughEnabled para determinar qual o tipo de transação está ativo no momento.

```
Session session = objectGrid.getSession();
session.beginNoWriteThrough();
// fazer algumas alterações...
session.commit(); // estas alterações não serão enviadas ao Loader
```

Obter o Método de Objeto TxID

O objeto TxID é um objeto opaco que identifica a transação ativa. Utilize o objeto TxID para as seguintes finalidades:

- Para comparação quando estiver procurando uma transação específica.
- Para armazenar dados compartilhados entre os objetos TransactionCallback e Loader.
- Identificar se a transação foi iniciada a partir de uma transação de sessão que estava usando um protocolo one-phase ou two-phase commit. Examinando a saída TxID.toString(), é possível determinar se a transação era para uma transação de partição única ou multipartição. Se a sequência iniciar com a palavra-chave "Local", isto indica uma transação de partição única. Por exemplo: `Local-40000139-72B2-C037-E000-1C271366B073` Se a sequência iniciar com a palavra-chave "WXS", isto indica uma transação multipartição. Por exemplo: `WXS-40000139-72B2-BD3A-E000-1C271366B073`

Consulte o plug-in TransactionCallback e Loaders para obter informações adicionais sobre o recurso de slot do Objeto.

Método de monitoramento de desempenho

Se estiver usando o eXtreme Scale dentro do WebSphere Application Server, pode ser necessário reiniciar o tipo de transação para monitoramento de desempenho. É

possível configurar o tipo de transação com o método setTransactionType. Consulte Monitoramento do Desempenho do ObjectGrid com a PMI (Performance Monitoring Infrastructure) do WebSphere Application Server para obter informações adicionais sobre o método setTransactionType.

Processar um Método LogSequence Completo

O WebSphere eXtreme Scale pode propagar conjuntos de alterações de mapas para listeners de ObjectGrid como um meio de distribuição de mapas de um Java Virtual Machine para outro. Para facilitar o processamento pelo listener de LogSequences recebidos, a interface Session fornece o método processLogSequence. Este método examina cada LogElement no LogSequence e desempenha uma operação apropriada, por exemplo, inserção, atualização, invalidação e outros, no BackingMap identificado pelo MapName LogSequence. Uma Sessão do ObjectGrid deve estar disponível antes de o método processLogSequence ser chamado. O aplicativo também é responsável por emitir as chamadas de confirmação ou de rollback apropriadas para concluir a Sessão. O processamento da confirmação automática não está disponível para esta chamada de método. O processamento normal pelo ObjectGridEventListener receptor na JVM remota seria iniciar uma Sessão utilizando o método beginNoWriteThrough, que evita a propagação sem fim de alterações, seguido de uma chamada para este método processLogSequence e, então, consolidando ou retrocedendo a transação.

```
// Utilizar o objeto de Sessão transmitido durante
//ObjectGridEventListener.initialization...
session.beginNoWriteThrough();
// processar o LogSequence recebido
try {
 session.processLogSequence(receivedLogSequence);
} catch (Exception e) {
 session.rollback(); throw e;
}
// confirmar as alterações
session.commit();
```

Método markRollbackOnly

Este método é utilizado para marcar a transação atual como "apenas rollback". Marcar uma transação como "apenas rollback" assegura que, mesmo que o método commit seja chamado pelo aplicativo, a transação receba rollback. Este método geralmente é utilizado pelo próprio ObjectGrid ou pelo aplicativo quando ele sabe que pode ocorrer danos nos dados se a transação tiver permissão para ser confirmada. Após este método ser chamado, o objeto Throwable que é passado a este método é encadeado na exceção com.ibm.websphere.objectgrid.TransactionException que resulta do método commit se for chamado em uma Sessão que foi anteriormente marcada como "apenas retrocesso". As chamadas subsequentes para este método para uma transação que já está marcada como "apenas rollback" serão ignoradas. Ou seja, apenas a primeira chamada que transmite uma referência Throwable não nula é utilizada. Quando a transação marcada estiver concluída, a marca "apenas rollback" será removida para que a próxima transação iniciada pela Sessão possa ser confirmada.

Método isMarkedRollbackOnly

Retorna se a Sessão está marcada como "apenas rollback". O true booleano será retornado por este método apenas se um método markRollbackOnly tiver sido chamado anteriormente nesta Sessão e a transação iniciada pela Sessão ainda estiver ativa.

Método setTransactionTimeout

Configure o tempo limite de transação para a próxima transação iniciada por esta Sessão como um número de segundos especificado. Este método não afeta o tempo limite da transação de nenhuma transação iniciada anteriormente por esta Sessão. Afeta apenas as transações iniciadas após este método ter sido chamado. Se este método nunca for chamado, o valor de tempo limite transmitido para o método setTxTimeout do método com.ibm.websphere.objectgrid.ObjectGrid será utilizado.

Método getTransactionTimeout

Este método retorna o valor de tempo limite da transação em segundos. O último valor que foi transmitido como o valor de tempo limite para o método setTransactionTimeout é retornado por este método. Se o método setTransactionTimeout nunca for chamado, o valor de tempo limite transmitido para o método setTxTimeout do método com.ibm.websphere.objectgrid.ObjectGrid será utilizado.

transactionTimedOut

Este método retorna true booleano se a transação atual iniciada por esta Sessão tiver seu tempo limite excedido.

Método isFlushing

Este método retorna true booleano apenas se todas as alterações de transação forem esvaziadas do plug-in do Utilitário de Carga como resultado do método flush da interface Session que está sendo chamada. Um plug-in do Utilitário de Carga pode achar este método útil quando ele precisar saber porquê seu método batchUpdate foi chamado.

Método isCommitting

Este método retorna true booleano apenas se todas as alterações de transação forem confirmadas como resultado do método commit da interface Session que está sendo chamada. Um plug-in do Loader pode achar este método útil quando precisar saber por que seu método batchUpdate foi chamado.

Método setRequestRetryTimeout

Este método define o valor de tempo limite de nova tentativa para a sessão em milissegundos. Se o cliente definir um tempo limite de nova tentativa de solicitação, a configuração da sessão prevalece em relação ao valor do cliente.

Método getRequestRetryTimeout

Este método obtém a configuração atual de tempo limite de nova tentativa na sessão. Uma valor de `-1` indica que o tempo limite não está configurado. Um valor de `0` indica que ele está no modo fail-fast. Um valor maior que `0` indica a configuração de tempo limite em milissegundos.

SessionHandle para Roteamento: Java

Quando estiver usando uma política de posicionamento de partição por contêiner, um objeto SessionHandle pode ser usado. Um objeto SessionHandle contém informações de partição para a Sessão atual e pode ser reusado para uma nova Sessão.

Um objeto SessionHandle inclui informações para a partição à qual a Sessão atual está limitada. O SessionHandle é extremamente útil para a política de posicionamento de partição por contêiner e pode ser serializado com a serialização Java padrão.

Se você tiver um objeto SessionHandle, esse identificador poderá ser aplicado em uma Sessão com o método setSessionHandle(SessionHandle target), passando o identificador como o destino. O objeto SessionHandle pode ser recuperado com o método Session.getSessionHandle.

Como ele se aplica apenas em um cenário de posicionamento por contêiner, obter o objeto SessionHandle emitirá uma IllegalStateException se uma determinada grade de dados tiver diversos conjuntos de mapas por contêiner ou não tiver nenhum conjunto de mapas por contêiner. Se o método setSessionHandle não for chamado antes de chamar o método getSessionHandle, o objeto SessionHandle apropriado será selecionado com base na configuração das propriedades do cliente.

Também é possível usar a classe auxiliar SessionHandleTransformer para converter o identificador em formatos diferentes. Os métodos desta classe podem alterar uma representação do identificador da matriz de bytes para a instância, da sequência para instância, e vice-versa, para ambos os casos e também podem gravar o conteúdo do identificador no fluxo de saída.

Para obter um exemplo de como é possível usar um objeto SessionHandle, consulte Roteamento para Zonas Preferenciais.

Integração do SessionHandle: Java

Um objeto SessionHandle inclui informações de partição para o Session ao qual ele está ligado e facilita o roteamento da solicitação. Os objetos SessionHandle se aplicam apenas no cenário de posicionamento de partição por contêiner.

Objeto SessionHandle para Roteamento de Solicitação

É possível ligar um objeto SessionHandle a um Session das seguintes formas:

Dica: Em cada uma das chamadas de método a seguir, depois de um objeto SessionHandle ser ligado a um Session, o objeto SessionHandle poderá ser obtido a partir do método Session.getSessionHandle.

- **Chame o método Session.getSessionHandle:** Quando este método é chamado, se nenhum objeto SessionHandle estiver ligado ao Session, um objeto SessionHandle será selecionado aleatoriamente e ligado ao Session.
- **Chame as operações transacionais de criação, leitura, atualização e de exclusão:** Quando esses métodos são chamados no tempo de confirmação, se nenhum objeto SessionHandle estiver ligado ao Session, um objeto SessionHandle será selecionado aleatoriamente e ligado ao Session.
- **Chame o método ObjectMap.getNextKey:** Quando esse método é chamado, se nenhum objeto SessionHandle estiver ligado ao Session, a solicitação da operação será roteada aleatoriamente para partições individuais até a chave ser obtida. Se uma chave for retornada de uma partição, um objeto SessionHandle

correspondente a essa partição será ligado ao Session. Se nenhuma chave for localizada, nenhum SessionHandle será ligado ao Session.

- **Chame os métodos QueryQueue.getNextEntity ou QueryQueue.getNextEntities:** Quando esse método é chamado, se nenhum objeto SessionHandle estiver ligado ao Session, a solicitação da operação será roteada aleatoriamente para partições individuais até um objeto ser obtido. Se um objeto for retornado de uma partição, um objeto SessionHandle correspondente a essa partição será ligado ao Session. Se nenhum objeto for localizado, nenhum SessionHandle será ligado ao Session.
- **Configure um SessionHandle com o método Session.setSessionHandle(SessionHandle sh):** Se SessionHandle for obtido a partir do método Session.getSessionHandle, o SessionHandle poderá ser ligado a um Session. A configuração de um SessionHandle influencia o roteamento de solicitações dentro do escopo do Session ao qual ele está ligado.

O método Session.getSessionHandle sempre retorna um objeto SessionHandle. O método também ligará automaticamente um SessionHandle no Session se nenhum objeto SessionHandle estiver ligado ao Session. Se desejar verificar se um Session tem apenas um objeto SessionHandle, chame o método Session.isSessionHandleSet. Se esse método retornar um valor `false`, nenhum SessionHandle estará ligado atualmente ao Session.

Principais Tipos de Operações no Cenário de Posicionamento por Contêiner

A seguir há um resumo do comportamento de roteamento dos principais tipos de operações no cenário de posicionamento de partição por contêiner em relação aos objetos SessionHandle.

- **Objeto Session com o objeto SessionHandle ligado**
  - Índice - API de MapIndex e MapRangeIndex: SessionHandle
  - Query e ObjectQuery: SessionHandle
  - Agente - API de MapGridAgent e ReduceGridAgent API: SessionHandle
  - ObjectMap.Clear: SessionHandle
  - ObjectMap.getNextKey: SessionHandle
  - QueryQueue.getNextEntity, QueryQueue.getNextEntities: SessionHandle
  - Operações transacionais de criação, recuperação, atualização e exclusão (API de ObjectMap e API de EntityManager): SessionHandle
- **Objeto Session sem o objeto SessionHandle ligado**
  - Índice - API de MapIndex e MapRangeIndex: Todas as partições ativas atuais
  - Query e ObjectQuery: Partição especificada com o método setPartition de Query e ObjectQuery
  - Agente - MapGridAgent e ReduceGridAgent
    - Não suportado: método ReduceGridAgent.reduce(Session s, ObjectMap map, Collection keys) e MapGridAgent.process(Session s, ObjectMap map, Object key).
    - Todas as partições ativas atuais: método ReduceGridAgent.reduce(Session s, ObjectMap map) e MapGridAgent.processAllEntries(Session s, ObjectMap map).
  - ObjectMap.clear: Todas as partições ativas atuais.
  - ObjectMap.getNextKey: Liga um SessionHandle ao Session se uma chave for retornada de uma das partições selecionadas aleatoriamente. Se nenhuma chave for retornada, o Session não será ligado a nenhum SessionHandle.

– QueryQueue: Especifica uma partição com o método QueryQueue.setPartition. Se nenhuma partição for configurada, o método seleciona aleatoriamente uma partição para retornar. Se um objeto for retornado, o Session atual será ligado com o SessionHandle que é ligado à partição que retorna o objeto. Se nenhum objeto for retornado, o Session não será ligado a nenhum SessionHandle.
– Operações transacionais de criação, recuperação, atualização e exclusão (API de ObjectMap e API de EntityManager): Selecione uma partição aleatoriamente.

Na maioria dos casos, use SessionHandle para controlar o roteamento para uma determinada partição. É possível recuperar e armazenar em cache o SessionHandle a partir do Session que insere dados. Depois de armazenar em cache o SessionHandle, é possível configurá-lo em outro Session para que você possa rotear solicitações para a partição especificada pelo SessionHandle em cache. Para executar operações como ObjectMap.clear sem o SessionHandle, é possível configurar temporariamente o SessionHandle como nulo ao chamar Session.setSessionHandle(null). Sem um SessionHandle especificado, as operações são executadas em todas as partições ativas atuais.

- **Comportamento de roteamento de QueryQueue**

  No cenário de posicionamento de partição por contêiner, o SessionHandle pode ser usado para controlar o roteamento dos métodos getNextEntity e getNextEntities da API de QueryQueue. Se o Session estiver ligado a um SessionHandle, as solicitações são roteadas para a partição à qual o SessionHandle está ligado. Se o Session não estiver ligado a um SessionHandle, as solicitações serão roteadas para a partição configurada com o método QueryQueue.setPartition se uma partição tiver sido configurada dessa forma. Se o Session não tiver ligado SessionHandle ou à partição, uma partição selecionada aleatoriamente será retornada. Se nenhuma partição for localizada, o processo será interrompido e nenhum SessionHandle será ligado ao Session atual.

O fragmento de código a seguir mostra como usar os objetos SessionHandle.

```
Session ogSession = objectGrid.getSession();

// binding the SessionHandle
SessionHandle sessionHandle = ogSession.getSessionHandle();

ogSession.begin();
ObjectMap map = ogSession.getMap("planet");
map.insert("planet1", "mercury");

// transaction is routed to partition specified by SessionHandle
ogSession.commit();

// cache the SessionHandle that inserts data
SessionHandle cachedSessionHandle = ogSession.getSessionHandle();

// verify if SessionHandle is set on the Session
boolean isSessionHandleSet = ogSession.isSessionHandleSet();

// temporarily unbind the SessionHandle from the Session
if(isSessionHandleSet) {
    ogSession.setSessionHandle(null);
}

// if the Session has no SessionHandle bound,
// the clear operation will run on all current active partitions
// and thus remove all data from the map in the entire grid
map.clear();
```

```
// after clear is done, reset the SessionHandle back,
// if the Session needs to use previous SessionHandle.
// Optionally, calling getSessionHandle can get a new SessionHandle
ogSession.setSessionHandle(cachedSessionHandle);
```

Considerações de Design do Aplicativo

No cenário de estratégia de posicionamento por contêiner, use o objeto SessionHandle para a maioria das operações. O objeto SessionHandle controla o roteamento para as partições. Para recuperar dados, o objeto SessionHandle que é ligado ao Session deverá ser o mesmo objeto SessionHandle de qualquer transação de inserção de dados.

Quando desejar executar uma operação sem um SessionHandle configurado no Session, é possível desvincular um SessionHandle de um Session ao chamar o método Session.setSessionHandle(null).

Quando um Session for ligado a um SessionHandle, todas as solicitações de operação serão roteadas para a partição especificada pelo objeto SessionHandle. Sem o objeto SessionHandle configurado, as operações serão roteadas para todas as partições ou para uma partição selecionada aleatoriamente.

Objetos de Armazenamento em Cache sem Relacionamentos Envolvidos (API ObjectMap)

Java

Os ObjectMaps são como Mapas Java que permitem que os dados sejam armazenados como pares chave-valor. Os ObjectMaps apresentam uma abordagem simples e intuitiva para o aplicativo que armazenará os dados. Um ObjectMap é ideal para o armazenamento em cache de objetos que não tenham nenhum relacionamento envolvido. Se os relacionamentos de objetos estiverem envolvidos, então você deve usar a API EntityManager.

Para obter informações adicionais sobre a API EntityManager, consulte “Objetos de Armazenamento em Cache e seus Relacionamentos (API EntityManager)” na página 388.

Os aplicativos normalmente obtêm uma referência do WebSphere eXtreme Scale e, então, obtêm um objeto Session da referência para cada encadeamento. As sessões não podem ser compartilhadas entre encadeamentos. O método getMap do Session retorna uma referência a um ObjectMap a ser utilizado para esse encadeamento.

Tarefas relacionadas:

"Introdução ao Desenvolvimento de Aplicativos" na página 254
Para iniciar o desenvolvimento de aplicativos WebSphere eXtreme Scale, você deve configurar seu ambiente de desenvolvimento, aprender sobre APIs que podem ser usadas e, em seguida, desenvolver e testar seu aplicativo.

"Tutorial: Armazenando Informações de Pedido nas Entidades" na página 9
Este tutorial do gerenciador de entidade mostra como utilizar o WebSphere eXtreme Scale para armazenar informações de pedido em um Web site. É possível criar um aplicativo Java Platform, Standard Edition 5 simples que utiliza um eXtreme Scale local e de memória. As entidades utilizam anotações e genéricos do Java SE 5.

Referências relacionadas:

Java "Introdução ao ObjectMap"
A interface ObjectMap é utilizada para interação transacional entre aplicativos e BackingMaps.

Java "ObjectMap e JavaMap" na página 383
Uma instância do JavaMap é obtida de um objeto ObjectMap. A interface JavaMap possui as mesmas assinaturas de método que ObjectMap, mas com manipulação de exceção diferente. O JavaMap estende a interface java.util.Map, portanto, todas as exceções são instâncias da classe java.lang.RuntimeException. Como o JavaMap estende a interface java.util.Map, é fácil utilizar o WebSphere eXtreme Scale rapidamente com um aplicativo existente que utiliza uma interface java.util.Map para armazenamento e cache do objeto.

Java "Mapas como Filas FIFO" na página 384
Com o WebSphere eXtreme Scale, é possível fornecer um recurso semelhante à fila first-in first-out (FIFO) para todos os mapas. O WebSphere eXtreme Scale controla a ordem de inserção para todos os mapas. Um cliente pode solicitar um mapa para a próxima entrada não-bloqueada em um mapa na ordem de inserção e bloqueia a entrada. Este processo permite que vários clientes consumam entradas do mapa de maneira eficiente.

Informações relacionadas:

Documentação da API

"Tutorial de Introdução - Lição 2.1: Criando um Aplicativo de Cliente Java" na página 238
Para inserir, excluir, atualizar e recuperar dados de sua grade de dados, você deverá gravar um aplicativo cliente. A amostra de introdução inclui um aplicativo de cliente Java que pode ser usado para aprender sobre como criar seu próprio aplicativo cliente.

Java Interface ObjectMap

Java Interface BackingMap

Java Interface JavaMap

Introdução ao ObjectMap: Java

A interface ObjectMap é utilizada para interação transacional entre aplicativos e BackingMaps.

Propósito

Uma instância do ObjectMap é obtida do objeto de Sessão que corresponde ao encadeamento atual. A interface ObjectMap é o principal veículo utilizado pelos

aplicativos para fazer alterações em entradas em um BackingMap.

Obtenha uma Instância do ObjectMap

Um aplicativo obtém uma instância do ObjectMap a partir de um objeto Session utilizando método Session.getMap(String). O trecho de código a seguir demonstra como obter uma instância de ObjectMap:

```
ObjectGrid objectGrid = ...;
BackingMap backingMap = objectGrid.defineMap("mapA");
Session sess = objectGrid.getSession();
ObjectMap objectMap = sess.getMap("mapA");
```

Cada instância de ObjectMap corresponde a um objeto de Sessão específico. Chamar o método getMap várias vezes em um objeto Session particular com o mesmo nome de BackingMap sempre retorna a mesma instância do ObjectMap.

Executar Commit de Transações Automaticamente

As operações junto a BackingMaps que utilizam ObjectMaps e JavaMaps são executadas de maneira mais eficiente em uma transação Session. O WebSphere eXtreme Scale fornece suporte a autocommit quando métodos nas interfaces ObjectMap e JavaMap são chamados fora de uma transação Session. Os métodos iniciam uma transação implícita, desempenham a operação solicitada e confirmam a transação implícita.

Semântica do Método

A seguir, está uma explicação da semântica por trás de cada método nas interfaces ObjectMap e JavaMap.

Método containsKey
O método containsKey determina se uma chave possui um valor no BackingMap ou Utilitário de Carga. Se valores nulos forem suportados por um aplicativo, este método poderá ser utilizado para determinar se uma referência nula retornada de uma operação get refere-se a um valor nulo ou indica que o BackingMap e o Utilitário de Carga não contêm a chave.

Método flush
A semântica do método flush é semelhante ao método flush na interface Session. A diferença notável é que a limpeza de Sessão aplica as alterações pendentes atuais para todos os mapas que foram modificados na sessão atual. Com este método, o flush ocorre apenas nas alterações nesta instância do ObjectMap para o utilitário de carga.

Método get
O método get busca a entrada a partir da instância do BackingMap. Se a entrada não for localizada na instância do BackingMap mas um Utilitário de Carga estiver associado com a instância do BackingMap, a instância do BackingMap tenta buscar a entrada a partir do Utilitário de Carga. O método getAll é fornecido para permitir o processamento de busca em lote.

Método getForUpdate
O método getForUpdate é o mesmo que o método get, mas utilizar o método getForUpdate informa ao BackingMap e ao Utilitário de Carga que a intenção é atualizar a entrada. Um Utilitário de Carga pode utilizar esta sugestão para emitir uma consulta SELECT for UPDATE para um backend de banco de dados. Se uma estratégia de bloqueio pessimistic for definida

para o BackingMap, o gerenciador de bloqueios bloqueia a entrada. O método getAllForUpdate é fornecido para permitir o processamento de busca em lote.

Método insert

O método insert insere uma entrada no BackingMap e no Utilitário de Carga. Utilize este método informa ao BackingMap e ao Utilitário de Carga que você deseja inserir uma entrada que não existia anteriormente. Quando você chama este método em uma entrada existente, ocorre uma exceção quando o método é chamado ou quando a transação atual é confirmada.

Método invalidate

A semântica do método invalidate depende do valor do parâmetro **isGlobal** que é passado para o método. O método invalidateAll é fornecido para permitir o processamento de invalidação em lote.

A invalidação local é especificada quando o valor false é passado como o parâmetro **isGlobal** do método invalidate. A invalidação local descarta as alterações na entrada no cache de transação. Se o aplicativo emitir um método get, a entrada será buscada no último valor confirmado no BackingMap. Se nenhuma entrada estiver presente no BackingMap, a entrada será buscada no último valor limpo ou confirmado no Utilitário de Carga. Quando uma transação é confirmada, todas as entradas que estão marcadas como estando invalidadas localmente não têm nenhum impacto no BackingMap. As alterações que foram limpas no Utilitário de Carga ainda serão confirmadas, mesmo que a entrada tenha sido invalidada.

A invalidação global é especificada quando true é passado como o parâmetro **isGlobal** do método invalidate. A invalidação global descarta as alterações pendentes na entrada no cache de transação e ignora o valor de BackingMap nas operações seguintes que são executadas na entrada. Quando ocorre um commit de uma transação, as entradas que estão marcadas como invalidadas globalmente são despejadas do BackingMap. Considere o seguinte caso de uso para invalidação como um exemplo: O BackingMap é suportado por uma tabela de banco de dados que tem uma coluna de auto-incremento. As colunas de incremento são úteis para designar números exclusivos a registros. O aplicativo insere uma entrada. Após a inserção, o aplicativo precisa saber o número de sequência para a linha inserida. Ele sabe que sua cópia do objeto é antiga, por isso, utiliza a invalidação global para obter o valor do Utilitário de Carga. O código a seguir demonstra este caso de uso:

```
Session sess = objectGrid.getSession();
ObjectMap map = sess.getMap("mymap");
sess.begin();
map.insert("Billy", new Person("Joe", "Bloggs", "Manhattan"));
sess.flush();
map.invalidate("Billy", true);
Person p = map.get("Billy");
System.out.println("Version column is: " + p.getVersion());
map.commit();
// Close the session (optional in Version 7.1.1 and later) for improved performance
session.close();
```

Esta amostra de código inclui uma entrada para `Billy`. O atributo version de Person é configurado utilizando uma coluna de auto-incremento no banco de dados. Primeiro, o aplicativo executa um comando insert. Em seguida, ele emite um flush, que faz a inserção ser enviada para o Utilitário de Carga e o banco de dados. O banco de dados configura a

coluna de versão para o próximo número na sequência, que desatualiza o objeto Person na transação. Para atualizar o objeto, o aplicativo é globalmente invalidado. O próximo método get que é emitido obtém a entrada do Utilitário de Carga, ignorando o valor da transação. A entrada é buscada no banco de dados com o valor de versão atualizado.

Método put

A semântica do método put é independente de um método get anterior ter sido chamado na transação para a chave. Se o aplicativo emite uma operação get que retorna uma entrada que existe no BackingMap ou no carregador, a chamada do método put é interpretada como uma atualização e retorna o valor anterior na transação. Se uma chamada do método put foi executada sem uma chama do método get anterior ou uma chamada do método get anterior não localizou uma entrada, a operação é interpretada como uma inserção. A semântica dos métodos insert e update é aplicável quando ocorre o commit da operação put. O método putAll é fornecido para ativar inserção em lote e processamento de atualizações.

Nota:  8.6+ O método setPutMode(PutMode.UPSERT) é incluído para alterar o comportamento padrão dos métodos ObjectMap e JavaMap put() e putAll() para se comportarem como os métodos ObjectMap.upsert() e upsertAll().

O método PutMode.UPSERT substitui o método setPutMode(PutMode.INSERTUPDATE). Use o método PutMode.UPSERT para indicar ao BackingMap e ao carregador que uma entrada na grade de dados precisa colocar a chave e o valor na grade. O BackingMap e carregador executam uma inserção ou uma atualização para colocar o valor na grade e no carregador. Se você executar a API upsert dentro de seus aplicativos, o carregador obterá um tipo UPSERT de LogElement, que permite que carregadores façam a mesclagem do banco de dados ou chamadas upsert em vez de usar insert ou update.

8.6+ método upsert

Use o método upsert para informar ao BackingMap e carregador que uma entrada na grade de dados precisa colocar a chave e o valor na grade. O BackingMap e carregador executam uma inserção ou uma atualização para colocar o valor na grade e no carregador. Se você executar a API upsert dentro de seus aplicativos, o carregador obterá um tipo UPSERT de LogElement, que permite que carregadores façam a mesclagem do banco de dados ou chamadas upsert em vez de usar insert ou update.

Nota: Antes de o método upsert, você usava os métodos put ou getForUpdate para, em seu código do aplicativo, inserir ou atualizar dados; por exemplo:

```
session.begin();
map.getForUpdate();
map.put();
session.commit();
```

Com o método upsert, é possível utilizar as seguintes linhas de código para inserir ou atualizar dados:

```
session.begin();
map.upsert();
session.commit();
```

8.6+ Método lock

Ao usar o bloqueio pessimista, é possível usar o método de bloqueio para bloquear dados, ou chaves, sem retornar nenhum valor dos dados. Com o método de bloqueio, é possível bloquear a chave na grade ou bloquear a chave e determinar se o valor existe na grade. Em liberações anteriores, você usava as APIs get e getForUpdate para bloquear chaves na grade de dados. No entanto, se você não precisou de dados do cliente, o desempenho é degradado pela recuperação em potencial de objetos de valores grandes no cliente. Além disso, containsKey não contém atualmente nenhum bloqueio, portanto, você foi forçado a usar get e getForUpdate para obter bloqueios apropriados ao usar bloqueio pessimista. A API de bloqueio agora fornece a você uma semântica containsKey enquanto mantém o bloqueio. Verifique os seguintes exemplos:

- `boolean ObjectMap.lock(Object key, LockMode lockMode);`

  Bloqueia a chave no mapa, retornando true se a chave existir e retornando false se a chave não existir.

- `List<Boolean> ObjectMap.lockAll(List keys, LockMode lockMode);`

  Bloqueia uma lista de chaves no mapa, retornando uma lista de valores true ou false; retornando `true` se a chave existir e retornando `false` se a chave não existir.

LockMode é uma enumeração com possíveis valores SHARED, UPGRADABLE e EXCLUSIVE, nos quais é possível especificar as chaves que você deseja bloquear. Consulte a tabela a seguir para entender o relacionamento entre estes valores do modo de bloqueio e o comportamento de métodos existentes:

Tabela 9. Valores de LockMode e Equivalentes do Método Existente

Modo de bloqueio	Equivalente do Método
SHARED	get()
UPGRADABLE	getForUpdate()
EXCLUSIVE	getNextKey() e commit()

Consulte o código de exemplo a seguir do parâmetro LockMode:

```
session.begin();
map.lock(key, LockMode.UPGRADABLE);
map.upsert();
session.commit()
```

Método remove

O método remove remove a entrada do BackingMap e do Utilitário de Carga, se um Utilitário de Carga estiver conectado. O valor do objeto que foi removido é retornado por este método. Se o objeto não existir, este método retornará um valor nulo. O método removeAll é fornecido para ativar o processamento de exclusão em lote sem os valores de retorno.

Método setCopyMode

O método setCopyMode especifica um valor CopyMode para este ObjectMap. Com este método, um aplicativo pode substituir o valor CopyMode que é especificado no BackingMap. O valor CopyMode especificado fica em efeito até que o método clearCopyMode seja chamado. Os dois métodos são chamados fora dos limites transacionais. Um valor CopyMode não pode ser alterado no meio de uma transação.

Método touch

O método touch atualiza o horário do último acesso para uma entrada.

Este método não recupera o valor do BackingMap. Utilize este método em sua própria transação. Se a chave fornecida não existir no BackingMap devido a uma invalidação ou remoção, ocorrerá uma exceção durante o processamento de confirmação.

Método update

O método update atualiza explicitamente uma entrada no BackingMap e no Utilitário de Carga. A utilização deste método indica ao BackingMap e ao Utilitário de Carga que você deseja atualizar uma entrada existente. Ocorrerá uma exceção se você chamar este método em uma entrada que não existe quando o método for chamado ou durante o processamento de confirmação.

Método getIndex

O método getIndex tenta obter um índice denominado que é baseado no BackingMap. O índice não pode ser compartilhado entre encadeamentos e funciona de acordo com as mesmas regras que um objeto Session. O objeto index retornado deve ser convertido para a interface de índice do aplicativo tal como a interface MapIndex, a interface MapRangeIndex ou uma interface de índice customizada.

Método clear

O método clear remove todas as entradas de cache de um mapa de todas as partições. Esta operação é uma função auto-commit, assim, nenhuma transação ativa deverá estar presente ao chamar o método clear.

Nota: O método clear limpa apenas o mapa no qual é chamado, deixando quaisquer mapas de entidade relacionados não-afetados. Este método não chama o plug-in do Utilitário de Carga.

Conceitos relacionados:

Java "Objetos de Armazenamento em Cache sem Relacionamentos Envolvidos (API ObjectMap)" na página 372
Os ObjectMaps são como Mapas Java que permitem que os dados sejam armazenados como pares chave-valor. Os ObjectMaps apresentam uma abordagem simples e intuitiva para o aplicativo que armazenará os dados. Um ObjectMap é ideal para o armazenamento em cache de objetos que não tenham nenhum relacionamento envolvido. Se os relacionamentos de objetos estiverem envolvidos, então você deve usar a API EntityManager.

Java "Mapas Dinâmicos"
Com mapas dinâmicos, é possível criar mapas depois que grade de dados já tiver sido inicializada.

Informações relacionadas:

Java Interface ObjectMap

Java Interface BackingMap

Java Interface JavaMap

Mapas Dinâmicos: Java

Com mapas dinâmicos, é possível criar mapas depois que grade de dados já tiver sido inicializada.

Nas versões anteriores, o WebSphere eXtreme Scale precisava que você definisse mapas antes de inicializar o ObjectGrid. Como resultado, você precisava criar todos os mapas a serem usados antes de executar transações em relação a qualquer um dos mapas.

Vantagens dos mapas dinâmicos

A introdução de mapas dinâmicos reduz a necessidade de definir todos os mapas antes da inicialização. Por meio do uso de mapas modelos, os mapas podem agora ser criados após o ObjectGrid ter sido inicializado.

Mapas modelos são definidos no arquivo XML do ObjectGrid. As comparações de modelo são executadas quando uma Sessão requer um mapa que não foi previamente definido. Se o nome do novo mapa corresponder à expressão regular de um mapa modelo, o mapa é criado dinamicamente e recebe o nome do mapa solicitado. Este mapa recentemente criado herda todas as configurações do mapa modelo como definido pelo arquivo XML ObjectGrid.

Criando Mapas Dinâmicos

A criação de mapa dinâmico está ligada ao método Session.getMap(String). Chamadas para este mapa retornam um ObjectMap baseado no BackingMap que foi configurado pelo arquivo XML ObjectGrid.

Passar uma Sequência que corresponde à expressão regular de um mapa modelo resulta na criação de um ObjectMap e em um BackingMap associado.

Consulte a documentação da API para obter mais informações sobre o método Session.getMap(String cacheName).

Definir uma mapa modelo em XML é tão simples quanto configurar um atributo booleano modelo no elemento backingMap. Quando o modelo é configurado para true, o nome do backingMap é interpretado como uma expressão regular.

O WebSphere eXtreme Scale usa a correspondência padrão de expressão regular Java. Para obter mais informações sobre o mecanismo de expressão regular em Java, consulte a documentação da API para o pacote e as classes java.util.regex.

Nota: Quando estiver definindo mapas de modelo, verifique se os nomes dos mapas são exclusivos o suficiente para que o aplicativo possa corresponder a apenas um dos mapas de modelo com o método Session.getMap(String mapName). Se o método getMap() corresponder a mais de um padrão de mapa de modelo, uma exceção `IllegalArgumentException` resultará.

Um arquivo XML do ObjectGrid XML de amostra com um mapa modelo definido está a seguir.

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">
 <objectGrids>
  <objectGrid name="accounting">
   <backingMap name="payroll" readOnly="false" />
   <backingMap name="templateMap.*" template="true"
    pluginCollectionRef="templatePlugins" lockStrategy="PESSIMISTIC" />
  </objectGrid>
 </objectGrids>
```

```
 <backingMapPluginCollections>
  <backingMapPluginCollection id="templatePlugins">
   <bean id="Evictor"
    className="com.ibm.websphere.objectgrid.plugins.builtins.LFUEvictor" />
  </backingMapPluginCollection>
 </backingMapPluginCollections>
</objectGridConfig>
```

O arquivo XML anterior define um mapa modelo em uma mapa não-modelo. O nome do mapa modelo é uma expressão regular: `templateMap.*`. Quando o método Session.getMap(String) é chamado com um nome de mapa correspondente a esta expressão regular, o aplicativo cria um mapa.

Exemplo

A configuração de um mapa modelo é necessária para criar um mapa dinâmico. Inclua um booleano modelo em um backingMap no arquivo XML do ObjectGrid.

```
<backingMap name="templateMap.*" template="true" />
```

O nome do mapa modelo é tratado como uma expressão regular.

Chamar o método Session.getMap(String cacheName) com um cacheName que seja uma correspondência para a expressão regular resulta na criação do mapa dinâmico. Um objeto ObjectMap é retornado a partir desta chamada de método e um objeto BackingMap associado é criado.

```
Session session = og.getSession();
ObjectMap map = session.getMap("templateMap1");
```

O mapa criado mais recentemente é configurado com todos os atributos e plug-ins que foram definidos na definição do mapa modelo. Considere novamente o arquivo XML do ObjectGrid anterior.

Um mapa dinâmico criado com base no mapa modelo neste arquivo XML teria um evictor configurado e sua estratégia de bloqueio seria pessimista.

Nota: Um modelo não é um BackingMap real. Isto é, o ObjectGrid "contabilidade" não contém um mapa "templateMap.*" real. O modelo é usado apenas como uma base para a criação de mapa dinâmico. Entretanto, você deve incluir o mapa dinâmico no elemento mapRef no arquivo XML da política de implementação nomeado exatamente como no XML do ObjectGrid. Este elemento identifica quais mapas dinâmicos são definidos e em quais mapSet.

Considere a mudança no comportamento do método Session.getMap(String cacheName) ao usar mapas modelos. Antes do WebSphere eXtreme Scale Versão 7.0, todas as chamadas ao método Session.getMap(String cacheName) resultavam em uma exceção UndefinedMapException se o mapa solicitado não existisse. Com mapas dinâmicos, cada nome que corresponde à expressão regular para um mapa modelo resulta na criação do mapa. Certifique-se de anotar o número de mapas que o seu aplicativo cria, particularmente se a sua expressão regular for genérica.

Também, ObjectGridPermission.DYNAMIC_MAP é necessário para a criação de mapa dinâmico quando a segurança doeXtreme Scale está ativada. Esta permissão é verificada quando o método Session.getMap(String) é chamado. Para obter mais informações, consulte o "Autorizando Aplicativos Clientes" na página 774.

Exemplos Adicionais

objectGrid.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
    xmlns="http://ibm.com/ws/objectgrid/config">
<objectGrids>
 <objectGrid name="session">
    <backingMap name="objectgrid.session.metadata.dynamicmap.*" template="true"
        lockStrategy="PESSIMISTIC" ttlEvictorType="LAST_ACCESS_TIME">
    <backingMap name="objectgrid.session.attribute.dynamicmap.*"
        template="true" lockStrategy="OPTIMISTIC"/>
    <backingMap name="datagrid.session.global.ids.dynamicmap.*"
        lockStrategy="PESSIMISTIC"/>
 </objectGrid>
</objectGrids>
</objectGridConfig>
```

objectGridDeployment.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<deploymentPolicy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://ibm.com/ws/objectgrid/deploymentPolicy
   ../deploymentPolicy.xsd"
  xmlns="http://ibm.com/ws/objectgrid/deploymentPolicy">
  <objectgridDeployment objectgridName="session">
    <mapSet name="mapSet2" numberOfPartitions="5" minSyncReplicas="0"

maxSyncReplicas="1" >"0" maxAsyncReplicas="1" developmentMode="false"
      placementStrategy="PER_CONTAINER">
     <map ref="logical.name"/>
     <map ref="objectgrid.session.metadata.dynamicmap.*"/>
     <map ref="objectgrid.session.attribute.dynamicmap.*"/>
     <map ref="datagrid.session.global.ids"/>
    </mapSet>
  </objectgridDeployment>

</deploymentPolicy>
```

Limitações e Considerações

Limitações:

- O elemento QuerySchema não suporta o modelo para mapName.
- Não é possível usar entidades com mapas dinâmicos.
- Um BackingMap de entidade é implicitamente definido, mapeado para a entidade através do nome da classe.

Considerações:

- Muitos plug-ins não têm como determinar o mapa com o qual cada plug-in está associado.
- Outros plug-ins se diferenciam usando um nome de mapa ou nome de BackingMap como um argumento.
- Quando estiver definindo mapas de modelo, verifique se os nomes dos mapas são exclusivos o suficiente para que o aplicativo possa corresponder a apenas um dos mapas de modelo usando o método Session.getMap(String mapName). Se o método getMap() corresponder a mais de um padrão de mapa de modelo, uma exceção `IllegalArgumentException` resultará.

Referências relacionadas:

Java "Introdução ao ObjectMap" na página 373
A interface ObjectMap é utilizada para interação transacional entre aplicativos e BackingMaps.

Java "ObjectMap e JavaMap" na página 383
Uma instância do JavaMap é obtida de um objeto ObjectMap. A interface JavaMap possui as mesmas assinaturas de método que ObjectMap, mas com manipulação de exceção diferente. O JavaMap estende a interface java.util.Map, portanto, todas as exceções são instâncias da classe java.lang.RuntimeException. Como o JavaMap estende a interface java.util.Map, é fácil utilizar o WebSphere eXtreme Scale rapidamente com um aplicativo existente que utiliza uma interface java.util.Map para armazenamento e cache do objeto.

Java "Mapas como Filas FIFO" na página 384
Com o WebSphere eXtreme Scale, é possível fornecer um recurso semelhante à fila first-in first-out (FIFO) para todos os mapas. O WebSphere eXtreme Scale controla a ordem de inserção para todos os mapas. Um cliente pode solicitar um mapa para a próxima entrada não-bloqueada em um mapa na ordem de inserção e bloqueia a entrada. Este processo permite que vários clientes consumam entradas do mapa de maneira eficiente.

Informações relacionadas:

Java Interface ObjectMap

Java Interface BackingMap

Java Interface JavaMap

Opções de Configuração de Mapa Dinâmico:

É possível criar mapas adicionais em uma grade de dados permitindo que seu aplicativo cliente se conecte ao mapa especialmente nomeado. Quando essa conexão ocorre, o mapa é criado automaticamente.

Nomenclatura de Mapa Dinâmico

Quando você cria uma grade de dados, um único mapa é criado por padrão. Esse mapa é nomeado igual à sua grade de dados. Por exemplo, se você criar a grade de dados `myGrid`, obterá automaticamente um mapa `myGrid`. Entretanto, também é possível incluir mapas na grade de dados. Um mapa é criado automaticamente quando o aplicativo cliente se conecta a um mapa usando a convenção de nomenclatura a seguir:

```
<nome_do_mapa>.<modelo>.<opção_de_bloqueio>
```

onde:

nome_do_mapa **(obrigatório)**
Especifica o nome do mapa.

modelo **(obrigatório)**
Especifica o modelo que define quando as entradas expiram do mapa, definindo o comportamento de tempo de vida (TTL). Consulte "Modelos de Mapa" na página 383 para obter uma lista das opções disponíveis.

opção_de_bloqueio
Especifique o mecanismo de bloqueio que é usado para o mapa. Consulte "Opções de Bloqueio" na página 383 para obter uma lista das opções disponíveis.

Você deve incluir um nome de modelo para o mapa. Se você não especificar uma opção de bloqueio, nenhum bloqueio ocorrerá no mapa.

Modelos de Mapa

Tabela 10. Modelos de Mapa Dinâmico

Modelo de Mapa	Descrição
*.NONE	Especifica um mapa sem nenhuma expiração de tempo de vida (TTL).
*.LUT	Especifica um mapa no qual as entradas são expiradas com base na última duração da atualização da entrada. O TTL padrão é uma hora.
*.LAT	Um mapa no qual as entradas são expiradas com base no último tempo de acesso da entrada. O TTL padrão é uma hora.
*.CT	Um mapa no qual as entradas são expiradas com base no horário de criação da entrada mais o valor de TTL. O TTL padrão é uma hora.

Opções de Bloqueio

Tabela 11. Opções de Bloqueio de Mapa Dinâmico

Opção de Bloqueio	Descrição
(em branco)	Se você não indicar uma opção de bloqueio, nenhum mecanismo de bloqueio será usado.
.P	Especifica que o mapa tem bloqueio pessimista
.O	Especifica que o mapa tem bloqueio otimista

ObjectMap e JavaMap: Java

Uma instância do JavaMap é obtida de um objeto ObjectMap. A interface JavaMap possui as mesmas assinaturas de método que ObjectMap, mas com manipulação de exceção diferente. O JavaMap estende a interface java.util.Map, portanto, todas as exceções são instâncias da classe java.lang.RuntimeException. Como o JavaMap estende a interface java.util.Map, é fácil utilizar o WebSphere eXtreme Scale rapidamente com um aplicativo existente que utiliza uma interface java.util.Map para armazenamento e cache do objeto.

Obter uma Instância do JavaMap

Um aplicativo obtém uma instância do JavaMap a partir de um objeto ObjectMap utilizando o método ObjectMap.getJavaMap. O trecho de código a seguir demonstra como obter uma instância JavaMap.

```
ObjectGrid objectGrid = ...;
BackingMap backingMap = objectGrid.defineMap("mapA");
Session sess = objectGrid.getSession();
ObjectMap objectMap = sess.getMap("mapA");
java.util.Map map = objectMap.getJavaMap();
JavaMap javaMap = (JavaMap) javaMap;
```

Um JavaMap é suportado pelo ObjectMap a partir do qual ele foi obtido. Chamar o método getJavaMap várias vezes utilizando um ObjectMap particular sempre retorna a mesma instância do JavaMap.

Métodos

A interface JavaMap suporta apenas um subconjunto dos métodos na interface java.util.Map. A interface java.util.Map suporta os seguintes métodos:

Método containsKey(java.lang.Object)

Método get(java.lang.Object)

Método put(java.lang.Object, java.lang.Object)

Método putAll(java.util.Map)

Método remove(java.lang.Object)

clear()

Todos os métodos herdados da interface java.util.Map resultam em uma exceção java.lang.UnsupportedOperationException.

Conceitos relacionados:

Java "Objetos de Armazenamento em Cache sem Relacionamentos Envolvidos (API ObjectMap)" na página 372
Os ObjectMaps são como Mapas Java que permitem que os dados sejam armazenados como pares chave-valor. Os ObjectMaps apresentam uma abordagem simples e intuitiva para o aplicativo que armazenará os dados. Um ObjectMap é ideal para o armazenamento em cache de objetos que não tenham nenhum relacionamento envolvido. Se os relacionamentos de objetos estiverem envolvidos, então você deve usar a API EntityManager.

Java "Mapas Dinâmicos" na página 378
Com mapas dinâmicos, é possível criar mapas depois que grade de dados já tiver sido inicializada.

Informações relacionadas:

Java Interface ObjectMap

Java Interface BackingMap

Java Interface JavaMap

Mapas como Filas FIFO: Java

Com o WebSphere eXtreme Scale, é possível fornecer um recurso semelhante à fila first-in first-out (FIFO) para todos os mapas. O WebSphere eXtreme Scale controla a ordem de inserção para todos os mapas. Um cliente pode solicitar um mapa para a próxima entrada não-bloqueada em um mapa na ordem de inserção e bloqueia a entrada. Este processo permite que vários clientes consumam entradas do mapa de maneira eficiente.

Exemplo de FIFO

O trecho de código a seguir mostra um cliente entrando em um loop para processar entradas do mapa até que o mapa seja esvaziado. O loop inicia uma transação e, então, chama o método ObjectMap.getNextKey(5000). Este método

retorna a chave da próxima entrada desbloqueada disponível e a bloqueia. Se a transação é bloqueada por mais de 5000 milissegundos, então, o método retorna null.

```
Session session = ...;
ObjectMap map = session.getMap("xxx");
// this needs to be set somewhere to stop this loop
boolean timeToStop = false;

while(!timeToStop)
{
  session.begin();
  Object msgKey = map.getNextKey(5000);
  if(msgKey == null)
  {
    // current partition is exhausted, call it again in
    // a new transaction to move to next partition
    session.rollback();
    continue;
  }
  Message m = (Message)map.get(msgKey);
  // now consume the message
  ...
  // need to remove it
  map.remove(msgKey);
  session.commit();
}
```

Modo Local versus Modo do Cliente

Se o aplicativo estiver utilizando um núcleo local, ou seja, se ele não for um cliente, então o mecanismo funcionará conforme descrito anteriormente.

Para o modo cliente, se a Java virtual machine (JVM) for um cliente, então, o cliente inicialmente se conecta ao primário de partição aleatório. Se não existir nenhum trabalho em tal partição, então, o cliente move para a próxima partição para procurar trabalho. O cliente localiza uma partição com entrada ou executa um loop pela partição aleatória inicial. Se o cliente executa um loop pela partição inicial, então, ele retorna um valor nulo para o aplicativo. Se o cliente localiza uma partição com um mapa que possui entradas, então ele consome entradas até que nenhuma esteja disponível para o período de tempo limite. Após o tempo limite passar, então, um nulo é retornado. Esta ação significa que quando um nulo é retornado e um mapa particionado é utilizado, então, ele deve iniciar uma nova transação e retomar o atendimento. O fragmento de amostra do código anterior possui este comportamento.

Exemplo

Quando você está executando com um cliente é uma chave é retornada, tal transação é vinculada à partição com a entrada para tal chave. Se não desejar atualizar nenhum outro mapa durante tal transação, então, não há um problema. Se você não desejar atualizar, então, será possívelapenas atualizar os mapas a partir da mesma partição que o mapa, a partir da qual obteve a chave. A entrada que é retornada do método getNextKey precisa fornecer ao aplicativo uma maneira de descobrir dados relevantes nesta partição. Como exemplo, se você possui dois mapas; um para eventos e um outro para tarefas que os eventos impactam. Você define os dois mapas com as seguintes entidades:

Job.java

```
package tutorial.fifo;

import com.ibm.websphere.projector.annotations.Entity;
```

```
import com.ibm.websphere.projector.annotations.Id;

@Entity
public class Job
{
 @Id String jobId;

 int jobState;
}
```

JobEvent.java

```
package tutorial.fifo;

import com.ibm.websphere.projector.annotations.Entity;
import com.ibm.websphere.projector.annotations.Id;
import com.ibm.websphere.projector.annotations.OneToOne;

@Entity
public class JobEvent
{
 @Id String eventId;
 @OneToOne Job job;
}
```

A tarefa possui um ID, que é uma cadeia, e um estado, que é um número inteiro. Suponha que você deseja incrementar o estado sempre que chega um evento. Os eventos são armazenados no Mapa de JobEvent. Cada entrada possui uma referência para a tarefa que o evento tem interesse. O código para o listener fazer isto é semelhante ao exemplo a seguir:

JobEventListener.java

```
package tutorial.fifo;

import com.ibm.websphere.objectgrid.ObjectGridException;
import com.ibm.websphere.objectgrid.ObjectMap;
import com.ibm.websphere.objectgrid.Session;
import com.ibm.websphere.objectgrid.em.EntityManager;

public class JobEventListener
{
 boolean stopListening;

 public synchronized void stopListening()
 {
  stopListening = true;
 }

 synchronized boolean isStopped()
 {
  return stopListening;
 }

 public void processJobEvents(Session session)
  throws ObjectGridException {
  EntityManager em = session.getEntityManager();
  ObjectMap jobEvents = session.getMap("JobEvent");
  while(!isStopped())
  {
   em.getTransaction().begin();

   Object jobEventKey = jobEvents.getNextKey(5000);
   if(jobEventKey == null)
   {
    em.getTransaction().rollback();
    continue;
   }
   JobEvent event = (JobEvent)em.find(JobEvent.class, jobEventKey);
```

```
   // process the event, here we just increment the
   // job state
   event.job.jobState++;
   em.getTransaction().commit();
  }
 }
}
```

Um listener é iniciado em um encadeamento pelo aplicativo. O listener é executado até que o método stopListening seja chamado. O método processJobEvents é executado no encadeamento até que o método stopListening seja chamado. O loop bloqueia a espera por um eventKey a partir do Mapa JobEvent e, em seguida, utiliza o EntityManager para acessar o objeto de evento, aponta para a tarefa e incrementa o estado.

A API do EntityManager não possui um método getNextKey, mas o ObjectMap possui. Portanto, o código utiliza o ObjectMap para JobEvent para obter a chave. Se um mapa é utilizado com entidades, então ele não mais armazena objetos. Em vez disso, ele armazena Tuplas; um objeto Tupla para a chave e um objeto Tupla para o valor. O método EntityManager.find aceita uma Tupla para a chave.

O código para criar um evento é semelhante ao exemplo a seguir:

```
em.getTransaction().begin();
Job job = em.find(Job.class, "Job Key");
JobEvent event = new JobEvent();
event.id = Random.toString();
event.job = job;
em.persist(event); // insert it
em.getTransaction().commit();
```

Você localiza a tarefa para o evento, constrói um evento, aponta o evento para a tarefa, insere o evento no Mapa de JobEvent e consolida a transação.

Utilitários de Carga e Mapas FIFO

Se você desejar apoiar um mapa que é utilizado como uma fila FIFO com um Utilitário de Carga, então, pode ser necessário executar algum trabalho adicional. Se a ordem das entradas no mapa não for uma preocupação, não há trabalho extra. Se a ordem for importante, então, é necessário incluir um número de sequência em todos os registros inseridos quando você está persistindo os registros para o backend. O mecanismo de pré-carregamento deve ser escrito para inserir os registros na inicialização utilizando esta ordem.

Conceitos relacionados:

Java "Objetos de Armazenamento em Cache sem Relacionamentos Envolvidos (API ObjectMap)" na página 372
Os ObjectMaps são como Mapas Java que permitem que os dados sejam armazenados como pares chave-valor. Os ObjectMaps apresentam uma abordagem simples e intuitiva para o aplicativo que armazenará os dados. Um ObjectMap é ideal para o armazenamento em cache de objetos que não tenham nenhum relacionamento envolvido. Se os relacionamentos de objetos estiverem envolvidos, então você deve usar a API EntityManager.

Java "Mapas Dinâmicos" na página 378
Com mapas dinâmicos, é possível criar mapas depois que grade de dados já tiver sido inicializada.

Informações relacionadas:

Java Interface ObjectMap

Java Interface BackingMap

Java Interface JavaMap

Objetos de Armazenamento em Cache e seus Relacionamentos (API EntityManager)

Java

A maioria dos produtos de cache utiliza APIs baseadas em mapa para armazenar dados como pares de chave-valor. A API ObjectMap e o cache dinâmico no WebSphere Application Server, entre outros, usam essa abordagem. Entretanto, APIs baseadas em mapas têm limitações. A API EntityManager simplifica a interação com a grade de dados ao fornecer uma maneira fácil de declarar e interagir com um gráfico complexo de objetos relacionados.

Limitações de API Baseada em Mapa

Se estiver usando uma API baseada em mapa, como o cache dinâmico no WebSphere Application Server ou a API ObjectMap, leve em consideração as seguintes limitações:

- Os índices e consultas devem usar a reflexão para consultar campos e propriedades nos objetos em cache.
- A serialização de dados customizados é necessária para atingir o desempenho para objetos complexos.
- É difícil trabalhar com gráficos de objetos. Você deve desenvolver o aplicativo para armazenar referências artificiais entre objetos e uni-los manualmente.

Benefícios da API EntityManager

A API EntityManager usa a infraestrutura baseada em mapa existente, porém converte os objetos de entidade em, e a partir de, tuplas antes de serem armazenados ou lidos a partir do mapa. Um objeto de entidade é transformado em uma tupla de chave e uma tupla de valor, que são então armazenadas como pares chave-valor. Uma tupla é uma matriz de atributos primitivos.

Este conjunto de APIs segue o estilo de programação Plain Old Java Object (POJO) que é adotado pela maioria das estruturas.

Tarefas relacionadas:

Java "Tutorial: Armazenando Informações de Pedido nas Entidades" na página 9
Este tutorial do gerenciador de entidade mostra como utilizar o WebSphere eXtreme Scale para armazenar informações de pedido em um Web site. É possível criar um aplicativo Java Platform, Standard Edition 5 simples que utiliza um eXtreme Scale local e de memória. As entidades utilizam anotações e genéricos do Java SE 5.

"Colocando Diversos Objetos de Cache na Mesma Partição" na página 429
Ao definir dados relacionados em conjuntos de mapas que são organizados na mesma partição, você pode evitar a duplicação de dados e permitir o acesso a dados de baixa granularidade.

Referências relacionadas:

Java "Agente de Instrumentação de Desempenho da Entidade" na página 762
É possível melhorar o desempenho de entidades de acesso ao campo ativando o agente de instrumentação do WebSphere eXtreme Scale ao usar o Java Development Kit (JDK) Versão 6 ou posterior.

Java "Definindo um Esquema de Entidade" na página 391
Um ObjectGrid pode ter inúmeros esquemas de entidade lógicos. As entidades são definidas usando as classes Java anotadas, o XML ou uma combinação de classes XML e Java. Entidades definidas são registradas com um servidor eXtreme Scale e ligadas a BackingMaps, índices e outros plug-ins.

Java "Listeners de Entidade e Métodos de Retorno de Chamada" na página 408
Os aplicativos podem ser notificados quando o estado de uma entidade é alterado de estado para estado. Dois mecanismos de retorno de chamada existem para os eventos de mudança de estado: os métodos de retorno de chamada do ciclo de vida que são definidos em uma classe de entidade e são chamados sempre que o estado da entidade é alterado e os listeners de entidade, que são mais gerais porque o listener da entidade pode ser registrado em várias entidades.

Java "Exemplos do Listener de Entidade" na página 414
É possível gravar EntityListeners com base em seus requisitos. Veja a seguir vários scripts de exemplo.

Java "Interface EntityTransaction" na página 426
É possível utilizar a interface EntityTransaction para demarcar transações.

Informações relacionadas:

Java Amostra: Executando as Consultas em Paralelo Usando um ReduceGridAgent

Gerenciamento de Relacionamentos: Java

Linguagens orientadas a objetos como Java, e relacionamentos ou associações de suporte a bancos de dados relacionais. Os relacionamentos diminuem a quantidade de armazenamento através do uso de referências de objetos ou chaves estrangeiras.

Ao usar relacionamentos em uma grade de dados, os dados deverão ser organizados em uma árvore limitada. Um tipo de raiz deve existir na árvore e todos os filhos devem estar associados a apenas uma raiz. Por exemplo: Departamento pode ter muitos Funcionários e um Funcionário pode ter muitos Projetos. Porém um Projeto não pode ter muitos Funcionários pertencentes a diferentes departamentos. Depois de uma raiz ser definida, todo o acesso a este

objeto raiz e seus descendentes será gerenciado através da raiz. O WebSphere eXtreme Scale usa o código hash da chave do objeto raiz para escolher uma partição. Por exemplo:

```
partition = (hashCode MOD numPartitions).
```

Quando todos os dados para um relacionamento estiverem ligados a um única instância do objeto, toda a árvore pode ser co-localizada em uma única partição e pode ser acessada muito eficientemente usando uma transação. Se os dados englobarem múltiplos relacionamentos, então múltiplas partições devem estar envolvidas que envolvem chamadas remotas adicionais, o que pode levar a gargalos no desempenho.

Dados de Referência

Alguns relacionamentos incluem dados de consulta ou de referência como: `CountryName`. Para dados de consulta ou de referência, os dados devem existir em cada partição. Os dados podem ser acessados por qualquer chave raiz e o mesmo resultado é retornado. Os dados de referência como estes devem ser usados apenas nos casos em que os dados forem razoavelmente estáticas. Atualizar esses dados pode ser dispendioso porque eles precisam ser atualizados em cada partição. A API DataGrid é uma técnica comum para manter os dados de referência atualizados.

Custos e Benefícios de Normalização

A normalização dos dados usando os relacionamentos pode ajudar a reduzir a quantidade de memória usada pela grade de dados pois a duplicação dos dados é diminuída. Porém, em geral, quanto mais dados relacionais forem incluídos, menos eles irão expandir. Quando os dados são agrupados juntos, torna-se mais caro manter os relacionamentos e manter os tamanhos gerenciáveis. Como os dados das partições da grade baseiam-se na chave da raiz da árvore, o tamanho da árvore não é levado em consideração. Assim, se você tiver uma grande quantidade de relacionamentos para uma instância da árvore, a grade de dados poderá ficar desequilibrada, fazendo com que uma partição mantenha mais dados do que as outras.

Quando os dados forem não normalizados ou simplificados, os dados que normalmente seriam compartilhados entre os dois objetos são duplicados e cada tabela pode ser particionada de modo independente, oferecendo uma grade de dados muito mais equilibrada. Apesar disto aumentar a quantidade de memória usada, permite que o aplicativo escale pois uma única linha de dados pode ser acessada que pode ter todos os dados necessários. Isto é ideal para grades com maior quantidade de leituras pois a manutenção dos dados se torna mais cara.

Para obter informações adicionais, consulte Classificação de sistemas XTP e escalamento.

Gerenciamento de Relacionamentos Usando as APIs de Acesso a Dados

A API ObjectMap é a mais rápida, mais flexível e granular das APIs de acesso a dados, oferecendo uma abordagem transacional baseada em sessão no acesso aos dados na grade de mapas. A API ObjectMap permite que os clientes usem operações comuns, como create, read, update e delete (CRUD), para gerenciar pares de valores de chave de objetos na grade de dados distribuída.

Ao usar a API ObjectMap, os relacionamentos de objetos devem ser expressos pela incorporação da chave estrangeira para todos os relacionamentos no objeto-pai.

A seguir, está um exemplo.

```
public class Department {
 Collection<String> employeeIds;
}
```

A API EntityManager simplifica o gerenciamento de relacionamentos através da extração de dados persistentes a partir de objetos incluindo as chaves estrangeiras. Quando o objeto é posteriormente recuperado da grade de dados, o gráfico de relacionamentos é reconstruído, como no seguinte exemplo.

```
@Entity
public class Department {
 Collection<String> employees;
}
```

A API EntityManager é muito semelhante a outras tecnologias de persistência do objeto Java como JPA e Hibernate na qual ela sincroniza um gráfico de instâncias de objetos Java gerenciados com o armazenamento persistente. Nesse caso, o armazenamento persistente é uma grade de dados do eXtreme Scale, em que cada entidade é representada como um mapa e o mapa contém os dados da entidade em vez das instâncias do objeto.

Definindo um Esquema de Entidade: Java

Um ObjectGrid pode ter inúmeros esquemas de entidade lógicos. As entidades são definidas usando as classes Java anotadas, o XML ou uma combinação de classes XML e Java. Entidades definidas são registradas com um servidor eXtreme Scale e ligadas a BackingMaps, índices e outros plug-ins.

Ao projetar uma esquema de entidade, é necessário concluir as seguintes tarefas:

1. Definir as entidades e seus relacionamentos.
2. Configurar o eXtreme Scale.
3. Registrar as entidades.
4. Criar aplicativos baseados em entidade que interajam com as APIs EntityManager do eXtreme Scale.

Configuração do Esquema de Entidade

Um esquema de entidade é um conjunto de entidades e relacionamentos entre as entidades. Em um aplicativo eXtreme Scale com várias partições, as opções e restrições a seguir aplicam-se aos esquemas de entidade:

- Cada esquema de entidade deve ter uma raiz única definida. Esta é conhecida como a raiz do esquema.
- Todas as entidades para um determinado esquema devem estar no mesmo conjunto de mapas, o que significa que todas as entidades que podem ser alcançadas a partir de uma raiz de esquema com relacionamentos de chave e não-chave devem ser definidas no mesmo conjunto de mapas como a raiz do esquema.
- Cada entidade pode pertencer a apenas um esquema de entidade.
- Cada aplicativo eXtreme Scale pode ter vários esquemas.

Entidades são registradas com uma instância de ObjectGrid antes de serem inicializadas. Cada entidade definida deve ser nomeada exclusivamente e ligada automaticamente a um BackingMap de ObjectGrid de mesmo nome. O método de inicialização varia dependendo da configuração que você utilizando:

Configuração do eXtreme Scale local

Se estiver utilizando um ObjectGrid local, será possível configurar programaticamente o esquema de entidade. Neste modo, é possível utilizar os métodos ObjectGrid.registerEntities para registrar classes de entidade anotadas ou um arquivo descritor de metadados.

Configuração do eXtreme Scale distribuída

Se você estiver utilizando uma configuração do eXtreme Scale distribuída, é necessário fornecer um arquivo descritor de metadados da entidade com o esquema de entidade.

Para obter detalhes adicionais, consulte “Entity Manager em um Ambiente Distribuído” na página 401.

Requisitos de Entidade

Os metadados de entidade são configurados com o uso de arquivos de classe Java, um XML do descritor de entidade ou ambos. No mínimo, o XML do descritor de entidade é requerido para identificar quais BackingMaps do eXtreme Scale devem ser associados às entidades. Os atributos persistentes da entidade e seus relacionamentos com outras entidades são descritos em uma classe Java anotada (classe de metadados da entidade) ou arquivo XML do descritor de entidade. A classe de metadados da entidade, quando especificada, também é utilizada pela API EntityManager para interagir com dados na grade.

Uma grade do eXtreme Scale pode ser definida sem fornecer quaisquer classes de entidade. Isso pode ser benéfico quando o servidor e o cliente estiverem interagindo diretamente com os dados da tupla armazenados nos mapas subjacentes. Tais entidades são definidas completamente no arquivo XML do descritor de entidade e são referidas como entidades sem classe.

Entidades sem Classe

As entidades sem classe são úteis quando não é possível incluir classes de aplicativo no caminho de classe do servidor ou do cliente. Tais entidades são definidas no arquivo XML do descritor de entidade, onde o nome da classe da entidade é especificado utilizando um identificador de entidade sem classe no formato: @<identificador de entidade>. O símbolo @ identifica a entidade como sem classe e é utilizado para mapear associações entre entidades. Consulte a figura "Metadados da Entidade sem Classe" para ver um exemplo de um arquivo XML do descritor de metadados da entidade com duas entidades sem classe definidas.

Se um cliente ou servidor eXtreme Scale não tiver acesso às classes, eles poderão utilizar a API EntityManager utilizando as entidades sem classes. Casos de uso comuns incluem o seguinte:

- O contêiner do eXtreme Scale é hospedado em um servidor que não permite classes de aplicativo no caminho de classe. Nesse caso, os clientes ainda podem acessar a grade utilizando a API EntityManager de um cliente em que as classes sejam permitidas.
- O cliente eXtreme Scale não requer acesso às classes de entidade porque o cliente está utilizando um cliente não Java, como o serviço de dados REST do eXtreme Scale, ou o cliente está acessando os dados da tupla na grade utilizando a API de ObjectMap.

Se os metadados da entidade forem compatíveis entre cliente e servidor, eles poderão ser criados utilizando classes de metadados da entidade, um arquivo XML ou ambos.

Por exemplo, a "Classe de Entidade Programática" na figura a seguir é compatível com o código de metadados sem classe na próxima seção.

Classe de entidade programática

```
@Entity
public class Employee {
    @Id long serialNumber;
    @Basic byte[] picture;
    @Version int ver;
    @ManyToOne(fetch=FetchType.EAGER, cascade=CascadeType.PERSIST)
    Department department;
}

@Entity
public static class Department {
    @Id int number;
    @Basic String name;
    @OneToMany(fetch=FetchType.LAZY, cascade=CascadeType.ALL, mappedBy="department")
    Collection<Employee> employees;
}
```

Versões, Chaves e Campos sem Classe

Conforme mencionado anteriormente, as entidades sem classe são configuradas completamente no arquivo descritor XML da entidade. As entidades baseadas em classe definem seus atributos utilizando campos, propriedades e anotações Java. Portanto, as entidades sem classe precisam definir a estrutura de chave e atributo no descritor XML da entidade com as tags <basic> e <id>.

Metadados da entidade sem classe

```
<?xml version="1.0" encoding="UTF-8"?>
<entity-mappings xmlns="http://ibm.com/ws/projector/config/emd"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/projector/config/emd ./emd.xsd">

<entity class-name="@Employee" name="Employee">
    <attributes>
        <id name="serialNumber" type="long"/>
        <basic name="firstName" type="java.lang.String"/>
        <basic name="picture" type="[B"/>
        <version name="ver" type="int"/>
        <many-to-one name="department"
            target-entity="@Department"
            fetch="EAGER"">
                <cascade><cascade-persist/></cascade>
        </many-to-one>
    </attributes>
</entity>

<entity class-name="@Department" name="Department" >
    <attributes>
        <id name="number" type="int"/>
        <basic name="name" type="java.lang.String"/>
        <version name="ver" type="int"/>
        <one-to-many name="employees"
            target-entity="@Employee"
            fetch="LAZY"
            mapped-by="department">
```

```
            <cascade><cascade-all/></cascade>
        </one-to-many>
    </attributes>
</entity>
```

Observe que cada entidade acima tem um elemento <id>. Uma entidade sem classe deve ter um ou mais de um elemento <id> definido, ou uma associação com valor único que represente a chave para a entidade. Os campos da entidade são representados pelos elementos <basic>. Os elementos <id>, <version> e <basic> requerem um nome e um tipo nas entidades sem classe. Consulte a seguinte seção de tipos de atributo suportados para obter detalhes sobre os tipos suportados.

Requisitos de Classe da Entidade

As entidades baseadas em classe são identificadas por meio da associação de vários metadados com uma classe Java. Os metadados podem ser especificados usando anotações do Java Platform, Standard Edition Versão 5, um arquivo descritor de metadados da entidade ou uma combinação de anotações e do arquivo descritor. As classes de entidade precisam atender os seguintes critérios:

- A anotação `@Entity` é especificada no arquivo descritor XML da entidade.
- A classe tem um construtor no-argument público ou protegido.
- Ela deve ser uma classe de nível superior. Interfaces e tipos enumerados não são classes de entidade válidas.
- Não é possível utilizar a palavra-chave final.
- Não é possível utilizar herança.
- É necessário ter nome e tipo exclusivos para cada instância de ObjectGrid.

As entidades todas possuem um nome e tipo exclusivos. O nome, se utilizando anotações, é o nome simples (curto) da classe por padrão, mas pode ser substituído utilizando o atributo name da anotação `@Entity`.

Atributos Persistentes

O estado persistente de uma entidade é acessado por cliente e o entity manager utilizando qualquer um dos campos (variáveis de instância) ou acessores de propriedade do estilo Enterprise JavaBeans. Cada entidade deve definir um acesso baseado em campo ou em propriedade. Entidades anotadas são field-access se os campos de classe são anotados e property-access se o método getter da propriedade é anotada. Uma mistura de acesso por campo e acesso por propriedade não é permitida. Se o tipo não puder ser automaticamente determinado, o atributo **`accessType`** na anotação `@Entity` ou XML equivalente pode ser utilizado para identificar o tipo de acesso.

Campos persistentes
: As variáveis de instância da entidade field-access são acessadas diretamente a partir do entity manager e dos clientes. Os campos que são marcados com o modificador transiente ou a anotação transiente são ignorados. Campos persistentes devem ter modificadores final ou static.

Propriedades persistentes
: As entidades de acesso de propriedade devem seguir as convenções de assinatura do JavaBeans para as propriedades de leitura e gravação. Os métodos que não seguirem as convenções do JavaBeans ou possuírem a anotação Transient no método getter serão ignorados. Para uma propriedade do tipo `T`, deve haver um método getter getProperty que retorne um valor do tipo T e um método setter void setProperty(T). Para

tipos booleanos, o método getter pode ser expresso como isProperty, retornando true ou false. As propriedades persistentes não podem ter um modificador estático.

Tipos de atributos suportados

O seguinte campo persistente e tipos de propriedades são suportados:

- Os tipos primitivos Java incluindo wrappers
- java.lang.String
- java.math.BigInteger
- java.math.BigDecimal
- java.util.Date
- java.util.Calendar
- java.sql.Date
- java.sql.Time
- java.sql.Timestamp
- byte[]
- java.lang.Byte[]
- char[]
- java.lang.Character[]
- enum

Tipos de atributos serializáveis são suportados mas possuem limitações de desempenho, consulta e detecção de alterações. Dados persistentes que não podem ser colocados em proxy, como matrizes e objetos serializáveis de usuário, devem ser reatribuídos para a entidade se alterados.

Os atributos serializáveis são representados no arquivo XML do descritor de entidade utilizando o nome de classe do objeto. Se o objeto for uma matriz, o tipo de dado será representado utilizando a forma interna Java. Por exemplo, se um tipo de dado de atributo for java.lang.Byte[][], a representação de cadeia será [[Ljava.lang.Byte;

Os tipos serializáveis de usuários devem obedecer às seguintes boas práticas:

- Implemente métodos de serialização de alto desempenho. Implemente a interface java.lang.Cloneable e um método clone público.
- Implemente a interface java.io.Externalizable.
- Implemente iguais e hashCode

Associações de Entidade

Associações de entidades bidirecionais e unidirecionais, ou relacionamentos entre entidades podem ser definidos como um-para-um, muitos-para-um, um-para-muitos e muitos-para-muitos. O gerenciador de entidade resolve automaticamente os relacionamentos da entidade com as referências de chave apropriadas ao armazenar entidades.

A grade do eXtreme Scale é um cache de dados e não força integridade referencial como um banco de dados. Embora os relacionamentos permitam persistência em cascata e removam operações para entidades-filhas, eles não detectam ou impões links quebrados em objetos. Quando remover um objeto-filho, a referência a esse objeto deve ser removida do pai.

Se você definir uma associação bidirecional entre duas entidades, será preciso definir o proprietário do relacionamento. Em uma associação para-muitos, o lado muitos do relacionamento é sempre o lado do proprietário. Se a propriedade não puder ser determinada automaticamente, então, o atributo **mappedBy** da anotação ou equivalente XML, deve ser especificado. O atributo **mappedBy** identifica o campo na entidade de destino que é a proprietária do relacionamento. Este atributo também ajuda a identificar os campos relacionados quando há vários atributos do mesmo tipo e cardinalidade.

Associações com valor único

Associações um-para-um e muitos-para-um são indicadas utilizando anotações @OneToOne e @ManyToOne ou atributos XML equivalentes. O tipo de entidade de destino é determinado pelo tipo de atributo. O exemplo a seguir define uma associação unidirecional entre Person e Address.s A entidade Cliente tem uma referência a uma entidade Endereço. Nesse caso, a associação poderia também ser de muitos-para-um, já que não há relacionamento inverso.

```
@Entity
public class Customer {
  @Id id;
  @OneToOne Address homeAddress;
}

@Entity
public class Address{
  @Id id
  @Basic String city;
}
```

Para especificar um relacionamento bidirecional entre as classes Customer e Address, inclua uma referência à classe Customer a partir da classe Address e inclua a anotação apropriada para marcar o lado inverso do relacionamento. Como essa associação é um-para-um, você precisa especificar um proprietário do relacionamento utilizando o atributo mappedBy na anotação @OneToOne.

```
@Entity
public class Address{
  @Id id
  @Basic String city;
  @OneToOne(mappedBy="homeAddress") Customer customer;
}
```

Associações com valor de coleta

Associações um-para-muitos e muitos-para-muitos são denotadas utilizando as anotações `@OneToMany` e `@ManyToMany` ou atributos XML XML equivalente. Todos os relacionamentos muito são representados utilizando os tipos: java.util.Collection, java.util.List ou java.util.Set. O tipo de entidade de destino é determinado pelo tipo genérico de Collection, List ou Set ou explicitamente utilizando atributo **`targetEntity`** na anotação `@OneToMany` ou `@ManyToMany` (ou XML equivalente).

No exemplo anterior, não é prático ter um objeto address por cliente porque muitos clientes podem compartilhar um endereço ou podem ter vários endereços. Esta situação é melhor resolvida utilizando uma associação many:

```
@Entity
public class Customer {
  @Id id;
  @ManyToOne Address homeAddress;
  @ManyToOne Address workAddress;
}
```

```
@Entity
public class Address{
  @Id id
  @Basic String city;
  @OneToMany(mappedBy="homeAddress") Collection<Customer> homeCustomers;


  @OneToMany(mappedBy="workAddress", targetEntity=Customer.class)
  Collection workCustomers;
}
```

Neste exemplo, existem dois diferentes relacionamentos entre as mesmas entidades: um relacionamento de endereços Home e Work. Uma Collection não genérica é utilizada para o atributo **workCustomers** para demonstrar como utilizar o atributo **targetEntity** quando genéricos não estiverem disponíveis.

Associações sem classe

As associações de entidade sem classe são definidas no arquivo XML do descritor de metadados da entidade de forma semelhante ao modo como as associações baseadas em classe são definidas. A única diferença é que em vez de a entidade de destino apontar para uma classe real, ela aponta para o identificador da entidade sem classe utilizado para o nome de classe da entidade.

Este é um exemplo:

```
<many-to-one name="department" target-entity="@Department"
fetch="EAGER">
      <cascade><cascade-all/></cascade>
</many-to-one>
<one-to-many name="employees" target-entity="@Employee"
fetch="LAZY">
      <cascade><cascade-all/></cascade>
</one-to-many>
```

Chaves Primárias

Todas as entidades devem ter uma chave primária, que pode ser uma chave simples (atributo único) ou composta (atributos múltiplos). Os atributos-chave são denotados utilizando a anotação Id ou definidos no arquivo descritor XML da entidade. Atributos-chave possuem os seguintes requisitos:

- O valor de uma chave primária não pode mudar.
- Um atributo de chave principal deve ser um dos seguintes tipos: tipo primitivo Java e wrappers, java.lang.String, java.util.Date ou java.sql.Date.
- Uma chave primária pode conter qualquer número de associações com valor único. A entidade de destino da associação de chave primária não pode ter uma associação inversa direta ou indiretamente à entidade de origem.

As chaves primárias compostas podem definir opcionalmente uma classe de chave primária. Uma entidade é associada a uma classe de chave primária com o uso da anotação `@IdClass` ou arquivo descritor XML da entidade. Uma anotação `@IdClass` é útil junto com o método EntityManager.find.

As classes de chave primária possuem os seguintes requisitos:

- Ela deve ser pública com um construtor no-argument.
- O tipo de acesso da classe de chave primária é determinado pela entidade que declara a classe da chave primária.

- Se acesso por propriedade, as propriedades da classe de chave primária precisam ser públicas ou protegidas.
- Os campos-chave primários ou propriedades devem corresponder aos nomes do atributo-chave e tipos definidos na entidade de referência.
- As classes de chave primária devem implementar os métodos equals e hashCode.

Este é um exemplo:

```
@Entity
@IdClass(CustomerKey.class)
public class Customer {
    @Id @ManyToOne Zone zone;
    @Id int custId;
    String name;
    ...
}

@Entity
public class Zone{
    @Id String zoneCode;
    String name;
}

public class CustomerKey {
    Zone zone;
    int custId;

    public int hashCode() {...}
    public boolean equals(Object o) {...}
}
```

Chaves primárias sem classe

Entidades sem classe devem ter pelo menos um elemento <id> ou uma associação no arquivo XML com o atributo `id=true`. Um exemplo de ambos seria semelhante ao seguinte:

```
<id name="serialNumber" type="int"/>
<many-to-one name="department" target-entity="@Department"
id="true">
<cascade><cascade-all/></cascade>
</many-to-one>
```

Lembre-se:
A tag XML <id-class> não é suportada para entidades sem classe.

Proxies de Entidade e Intercepção de Campo

As classes de entidade e os tipos de atributos suportados mutáveis são estendidos pelas classes de proxy para entidades de acesso à propriedade e código de byte aprimorado para entidades de acesso ao campo. Todos os acessos à entidade, mesmo por meio de métodos de negócios internos e dos métodos equals, devem utilizar o campo apropriado ou os métodos de acesso da propriedade.

Os proxies e interceptores de campo são utilizados para permitir que o entity manager controle o estado da entidade, determine se a entidade foi alterada e aprimore o desempenho.

Atenção: Ao utilizar entidades property-access, o método equals deve utilizar o operador instanceof para comparar a instância atual com o objeto input. Toda a introspecção do objeto de destino deve ser por meio das propriedades do objeto, e não dos campos em si, pois a instância do objeto será o proxy.

Conceitos relacionados:

Java "Ajustando o Desempenho da Interface EntityManager" na página 760
A interface EntityManager separa aplicativos do estado de suspensão no armazenamento de dados da grade do servidor.

Java "Objetos de Armazenamento em Cache e seus Relacionamentos (API EntityManager)" na página 388
A maioria dos produtos de cache utiliza APIs baseadas em mapa para armazenar dados como pares de chave-valor. A API ObjectMap e o cache dinâmico no WebSphere Application Server, entre outros, usam essa abordagem. Entretanto, APIs baseadas em mapas têm limitações. A API EntityManager simplifica a interação com a grade de dados ao fornecer uma maneira fácil de declarar e interagir com um gráfico complexo de objetos relacionados.

Java "Entity Manager em um Ambiente Distribuído" na página 401
É possível usar a API EntityManager com um ObjectGrid local ou em um ambiente distribuído do eXtreme Scale . A principal diferença é como você se conecta a esse ambiente remoto. Após você estabelecer uma conexão, não existe diferença entre o uso de um objeto Session ou uma API do EntityManager.

Java "Interagindo com EntityManager" na página 405
Geralmente os aplicativos primeiro obtêm uma referência do ObjectGrid e, depois, uma Sessão dessa referência para cada encadeamento. As sessões não podem ser compartilhadas entre encadeamentos. Um método extra em Session, o método getEntityManager, está disponível. Este método retorna uma referência para um gerenciador de entidades para uso para este encadeamento. A interface de EntityManager pode substituir as interfaces de Session e ObjectMap para todos os aplicativos. É possível utilizar essas APIs de EntityManager se o cliente tiver acesso às classes de entidade definidas.

Java "Suporte ao Plano de Carregamento do EntityManager" na página 417
Um FetchPlan é a estratégia que o gerenciador de entidade usa para recuperar objetos associados se o aplicativo precisar acessar relacionamentos.

Java "Filas de Consulta da Entidade" na página 421
Filas de consulte permitem que aplicativos criem uma fila qualificada por uma consulta no lado do servidor ou eXtreme Scale local sobre uma entidade. As entidades do resultado da consulta são armazenadas nesta fila. Atualmente, a fila de consulta é suportada apenas em um mapa que está utilizando a estratégia de bloqueio pessimista.

Java "Roteando os Objetos de Cache para a Mesma Partição" na página 432
Quando a configuração do eXtreme Scale usa a estratégia de colocação de partição fixa, ela dependerá do hash da chave para uma partição inserir, obter, atualizar ou remover o valor. O método hashCode é chamado na chave e ele deverá ser bem definido se uma chave customizada for criada. No entanto, outra opção é usar a interface PartitionableKey. Com a interface PartitionableKey, será possível usar um objeto diferente da chave para efetuar hash de uma partição.

Tarefas relacionadas:

Java "Tutorial: Armazenando Informações de Pedido nas Entidades" na página 9
Este tutorial do gerenciador de entidade mostra como utilizar o WebSphere eXtreme Scale para armazenar informações de pedido em um Web site. É possível criar um aplicativo Java Platform, Standard Edition 5 simples que utiliza um eXtreme Scale local e de memória. As entidades utilizam anotações e genéricos do Java SE 5.

"Colocando Diversos Objetos de Cache na Mesma Partição" na página 429

Ao definir dados relacionados em conjuntos de mapas que são organizados na mesma partição, você pode evitar a duplicação de dados e permitir o acesso a dados de baixa granularidade.

Informações relacionadas:

Java Amostra: Executando as Consultas em Paralelo Usando um ReduceGridAgent

Entity Manager em um Ambiente Distribuído: Java

É possível usar a API EntityManager com um ObjectGrid local ou em um ambiente distribuído do eXtreme Scale . A principal diferença é como você se conecta a esse ambiente remoto. Após você estabelecer uma conexão, não existe diferença entre o uso de um objeto Session ou uma API do EntityManager.

Arquivos de Configuração Necessários

Os seguintes arquivos de configuração XML são necessários:

- Arquivo XML descritor do ObjectGrid
- Arquivo XML descritor da entidade
- Arquivo XML descritor de implementação ou de grade de dados

Esses arquivos especificam as entidades e os BackingMaps que um servidor hospeda.

O arquivo descritor de metadados da entidade contém uma descrição das entidades que são utilizadas. No mínimo, você deve especificar o nome e a classe da entidade. Se você estiver executando em um ambiente Java Platform, Standard Edition 5, oeXtreme Scale automaticamente lê a classe da entidade e suas anotações. É possível definir atributos XML adicionais se a classe de entidade não tiver anotações ou se você precisar substituir os atributos de classe. Se estiver registrando as entidades sem classe, forneça todas as informações da entidade apenas no arquivo XML.

É possível usar o seguinte fragmento de configuração XML para definir uma grade de dados com entidades. Nesse fragmento, o servidor cria um ObjectGrid com o nome `bookstore` e um mapa de apoio associado com o nome `order`. O fragmento no arquivo `objectgrid.xml` refere-se ao arquivo `entity.xml`. Nesse caso, o arquivo `entity.xml` contém uma entidade, a Order.

objectgrid.xml

```
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">

 <objectGrids>
    <objectGrid name="bookstore" entityMetadataXMLFile="entity.xml">
     <backingMap name="Order"/>
    </objectGrid>
</objectGrids>

</objectGridConfig>
```

Este arquivo `objectgrid.xml` especifica o arquivo `entity.xml` com o atributo **`entityMetadataXMLFile`**. O valor pode ser um diretório relativo ou um caminho absoluto.

- **Para um relatório relativo:** Especifique o local relativo com o local do arquivo `objectgrid.xml`.

- **Para um caminho absoluto:** Especifique o local com um formato de URL, como `file://` ou `http://`.

Este é um exemplo do arquivo `entity.xml`:

entity.xml
```
<entity-mappings xmlns="http://ibm.com/ws/projector/config/emd"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/projector/config/emd ./emd.xsd">
 <entity class-name="com.ibm.websphere.tutorials.objectgrid.em.di
distributed.step1.Order" name="Order"/>
</entity-mappings>
```

Este exemplo assume que a classe Order teria os campos **orderNumber** e **desc** anotados de modo semelhante.

A seguir há um exemplo do arquivo `server.properties` sem classe equivalente:

classless entity.xml
```
<entity-mappings xmlns="http://ibm.com/ws/projector/config/emd"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/projector/config/emd ./emd.xsd">
 <entity class-name="@Order " name="Order">
     <description>"Entity named: Order"</description>
        <attributes>
            <id name="orderNumber" type="int"/>
            <basic name="desc" type="java.lang.String"/>
        </attributes>
 </entity>
</entity-mappings>
```

Para obter informações sobre como iniciar servidores, consulte Iniciando e Parando Servidores Independentes. É possível usar ambos os arquivos `deployment.xml` e `objectgrid.xml` para iniciar o servidor de catálogos.

Conectando-se a um Servidor eXtreme Scale Distribuído

O seguinte código ativa o mecanismo de conexão para um cliente e servidor no mesmo computador:

```
String catalogEndpoints="localhost:2809";
URL clientOverrideURL= new URL("file:etc/emtutorial/distributed/step1/objectgrid.xml");
ClientClusterContext clusterCtx = ogMgr.connect(catalogEndpoints, null, clientOverrideURL);
ObjectGrid objectGrid=ogMgr.getObjectGrid(clusterCtx, "bookstore");
```

No fragmento de código anterior, observe a referência ao servidor eXtreme Scale remoto. Após estabelecer uma conexão, é possível invocar os métodos de API do EntityManager como persist, update, remove e find.

Atenção: Quando estiver usando entidades, passe o arquivo XML do descritor do ObjectGrid de substituição para o método connect. Se um valor nulo é passado para a propriedade clientOverrideURL e o cliente tem uma estrutura de diretório doferente da estrutura de diretório do servidor, então o cliente pode falhar em localizar os arquivos XML do descritor de entidade ou ObjectGrid. No mínimo, os arquivos XML de entidade e ObjectGrid para o servidor podem ser copiados para o cliente.

Anteriormente, o uso de entidades no cliente ObjectGrid exigia que você deixasse o XML do ObjectGrid e o XML da entidade disponíveis para o cliente de uma das duas maneiras a seguir:

1. Passe um XML do ObjectGrid de substituição para o método ObjectGridManager.connect(String catalogServerEndpoints, ClientSecurityConfiguration securityProps, URL overRideObjectGridXml).

   ```
   String catalogEndpoints="myHost:2809";
   URL clientOverrideURL= new URL("file:etc/emtutorial/distributed/step1/objectgrid.xml");
   ClientClusterContext clusterCtx = ogMgr.connect(catalogEndpoints, null, clientOverrideURL);
   ObjectGrid objectGrid=ogMgr.getObjectGrid(clusterCtx, "bookstore");
   ```

2. Transmita nulo para o arquivo de substituição e certifique-se de que o XML do ObjectGrid e o XML da entidade referida estejam disponíveis para o cliente no mesmo caminho que no servidor.

```
String catalogEndpoints="myHost:2809";
ClientClusterContext clusterCtx = ogMgr.connect(catalogEndpoints,
null, null);
ObjectGrid objectGrid=ogMgr.getObjectGrid(clusterCtx, "bookstore");
```

Os arquivos XML eram necessários, independentemente de você querer ou não utilizar um subconjunto de entidades no lado do cliente. Esses arquivos não são mais necessários para o uso de entidades, conforme definido pelo servidor. Em vez disso, transmita nulo como o parâmetro overRideObjectGridXml como na opção 2 da seção anterior. Se o arquivo XML não estiver localizado no mesmo caminho configurado no servidor, o cliente usa a configuração da entidade no servidor.

Entretanto, se você utilizar entidades do subconjunto no cliente, será necessário fornecer um XML do ObjectGrid de substituição na opção 1.

Esquema do Lado do Cliente e do Servidor

O esquema do lado do servidor define o tipo de dado armazenado nos mapas em um servidor. O esquema do lado do cliente é um mapeamento para objetos de aplicativo do esquema no servidor. Por exemplo, é possível ter o seguinte esquema do lado do servidor:

```
@Entity
class ServerPerson
{
  @Id String ssn;
  String firstName;
  String surname;
  int age;
  int salary;
}
```

Um cliente pode ter um objeto anotado como no exemplo a seguir:

```
@Entity(name="ServerPerson")
class ClientPerson
{
  @Id @Basic(alias="ssn") String socialSecurityNumber;
  String surname;
}
```

Este cliente, então, toma uma entidade do lado do servidor e projeta o subconjunto da entidade no objeto do cliente. Esta projeção leva à economia de largura de banda e de memória em um cliente porque o cliente tem somente as informações que ele precisa em vez de todas as informações que estiverem na entidade do lado do servidor. Aplicativos diferentes podem utilizar seus próprios objetos em vez de forçarem todos os aplicativos a compartilharem um conjunto de classes para o acesso a dados.

O arquivo XML descritor da entidade do lado do cliente é necessário nos seguintes casos: se o servidor estiver em execução com entidades baseadas em classe enquanto o lado do cliente está em execução sem classes; ou se o servidor estiver sem classes e o cliente utilizar entidades baseadas em classe. Um modo de cliente sem classe permite que o cliente ainda execute consultas de entidade sem precisar acessar classes físicas. Supondo que o servidor tenha registrado a entidade ServerPerson acima, o cliente poderia substituir a grade de dados por um arquivo `entity.xml` como a seguir:

```
<entity-mappings xmlns="http://ibm.com/ws/projector/config/emd"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/projector/config/emd ./emd.xsd">
 <entity class-name="@ServerPerson " name="Order">
     <description>"Entity named: Order"</description>
        <attributes>
            <id name="socialSecurityNumber" type="java.lang.String"/>
```

```
            <basic name="surname" type="java.lang.String"/>
        </attributes>
 </entity>
</entity-mappings>
```

Este arquivo atinge uma entidade de subconjunto equivalente no cliente, sem exigir que o cliente forneça a classe anotada real. Se o servidor não tiver classe e o cliente tiver, o cliente fornecerá um arquivo XML do descritor de entidade de substituição. Este arquivo XML do descritor de entidade contém uma substituição para a referência do arquivo de classe.

Fazendo Referência ao Esquema

Se seu aplicativo estiver em execução no Java SE 5, o aplicativo poderá ser incluído nos objetos usando anotações. O EntityManager pode ler o esquema nas anotações de tais objetos. O aplicativo fornece ao tempo de execução do eXtreme Scale referências a esses objetos utilizando o arquivo `entity.xml`, que é referido no arquivo `objectgrid.xml`. O arquivo `entity.xml` lista todas as entidades, cada uma associada a uma classe ou a um esquema. Se um nome de classe apropriado for especificado, o aplicativo tentará ler as anotações do Java SE 5 a partir dessas classes para determinar o esquema. Se você não anotar o arquivo de classe ou especificar um identificador sem classe como o nome de classe, o esquema será tirado do arquivo XML. O arquivo XML é utilizado para especificar todos os atributos, chaves e relacionamentos para cada entidade.

Uma grade de dados local não precisa de arquivos XML. O programa pode obter uma referência do ObjectGrid e invocar o método ObjectGrid.registerEntities para especificar uma lista de classes anotadas do Java SE 5 ou um arquivo XML.

O tempo de execução utiliza o arquivo XML ou uma lista de classes anotadas para localizar nomes de entidades, nomes e tipos de atributos, tipos e campos chave e relacionamentos entre entidades. Se o eXtreme Scale estiver executando em um servidor ou em modo independente, então ele cria automaticamente um mapa nomeado após cada entidade. Estes mapas podem ser customizados adicionalmente utilizando o arquivo `objectgrid.xml` ou APIs configuradas pelo aplicativo ou por estruturas de injeção tais como Spring.

Arquivo Descritor de Metadados da Entidade

Consulte Arquivo `emd.xsd` para obter informações adicionais sobre o arquivo descritor de metadados.

Tarefas relacionadas:

Java "Tutorial: Armazenando Informações de Pedido nas Entidades" na página 9
Este tutorial do gerenciador de entidade mostra como utilizar o WebSphere eXtreme Scale para armazenar informações de pedido em um Web site. É possível criar um aplicativo Java Platform, Standard Edition 5 simples que utiliza um eXtreme Scale local e de memória. As entidades utilizam anotações e genéricos do Java SE 5.

"Colocando Diversos Objetos de Cache na Mesma Partição" na página 429
Ao definir dados relacionados em conjuntos de mapas que são organizados na mesma partição, você pode evitar a duplicação de dados e permitir o acesso a dados de baixa granularidade.

Referências relacionadas:

Java "Agente de Instrumentação de Desempenho da Entidade" na página 762
É possível melhorar o desempenho de entidades de acesso ao campo ativando o agente de instrumentação do WebSphere eXtreme Scale ao usar o Java Development Kit (JDK) Versão 6 ou posterior.

Java "Definindo um Esquema de Entidade" na página 391
Um ObjectGrid pode ter inúmeros esquemas de entidade lógicos. As entidades são definidas usando as classes Java anotadas, o XML ou uma combinação de classes XML e Java. Entidades definidas são registradas com um servidor eXtreme Scale e ligadas a BackingMaps, índices e outros plug-ins.

Java "Listeners de Entidade e Métodos de Retorno de Chamada" na página 408
Os aplicativos podem ser notificados quando o estado de uma entidade é alterado de estado para estado. Dois mecanismos de retorno de chamada existem para os eventos de mudança de estado: os métodos de retorno de chamada do ciclo de vida que são definidos em uma classe de entidade e são chamados sempre que o estado da entidade é alterado e os listeners de entidade, que são mais gerais porque o listener da entidade pode ser registrado em várias entidades.

Java "Exemplos do Listener de Entidade" na página 414
É possível gravar EntityListeners com base em seus requisitos. Veja a seguir vários scripts de exemplo.

Java "Interface EntityTransaction" na página 426
É possível utilizar a interface EntityTransaction para demarcar transações.

Informações relacionadas:

Java Amostra: Executando as Consultas em Paralelo Usando um ReduceGridAgent

Interagindo com EntityManager: Java

Geralmente os aplicativos primeiro obtêm uma referência do ObjectGrid e, depois, uma Sessão dessa referência para cada encadeamento. As sessões não podem ser compartilhadas entre encadeamentos. Um método extra em Session, o método getEntityManager, está disponível. Este método retorna uma referência para um gerenciador de entidades para uso para este encadeamento. A interface de EntityManager pode substituir as interfaces de Session e ObjectMap para todos os aplicativos. É possível utilizar essas APIs de EntityManager se o cliente tiver acesso às classes de entidade definidas.

Obtendo uma Instância de EntityManager de uma Sessão

O método getEntityManager está disponível em um objeto Session. O exemplo de código a seguir ilustra como criar uma instância de ObjectGrid local e acessar EntityManager. Consulte a interface EntityManager na documentação da API para obter detalhes sobre todos os métodos suportados.

```
ObjectGrid og =
ObjectGridManagerFactory.getObjectGridManager().createObjectGrid("intro-grid");
Session s = og.getSession();
EntityManager em = s.getEntityManager();
```

Existe um relacionamento um para um entre o objeto Session e o objeto EntityManager. É possível utilizar o objeto EntityManager mais de uma vez.

Persistindo uma Entidade

A persistência de uma entidade significa salvar o estado de uma nova entidade em um cache ObjectGrid. Depois de chamar o método "persist", a entidade fica no estado "managed". A operação persist é transacional e a nova entidade fica armazenada no cache do ObjectGrid depois da confirmação do cache.

Cada entidade tem um BackingMap correspondente no qual as tuplas são armazenadas. O BackingMap tem o mesmo nome que a entidade e será criado quando a classe for registrada. O seguinte exemplo de código demonstra como criar um objeto Order usando a operação persist.

```
Order order = new Order(123);
em.persist(order);
order.setX();
...
```

O objeto Order é criado com a chave 123 e o objeto é passado para método persist. É possível continuar a modificar o estado do objeto antes de consolidar a transação.

Importante: O exemplo anterior não inclui quaisquer limites transacionais necessários, como begin e commit. Consulte o “Tutorial: Armazenando Informações de Pedido nas Entidades” na página 9 para obter mais informações.

Localizando uma Entidade

É possível localizar a entidade no cache do ObjectGrid com o método find fornecendo uma chave após o armazenamento da entidade no cache. Esse método não requer nenhum limite transacional, o que será útil em caso de semântica de somente leitura. O exemplo a seguir ilustra que apenas uma linha de código é suficiente para localizar a entidade.

```
Order foundOrder = (Order)em.find(Order.class, new Integer(123));
```

Removendo uma Entidade

O método remove, a exemplo do método persist, é uma operação transacional. O exemplo a seguir mostra o limite transacional ao chamar os métodos begin e commit.

```
em.getTransaction().begin();
Order foundOrder = (Order)em.find(Order.class, new Integer(123));
em.remove(foundOrder );
em.getTransaction().commit();
```

Primeiro, a entidade deve estar no estado managed antes que a remoção seja possível; o que pode ser conseguido chamando o método find dentro do limite transacional. Depois, chame o método remove na interface de EntityManager.

Invalidando uma Entidade

O método invalidate se comporta de maneira muito semelhante ao método remove, mas não chama nenhum plug-in do Utilitário de Carga. Use este método para remover entidades do ObjectGrid, mas para preservá-las no armazém de dados de backend.

```
em.getTransaction().begin();
Order foundOrder = (Order)em.find(Order.class, new Integer(123));
em.invalidate(foundOrder );
em.getTransaction().commit();
```

Primeiro, a entidade deve ser gerenciada antes que possa ser invalidada, o que pode ser conseguido chamando o método find dentro do limite transacional. Após chamar o método find, será possível chamar o método invalidate na interface de EntityManager.

Atualizando uma Entidade

O método update também é uma operação transacional. A entidade deve ser gerenciada antes que quaisquer atualizações possam ser aplicadas.

```
em.getTransaction().begin();
Order foundOrder = (Order)em.find(Order.class, new Integer(123));
foundOrder.date = new Date(); // update the date of the order
em.getTransaction().commit();
```

No exemplo precedente, o método persist não é chamado depois da atualização da entidade. A entidade é atualizada no cache do ObjectGrid quando a transação é confirmada.

Consultas e Filas de Consultas

Com o mecanismo de consulta flexível, é possível recuperar entidades utilizando a API do EntityManager. Crie consultas do tipo SELECT para uma entidade ou esquema baseado em Objeto, utilizando a linguagem de consulta do ObjectGrid. A interface de consulta explica em detalhes como é possível executar as consultas utilizando a API do EntityManager. Consulte a API de Query para obter mais informações sobre o uso de consultas.

Uma QueryQueue de entidade é uma estrutura de dados semelhante a uma fila associada com uma consulta de entidade. Ela seleciona todas as entidades que correspondem à condição WHERE no filtro de consulta e coloca as entidades do resultado em uma fila. Os clientes podem, então, recuperar iterativamente as entidades dessa fila. Consulte “Filas de Consulta da Entidade” na página 421 para obter mais informações.

Tarefas relacionadas:

Java "Tutorial: Armazenando Informações de Pedido nas Entidades" na página 9
Este tutorial do gerenciador de entidade mostra como utilizar o WebSphere eXtreme Scale para armazenar informações de pedido em um Web site. É possível criar um aplicativo Java Platform, Standard Edition 5 simples que utiliza um eXtreme Scale local e de memória. As entidades utilizam anotações e genéricos do Java SE 5.

"Colocando Diversos Objetos de Cache na Mesma Partição" na página 429
Ao definir dados relacionados em conjuntos de mapas que são organizados na mesma partição, você pode evitar a duplicação de dados e permitir o acesso a dados de baixa granularidade.

Referências relacionadas:

Java "Agente de Instrumentação de Desempenho da Entidade" na página 762
É possível melhorar o desempenho de entidades de acesso ao campo ativando o agente de instrumentação do WebSphere eXtreme Scale ao usar o Java Development Kit (JDK) Versão 6 ou posterior.

Java "Definindo um Esquema de Entidade" na página 391
Um ObjectGrid pode ter inúmeros esquemas de entidade lógicos. As entidades são definidas usando as classes Java anotadas, o XML ou uma combinação de classes XML e Java. Entidades definidas são registradas com um servidor eXtreme Scale e ligadas a BackingMaps, índices e outros plug-ins.

Java "Listeners de Entidade e Métodos de Retorno de Chamada"
Os aplicativos podem ser notificados quando o estado de uma entidade é alterado de estado para estado. Dois mecanismos de retorno de chamada existem para os eventos de mudança de estado: os métodos de retorno de chamada do ciclo de vida que são definidos em uma classe de entidade e são chamados sempre que o estado da entidade é alterado e os listeners de entidade, que são mais gerais porque o listener da entidade pode ser registrado em várias entidades.

Java "Exemplos do Listener de Entidade" na página 414
É possível gravar EntityListeners com base em seus requisitos. Veja a seguir vários scripts de exemplo.

Java "Interface EntityTransaction" na página 426
É possível utilizar a interface EntityTransaction para demarcar transações.

Informações relacionadas:

Java Amostra: Executando as Consultas em Paralelo Usando um ReduceGridAgent

Listeners de Entidade e Métodos de Retorno de Chamada: Java

Os aplicativos podem ser notificados quando o estado de uma entidade é alterado de estado para estado. Dois mecanismos de retorno de chamada existem para os eventos de mudança de estado: os métodos de retorno de chamada do ciclo de vida que são definidos em uma classe de entidade e são chamados sempre que o estado da entidade é alterado e os listeners de entidade, que são mais gerais porque o listener da entidade pode ser registrado em várias entidades.

Ciclo de Vida de uma Instância de Entidade

Uma instância de entidade apresenta os seguintes estados:

- **Novo**: Uma instância da entidade recentemente criada que não existe no cache do eXtreme Scale.
- **Gerenciado**: A instância da entidade existe no cacho do eXtreme Scale e é recuperada ou persistida utilizando o entity manager. É preciso que uma entidade esteja associada a uma transação ativa para ficar no estado gerenciado.
- **Separado**: A instância da entidade existe no cache do eXtreme Scale, mas não é mais associada com uma transação ativa.
- **Removido**: A instância da entidade é removida ou está planejada para ser removida do cache do eXtreme Scale quando ocorre o flush ou o commit da transação.
- **Invalidado**: A instância da entidade está invalidada ou está planejada para ser invalidada no cache do eXtreme Scale quando a ocorre o flush ou o commit da transação.

Quando as entidades são alteradas de estado para estado, é possível chamar métodos life cycle e callback.

As seções a seguir descrevem com mais detalhes os significados dos estados Novo, Gerenciado, Separado, Removido e Invalidado à medida que os estados se aplicam a uma entidade.

Métodos do Retorno de Chamada do Ciclo de Vida da Entidade

Os métodos de retorno de chamada do ciclo de vida da entidade podem ser definidos na classe de entidade e são chamados quando o estado da entidade é alterado. Estes métodos são úteis para validar campos de entidade e atualizar o estado temporário que normalmente não é persistido com a entidade. Os métodos de retorno de chamada do ciclo de vida da entidade também podem ser definidos nas classes que não estão usando as entidades. Tais classes são classes de listener da entidade, que podem ser associadas a vários tipos de entidades. Os métodos de retorno de chamada do ciclo de vida podem ser definidos usando anotações de metadados e um arquivo descritor XML de metadados da entidade:

- **Anotações**: métodos de retorno de chamada do ciclo de vida podem ser denotados usando as anotações PrePersist, PostPersist, PreRemove, PostRemove, PreUpdate, PostUpdate e PostLoad em uma classe de entidade.
- **Descritor XML de Entidade**: Os métodos de retorno de chamada do ciclo de vida podem ser descritos usando o XML quando as anotações não estão disponíveis.

Listeners de Entidade

Uma classe de listener de entidade é uma classe que não usa entidades que define um ou mais métodos de retorno de chamada do ciclo de vida da entidade. Os listeners de entidade são úteis para aplicativos de auditoria e criação de log com propósito geral. Listeners de entidade podem ser definidos utilizando anotações de metadados e um arquivo descritor XML de metadados da entidade:

- **Anotação**: A anotação EntityListeners pode ser utilizada para denotar uma ou mais classes do listener de entidade em uma classe de entidade. Se vários listeners de entidade estiverem definidos, a ordem na qual eles são chamados é determinada pela ordem na qual estão especificados na anotação EntityListeners.
- **Descritor XML da entidade**: O descritor XML pode ser utilizado como uma alternativa para especificar a ordem de chamada dos listeners de entidade ou para substituir a ordem que é especificada nas anotações de metadados.

Requisitos do Método de Retorno de Chamada

Qualquer subconjunto ou combinação de anotações pode ser especificado em uma classe de entidade ou uma classe de listener. Uma única classe não pode ter mais de um método de retorno de chamada de ciclo de vida para o mesmo evento de ciclo de vida. Entretanto, o mesmo método pode ser utilizado para vários eventos de retorno de chamada. A classe de listener de entidade deve ter um construtor no-arg público. Listeners de entidade não têm definição de estado. O ciclo de vida de um listener de entidade não é especificado. O eXtreme Scale não suporta herança de entidades, portanto, os métodos callback podem ser definidos apenas na classe de entidade, mas não na superclasse.

Assinatura de Método callback

Os métodos de retorno de chamada de ciclo de vida da entidade podem ser definidos em uma classe de listener de entidade, diretamente em uma classe de entidade, ou ambos. Os métodos de retorno de chamada do ciclo de vida da entidade podem ser definidos usando as anotações de metadados e o descritor XML da entidade. As anotações utilizadas para métodos callback de entidade e na classe de listener da entidade são as mesmas. As assinaturas dos métodos callback são diferentes quando definidas em uma classe de entidade versus uma classe de listener de entidade. Os métodos callback definidos em uma classe de entidade ou superclasse mapeada possuem a seguinte assinatura:

```
void <METHOD>()
```

Os métodos callback que são definidos em uma classe de listener de entidade possuem a seguinte assinatura:

```
void <METHOD>(Object)
```

O argumento Object é a instância da entidade para a qual o método de retorno de chamada é chamado. O argumento Object pode ser declarado como um objeto java.lang.Object ou o tipo de entidade real.

Os métodos callback podem ter nível de acesso público, privado, protegido ou de pacote, mas não devem ser estáticos ou finais.

As seguintes anotações são definidas para designar os métodos de retorno de chamada de eventos do ciclo de vida dos tipos correspondentes:

- com.ibm.websphere.projector.annotations.PrePersist
- com.ibm.websphere.projector.annotations.PostPersist
- com.ibm.websphere.projector.annotations.PreRemove
- com.ibm.websphere.projector.annotations.PostRemove
- com.ibm.websphere.projector.annotations.PreUpdate
- com.ibm.websphere.projector.annotations.PostUpdate
- com.ibm.websphere.projector.annotations.PostLoad

Consulte a Documentação da API para obter mais detalhes. Cada anotação possui um atributo XML equivalente definido no arquivo descritor XML de metadados de entidade.

Semântica de Método de Retorno de Chamada do Ciclo de Vida

Cada um dos métodos de retorno de chamada do ciclo de vida diferentes possui um propósito diferente e é chamado nas diferentes fases do ciclo de entidade:

PrePersist
Chamado para uma entidade antes da entidade ter sido persistida para o armazém, o que inclui entidades que foram persistidas devido a uma operação em cascata. Este método é chamado no encadeamento da operação EntityManager.persist.

PostPersist
Chamado para uma entidade após a entidade ter sido persistida para o armazém, o que inclui entidades que foram persistidas devido a uma operação em cascata. Este método é chamado no encadeamento da operação EntityManager.persist. Ele é chamado após o EntityManager.flush ou EntityManager.commit ser chamado.

PreRemove
Chamado para um entidade antes da entidade ter sido removida, o que inclui entidades que foram removidas devido a uma operação em cascata. Este método é chamado no encadeamento da operação EntityManager.remove.

PostRemove
Chamado para uma entidade após a entidade ter sido removida, o que inclui entidades que foram removidas devido a uma operação em cascata. Este método é chamado no encadeamento da operação EntityManager.remove. Ele é chamado após o EntityManager.flush ou EntityManager.commit ser chamado.

PreUpdate
Chamado para uma entidade antes da entidade ter sido atualizada no armazém. Este método é chamado no encadeamento da operação flush ou commit da transação.

PostUpdate
Chamado para uma entidade após a entidade ter sido atualizada no armazém. Este método é chamado no encadeamento da operação flush ou commit da transação.

PostLoad
Chamado para uma entidade após a entidade ter sido carregada do armazém, o que inclui quaisquer entidades que são carregadas através de uma associação. Este método é chamado no encadeamento da operação de carregamento, tal como EntityManager.find ou uma consulta.

Métodos de Retorno de Chamada do Ciclo de Vida Duplicados

Se vários métodos de retorno de chamada forem definidos para um evento de ciclo de vida da entidade, a ordem de chamada desses métodos será a seguinte:

1. **Métodos de retorno de chamada do ciclo de vida definidos nos listeners de entidade**: Os métodos de retorno de chamada do ciclo de vida que são definidos nas classes de listener de entidade para uma classe de entidade são chamados na mesma ordem que a especificação das classes do listener de entidade na anotação EntityListeners ou no descritor XML.
2. **Superclasse do listener**: Os métodos callback definidos na superclasse do listener de entidade são chamados antes dos filhos.
3. **Métodos do ciclo de vida de entidade**: WebSphere eXtreme Scale não suportam herança de entidade, portanto, os métodos do ciclo de vida da entidade podem ser definidos apenas na classe de entidade.

Exceções

Os métodos retorno de chamada do ciclo de vida podem resultar em exceções de tempo de execução. Se um método de retorno de chamada do ciclo de vida resulta em uma exceção de tempo de execução em uma transação, a transação é recuperada. Nenhum método de retorno de chamada de ciclo de vida adicional é chamado depois que ocorre uma exceção de tempo de execução.

Conceitos relacionados:

Java "Ajustando o Desempenho da Interface EntityManager" na página 760
A interface EntityManager separa aplicativos do estado de suspensão no armazenamento de dados da grade do servidor.

Java "Objetos de Armazenamento em Cache e seus Relacionamentos (API EntityManager)" na página 388
A maioria dos produtos de cache utiliza APIs baseadas em mapa para armazenar dados como pares de chave-valor. A API ObjectMap e o cache dinâmico no WebSphere Application Server, entre outros, usam essa abordagem. Entretanto, APIs baseadas em mapas têm limitações. A API EntityManager simplifica a interação com a grade de dados ao fornecer uma maneira fácil de declarar e interagir com um gráfico complexo de objetos relacionados.

Java "Entity Manager em um Ambiente Distribuído" na página 401
É possível usar a API EntityManager com um ObjectGrid local ou em um ambiente distribuído do eXtreme Scale . A principal diferença é como você se conecta a esse ambiente remoto. Após você estabelecer uma conexão, não existe diferença entre o uso de um objeto Session ou uma API do EntityManager.

Java "Interagindo com EntityManager" na página 405
Geralmente os aplicativos primeiro obtêm uma referência do ObjectGrid e, depois, uma Sessão dessa referência para cada encadeamento. As sessões não podem ser compartilhadas entre encadeamentos. Um método extra em Session, o método getEntityManager, está disponível. Este método retorna uma referência para um gerenciador de entidades para uso para este encadeamento. A interface de EntityManager pode substituir as interfaces de Session e ObjectMap para todos os aplicativos. É possível utilizar essas APIs de EntityManager se o cliente tiver acesso às classes de entidade definidas.

Java "Suporte ao Plano de Carregamento do EntityManager" na página 417
Um FetchPlan é a estratégia que o gerenciador de entidade usa para recuperar objetos associados se o aplicativo precisar acessar relacionamentos.

Java "Filas de Consulta da Entidade" na página 421
Filas de consulte permitem que aplicativos criem uma fila qualificada por uma consulta no lado do servidor ou eXtreme Scale local sobre uma entidade. As entidades do resultado da consulta são armazenadas nesta fila. Atualmente, a fila de consulta é suportada apenas em um mapa que está utilizando a estratégia de bloqueio pessimista.

Java "Roteando os Objetos de Cache para a Mesma Partição" na página 432
Quando a configuração do eXtreme Scale usa a estratégia de colocação de partição fixa, ela dependerá do hash da chave para uma partição inserir, obter, atualizar ou remover o valor. O método hashCode é chamado na chave e ele deverá ser bem definido se uma chave customizada for criada. No entanto, outra opção é usar a interface PartitionableKey. Com a interface PartitionableKey, será possível usar um objeto diferente da chave para efetuar hash de uma partição.

Tarefas relacionadas:

Java "Tutorial: Armazenando Informações de Pedido nas Entidades" na página 9
Este tutorial do gerenciador de entidade mostra como utilizar o WebSphere eXtreme Scale para armazenar informações de pedido em um Web site. É possível criar um aplicativo Java Platform, Standard Edition 5 simples que utiliza um eXtreme Scale local e de memória. As entidades utilizam anotações e genéricos do Java SE 5.

"Colocando Diversos Objetos de Cache na Mesma Partição" na página 429

Ao definir dados relacionados em conjuntos de mapas que são organizados na mesma partição, você pode evitar a duplicação de dados e permitir o acesso a dados de baixa granularidade.

Informações relacionadas:

Java Amostra: Executando as Consultas em Paralelo Usando um ReduceGridAgent

Exemplos do Listener de Entidade: Java

É possível gravar EntityListeners com base em seus requisitos. Veja a seguir vários scripts de exemplo.

Exemplo de EntityListeners Utilizando Anotações

O exemplo a seguir mostra as chamadas de método de retorno de chamada do ciclo de vida e a ordem das chamadas. Assuma que existe uma classe de entidade Employee e dois listeners de entidade: EmployeeListener e EmployeeListener2.

```
@Entity
@EntityListeners({EmployeeListener.class, EmployeeListener2.class})
public class Employee {
    @PrePersist
    public void checkEmployeeID() {
        ....
    }
}

public class EmployeeListener {
    @PrePersist
    public void onEmployeePrePersist(Employee e) {
        ....
    }
}

public class PersonListener {
    @PrePersist
    public void onPersonPrePersist(Object person) {
        ....
    }
}

public class EmployeeListener2 extends PersonListener {
    @PrePersist
    public void onEmployeePrePersist2(Object employee) {
        ....
    }
}
```

Se um evento PrePersist ocorre em uma instância Employee, os seguintes métodos são chamados em ordem:

1. Método onEmployeePrePersist
2. Método onPersonPrePersist
3. Método onEmployeePrePersist2
4. Método checkEmployeeID

Exemplo de Listeners de Entidade Utilizando XML

O exemplo a seguir mostra como configurar um listener de entidade em uma entidade utilizando o arquivo XML descritor de entidade:

```
<entity
    class-name="com.ibm.websphere.objectgrid.sample.Employee"
    name="Employee" access="FIELD">
    <attributes>
        <id name="id" />
        <basic name="value" />
    </attributes>
    <entity-listeners>
        <entity-listener
            class-name="com.ibm.websphere.objectgrid.sample.EmployeeListener">
            <pre-persist method-name="onListenerPrePersist" />
            <post-persist method-name="onListenerPostPersist" />
        </entity-listener>
    </entity-listeners>
    <pre-persist method-name="checkEmployeeID" />
</entity>
```

A entidade Employee é configurada com uma classe de listener de entidade com.ibm.websphere.objectgrid.sample.EmployeeListener, que possui dois métodos de retorno de chamada de ciclo de vida definidos. O método onListenerPrePersist é para o evento PrePersist e o método onListenerPostPersist é para o evento PostPersist. Além disso, o método checkEmployeeID na classe Employee é configurado para atender o evento PrePersist.

Conceitos relacionados:

Java "Ajustando o Desempenho da Interface EntityManager" na página 760
A interface EntityManager separa aplicativos do estado de suspensão no armazenamento de dados da grade do servidor.

Java "Objetos de Armazenamento em Cache e seus Relacionamentos (API EntityManager)" na página 388
A maioria dos produtos de cache utiliza APIs baseadas em mapa para armazenar dados como pares de chave-valor. A API ObjectMap e o cache dinâmico no WebSphere Application Server, entre outros, usam essa abordagem. Entretanto, APIs baseadas em mapas têm limitações. A API EntityManager simplifica a interação com a grade de dados ao fornecer uma maneira fácil de declarar e interagir com um gráfico complexo de objetos relacionados.

Java "Entity Manager em um Ambiente Distribuído" na página 401
É possível usar a API EntityManager com um ObjectGrid local ou em um ambiente distribuído do eXtreme Scale . A principal diferença é como você se conecta a esse ambiente remoto. Após você estabelecer uma conexão, não existe diferença entre o uso de um objeto Session ou uma API do EntityManager.

Java "Interagindo com EntityManager" na página 405
Geralmente os aplicativos primeiro obtêm uma referência do ObjectGrid e, depois, uma Sessão dessa referência para cada encadeamento. As sessões não podem ser compartilhadas entre encadeamentos. Um método extra em Session, o método getEntityManager, está disponível. Este método retorna uma referência para um gerenciador de entidades para uso para este encadeamento. A interface de EntityManager pode substituir as interfaces de Session e ObjectMap para todos os aplicativos. É possível utilizar essas APIs de EntityManager se o cliente tiver acesso às classes de entidade definidas.

Java "Suporte ao Plano de Carregamento do EntityManager" na página 417
Um FetchPlan é a estratégia que o gerenciador de entidade usa para recuperar objetos associados se o aplicativo precisar acessar relacionamentos.

Java "Filas de Consulta da Entidade" na página 421
Filas de consulte permitem que aplicativos criem uma fila qualificada por uma consulta no lado do servidor ou eXtreme Scale local sobre uma entidade. As entidades do resultado da consulta são armazenadas nesta fila. Atualmente, a fila de consulta é suportada apenas em um mapa que está utilizando a estratégia de bloqueio pessimista.

Java "Roteando os Objetos de Cache para a Mesma Partição" na página 432
Quando a configuração do eXtreme Scale usa a estratégia de colocação de partição fixa, ela dependerá do hash da chave para uma partição inserir, obter, atualizar ou remover o valor. O método hashCode é chamado na chave e ele deverá ser bem definido se uma chave customizada for criada. No entanto, outra opção é usar a interface PartitionableKey. Com a interface PartitionableKey, será possível usar um objeto diferente da chave para efetuar hash de uma partição.

Tarefas relacionadas:

Java "Tutorial: Armazenando Informações de Pedido nas Entidades" na página 9
Este tutorial do gerenciador de entidade mostra como utilizar o WebSphere eXtreme Scale para armazenar informações de pedido em um Web site. É possível criar um aplicativo Java Platform, Standard Edition 5 simples que utiliza um eXtreme Scale local e de memória. As entidades utilizam anotações e genéricos do Java SE 5.

"Colocando Diversos Objetos de Cache na Mesma Partição" na página 429

Ao definir dados relacionados em conjuntos de mapas que são organizados na mesma partição, você pode evitar a duplicação de dados e permitir o acesso a dados de baixa granularidade.

Informações relacionadas:

Java Amostra: Executando as Consultas em Paralelo Usando um ReduceGridAgent

Suporte ao Plano de Carregamento do EntityManager: Java

Um FetchPlan é a estratégia que o gerenciador de entidade usa para recuperar objetos associados se o aplicativo precisar acessar relacionamentos.

Exemplo

Suponha, por exemplo, que seu aplicativo tenha duas entidades: Department e Employee. O relacionamento entre a entidade Department e a entidade Employee é um relacionamento bidirecional um-para-muitos: Um departamento tem vários funcionários, e um funcionário pertence a um único departamento. Como na maioria das vezes, quando é feita uma busca pela entidade Department, seus Employees provavelmente são buscados, e o tipo de busca desse relacionamento um-para-muitos é configurado como EAGER.

Aqui está um fragmento da classe Department.

```
 @Entity
public class Department {

    @Id
    private String deptId;

    @Basic
    String deptName;

  @OneToMany(fetch = FetchType.EAGER, mappedBy="department", cascade
= {CascadeType.PERSIST})
  public Collection<Employee> employees;

}
```

Em um ambiente distribuído, quando um aplicativo chama `em.find(Department.class, "dept1")` para localizar uma entidade Department com a chave "dept1", essa operação find obtém a entidade Department e todas as suas relações eager-fetched. No caso do fragmento anterior, elas são todos os funcionários do departamento "dept1".

Antes do WebSphere eXtreme Scale 6.1.0.5, a recuperação de uma entidade Department e N entidades Employee incorria em N+1 trips de cliente-servidor porque o cliente recuperava uma entidade para um trip de cliente-servidor. É possível melhorar o desempenho se você recuperar essas N+1 entidades em um trip.

Plano de Carregamento

Um plano de carregamento pode ser utilizado para customizar a forma como você executa um carregamento ansioso de relacionamentos customizando a profundidade máxima dos relacionamentos. A profundidade da busca substitui relações eager maiores do que a profundidade especificada para relações lazy. Por padrão, a profundidade da busca é a profundidade máxima da busca. Isso significa que relacionamentos eager de todos os níveis navegáveis como eager a partir da entidade raiz serão buscados. Um relacionamento EAGER é navegável como eager

a partir de uma entidade raiz se, e apenas se, todas as relações começando da entidade raiz para ela forem configuradas como eager-fetched.

No exemplo anterior, a entidade Employee é navegável como eager a partir da entidade Department porque o relacionamento Department-Employee é configurado como eager-fetched.

Se a entidade Employee tiver outro relacionamento eager com uma entidade Address, por exemplo, a entidade Address também será navegável como eager a partir da entidade Department. Entretanto, se os relacionamentos Department-Employee foram configurados como lazy-fetch, a entidade Address não será navegável como eager a partir da entidade Department, pois o relacionamento Department-Employee quebra a cadeia de eager fetch.

Um objeto Plano de Carregamento pode ser recuperado da instância EntityManager. O aplicativo pode utilizar o método setMaxFetchDepth para alterar a profundidade máxima da busca.

Um plano de carregamento é associado a uma instância EntityManager. O plano de carregamento aplica-se a qualquer operação de busca, mais especificamente da seguinte forma.

- Operações EntityManager `find(Class class, Object key)` e `findForUpdate(Class class, Object key)`
- Operações Query
- Operações QueryQueue

O objeto Plano de Carregamento é mutável. Após ser alterado, o valor será aplicado às operações de busca executadas posteriormente.

Um plano de carregamento é importante para uma implementação distribuída porque decide se as entidades de relacionamento eager-fetched são recuperadas com a entidade raiz em um trip de cliente/servidor ou em mais de uma.

Continuando com o exemplo anterior, considere que o plano de carregamento tenha profundidade máxima configurada como infinito. Nesse caso, quando o aplicativo chama `em.find(Department.class, "dept1")` para localizar Department, essa operação find obtém uma entidade Department e N entidades Employee em um trip de cliente/servidor. Entretanto, para um plano de carregamento com profundidade de busca máxima configurada como zero, apenas o objeto Department será recuperado do servidor, enquanto as entidades Employee são recuperadas do servidor apenas quando a coleta de Employees do objeto Department é acessada.

Planos de Carregamento Diferentes

Você tem diferentes planos de carregamentos baseados em seus requisitos, explicados nas seguintes seções.

Impacto em uma grade distribuída

- *Plano de carregamento de profundidade infinita:* Um Plano de Carregamento de profundidade infinita tem sua profundidade de busca máxima configurada como `FetchPlan.DEPTH_INFINITE`.

  Em um ambiente de cliente/servidor, se um plano de carregamento de profundidade infinita for utilizado, todas as relações navegáveis como eager a partir da entidade raiz serão recuperadas em um trip de cliente/servidor.

Exemplo: Se o aplicativo estiver interessado em todas as entidades Address de todos os employees de um determinado Department, ele utilizará um plano de carregamento de profundidade infinita para recuperar todas as entidades Address associadas. O código a seguir incorre apenas em um trip de cliente/servidor.

```
em.getFetchPlan().setMaxFetchDepth(FetchPlan.DEPTH_INFINITE);

tran.begin();
Department dept = (Department) em.find(Department.class, "dept1");
// do something with Address object.
for (Employee e: dept.employees) {
    for (Address addr: e.addresses) {
    // do something with addresses.
    }
}
tran.commit();
```

- *Plano de carregamento com profundidade zero:* Um plano de carregamento com profundidade zero tem sua profundidade máxima de busca configurada como 0.

  Em um ambiente de cliente/servidor, se um plano de carregamento com profundidade zero for utilizado, apenas a entidade raiz será recuperada no primeiro trip de cliente/servidor. Todos os relacionamentos eager são tratados como se fossem lazy.

  Exemplo: Neste exemplo, o aplicativo só está interessado no atributo da entidade Department. Ele não precisa acessar seus employees, portanto, o aplicativo configura a profundidade do plano de carregamento como 0.

  ```
  Session session = objectGrid.getSession();
  EntityManager em = session.getEntityManager();
  EntityTransaction tran = em.getTransaction();
  em.getFetchPlan().setMaxFetchDepth(0);

  tran.begin();
  Department dept = (Department) em.find(Department.class, "dept1");
  // do something with dept object.
  tran.commit();
  ```

- *Plano de carregamento com espessura k* :

  Um plano de carregamento de espessura *k*- tem sua espessura máxima de carregamento configurada para *k*.

  Em um ambiente eXtreme Scale de cliente/servidor, se um plano de carregamento de profundidade *k*- for utilizado, todos os relacionamentos navegáveis como eager a partir da entidade raiz dentro de *k* etapas serão recuperados no primeiro trip de cliente/servidor.

  O plano de carregamento de profundidade infinita (*k* = infinito) e o plano de carregamento de profundidade zero (*k* = 0) são apenas dois exemplos do plano de carregamento de profundidade *k*-.

  Para continuar expandindo o exemplo anterior, suponha que exista outro relacionamento eager da entidade Employee com a entidade Address. Se o plano de carregamento tiver profundidade de busca máxima configurada como 1, a operação `em.find(Department.class, "dept1")` irá recuperar a entidade Department e todas as entidades Employee em um trip de cliente/servidor. Entretanto, as entidades Address não serão recuperadas porque não são navegáveis como eager para a entidade Department dentro de 1 etapa, mas sim de 2 etapas.

  Se você utilizar um plano de carregamento com profundidade configurada como 2, a operação `em.find(Department.class, "dept1")` irá recuperar a entidade Department, todas as suas entidades Employee e todas as entidades Address associadas às entidades Employee em um trip de cliente/servidor.

  Dica: O plano de carregamento padrão tem profundidade de busca máxima configurada como infinito, portanto, o comportamento padrão de uma operação

fetch pode mudar. Todos os relacionamentos navegáveis como eager a partir da entidade raiz são recuperados. Em vez de várias viagens, agora a operação fetch incorre apenas um trip de cliente/servidor com o plano de carregamento padrão. Para manter as configurações para o produto da versão anterior, configure a profundidade da busca como 0.

- *Plano de carregamento utilizado na consulta:*

  Se você executar uma consulta de entidade, também será possível utilizar um plano de carregamento para customizar a recuperação de relacionamento.

  Por exemplo, o resultado da consulta `SELECT d FROM Department d WHERE "d.deptName='Department'"` tem um relacionamento com a entidade Department. Observe que a profundidade do plano de carregamento começa com a associação do resultado da consulta: nesse caso, a entidade Department, não o resultado da consulta em si. Ou seja, a entidade Department está no nível de profundidade de busca 0. Entretanto, um plano de carregamento com profundidade de busca máxima de 1 irá recuperar a entidade Department e suas entidades Employee em um trip de cliente/servidor.

  Exemplo: Neste exemplo, a profundidade do plano de carregamento está configurada como 1, portanto, a entidade Department e suas entidades Employee são recuperadas em um trip de cliente/servidor, mas as entidades Address não serão recuperadas no mesmo trip.

Importante: Se um relacionamento for solicitado, utilizando configuração ou anotação OrderBy, ele será considerado um relacionamento eager, mesmo que esteja configurado como lazy-fetch.

Considerações de Desempenho em um Ambiente Distribuído

Por padrão, todos os relacionamentos navegáveis como eager a partir da entidade raiz serão recuperados em um trip de cliente/servidor. Isso pode melhorar o desempenho se todos os relacionamentos forem utilizados. No entanto, em certos cenários de uso, nem todos os relacionamentos navegáveis como eager a partir da entidade raiz são utilizados, portanto eles incorrem em gasto adicional de tempo de execução e em gasto adicional de largura de banda ao recuperar essas entidades não utilizadas.

Para esses casos, o aplicativo pode configurar a profundidade de busca máxima para um número pequeno para diminuir a profundidade de entidades a serem recuperadas, tornando lazy todas as relações eager após essa profundidade específica. Essa configuração pode melhorar o desempenho.

Continuando com o exemplo Department-Employee-Address anterior, por padrão, todas as entidades Address associadas a employees de Department "dept1" serão recuperadas quando `em.find(Department.class, "dept1")` for chamado. Se o aplicativo não utilizar entidades Address, ele poderá configurar a profundidade máxima da busca como 1, portanto as entidades Address não serão recuperadas com a entidade Department.

Tarefas relacionadas:

Java "Tutorial: Armazenando Informações de Pedido nas Entidades" na página 9
Este tutorial do gerenciador de entidade mostra como utilizar o WebSphere eXtreme Scale para armazenar informações de pedido em um Web site. É possível criar um aplicativo Java Platform, Standard Edition 5 simples que utiliza um eXtreme Scale local e de memória. As entidades utilizam anotações e genéricos do Java SE 5.

"Colocando Diversos Objetos de Cache na Mesma Partição" na página 429
Ao definir dados relacionados em conjuntos de mapas que são organizados na mesma partição, você pode evitar a duplicação de dados e permitir o acesso a dados de baixa granularidade.

Referências relacionadas:

Java "Agente de Instrumentação de Desempenho da Entidade" na página 762
É possível melhorar o desempenho de entidades de acesso ao campo ativando o agente de instrumentação do WebSphere eXtreme Scale ao usar o Java Development Kit (JDK) Versão 6 ou posterior.

Java "Definindo um Esquema de Entidade" na página 391
Um ObjectGrid pode ter inúmeros esquemas de entidade lógicos. As entidades são definidas usando as classes Java anotadas, o XML ou uma combinação de classes XML e Java. Entidades definidas são registradas com um servidor eXtreme Scale e ligadas a BackingMaps, índices e outros plug-ins.

Java "Listeners de Entidade e Métodos de Retorno de Chamada" na página 408
Os aplicativos podem ser notificados quando o estado de uma entidade é alterado de estado para estado. Dois mecanismos de retorno de chamada existem para os eventos de mudança de estado: os métodos de retorno de chamada do ciclo de vida que são definidos em uma classe de entidade e são chamados sempre que o estado da entidade é alterado e os listeners de entidade, que são mais gerais porque o listener da entidade pode ser registrado em várias entidades.

Java "Exemplos do Listener de Entidade" na página 414
É possível gravar EntityListeners com base em seus requisitos. Veja a seguir vários scripts de exemplo.

Java "Interface EntityTransaction" na página 426
É possível utilizar a interface EntityTransaction para demarcar transações.

Informações relacionadas:

Java Amostra: Executando as Consultas em Paralelo Usando um ReduceGridAgent

Filas de Consulta da Entidade: Java

Filas de consulte permitem que aplicativos criem uma fila qualificada por uma consulta no lado do servidor ou eXtreme Scale local sobre uma entidade. As entidades do resultado da consulta são armazenadas nesta fila. Atualmente, a fila de consulta é suportada apenas em um mapa que está utilizando a estratégia de bloqueio pessimista.

Uma fila de consulta é compartilhada por várias transações e clientes. Após a fila de consulta ficar vazia, a consulta da entidade associada a esta fila é executada novamente e novos resultados são incluídos na fila. Uma fila de consulta é identificada exclusivamente pela cadeia e os parâmetro de consulta da entidade.

Há apenas uma instância para cada fila de consulta exclusiva em uma instância do ObjectGrid. Consulte a documentação da API do EntityManager para obter mais informações.

Exemplo de Fila de Consulta

O exemplo a seguir mostra como a fila de consulta pode ser utilizada.

```
/**
 * Get a unassigned question type task
 */
private void getUnassignedQuestionTask() throws Exception {
    EntityManager em = og.getSession().getEntityManager();
    EntityTransaction tran = em.getTransaction();

    QueryQueue queue = em.createQueryQueue("SELECT t FROM Task t
    WHERE t.type=?1 AND t.status=?2", Task.class);
    queue.setParameter(1, new Integer(Task.TYPE_QUESTION));
    queue.setParameter(2, new Integer(Task.STATUS_UNASSIGNED));

    tran.begin();
    Task nextTask = (Task) queue.getNextEntity(10000);
    System.out.println("next task is " + nextTask);
    if (nextTask != null) {
        assignTask(em, nextTask);
    }
    tran.commit();
}
```

O exemplo anterior primeiro cria um QueryQueue com uma cadeia de consulta de entidade, "SELECT t FROM Task t WHERE t.type=?1 AND t.status=?2". Depois ele configura os parâmetros para o objeto QueryQueue. Esta fila de consulta representa todas as tarefas "não-designadas" do tipo "questão". O objeto QueryQueue é muito semelhante a um objeto Query da entidade.

Após o QueryQueue ser criado, uma transação de entidade é iniciada e o método getNextEntity é chamado, que recupera a próxima entidade disponível sem um valor de tempo limite de 10 segundos. Após a entidade ser recuperada, ela é processada no método assignTask. O assignTask modifica a instância da entidade Task e altera o status para "designado" que efetivamente a remove da fila já que não corresponde mais ao filtro do QueryQueue. Uma vez designada, ocorre o commit da transação.

A partir deste exemplo, é possível visualizar uma fila de consulta que é semelhante a uma consulta de entidade. Entretanto, elas diferem nas seguintes maneiras:

1. As entidades na fila de consulta podem ser recuperadas de uma maneira iterativa. O aplicativo de usuário decide o número de entidades a ser recuperado. Por exemplo, se QueryQueue.getNextEntity(timeout) é utilizado, apenas uma entidade é recuperada e se QueryQueue.getNextEntities(5, timeout) é utilizado, 5 entidades são recuperadas. Em um ambiente distribuído, o número de entidades decide diretamente o número de bytes a ser transferido do servidor para o cliente.
2. Quando uma entidade é recuperada da fila de consulta, um bloqueio U é colocado na entidade, assim nenhuma outra transação pode acessá-la.

Recuperar Entidades em um Loop

É possível recuperar entidades em um loop. A seguir está um exemplo que ilustra como obter todas as tarefas não-designadas do tipo question concluídas.

```
/**
 * Get all unassigned question type tasks
 */
private void getAllUnassignedQuestionTask() throws Exception {
    EntityManager em = og.getSession().getEntityManager();
    EntityTransaction tran = em.getTransaction();

    QueryQueue queue = em.createQueryQueue("SELECT t FROM Task t WHERE
   t.type=?1 AND t.status=?2", Task.class);
    queue.setParameter(1, new Integer(Task.TYPE_QUESTION));
    queue.setParameter(2, new Integer(Task.STATUS_UNASSIGNED));

    Task nextTask = null;

    do {
        tran.begin();
        nextTask = (Task) queue.getNextEntity(10000);
        if (nextTask != null) {
            System.out.println("next task is " + nextTask);
        }
        tran.commit();
    } while (nextTask != null);
}
```

Se houver 10 tarefas não-designadas do tipo question no mapa de entidade, é possível esperar que você terá 10 entidades impressas no console. Entretanto, se este exemplo for executado, visualizará que o programa nunca sai, o que pode ser contrário ao que você assumiu.

Quando uma fila de consulta é criada e o getNextEntity é chamado, a consulta de entidade associada com a fila é executada e os 10 resultados são colocadas na fila. Quando o getNextEntity é chamado, uma entidade é retirada da fila. Após 10 chamadas do getNextEntity serem executadas, a fila fica vazia. A consulta da entidade será novamente executada automaticamente. Como estas 10 entidades ainda existem e correspondem aos critérios de filtro da fila de consulta, elas são colocadas na fila novamente.

Se a linha a seguir for incluída após a instrução println(), você verá apenas 10 entidades impressas.

```
em.remove(nextTask);
```

Para obter informações sobre o uso de SessionHandle com QueryQueue em uma implementação de posicionamento por contêiner, leia sobre Integração de SessionHandle.

Filas de Consulta Implementadas em todas as Partições

Em um eXtreme Scale distribuído, uma fila de consulta pode ser criada para uma partição ou todas as partições. Se uma fila de consulta é criada para todas as partições, haverá uma instância de fila de consulta em cada partição.

Quando um cliente tenta obter a próxima entidade utilizando o método QueryQueue.getNextEntity ou QueryQueue.getNextEntities, o cliente envia um pedido para uma das partições. Um cliente envia pedidos de peek e pin para o servidor:

- Com um pedido de peek, o cliente envia um pedido para uma partição e o servidor retorna imediatamente. Se houver uma entidade na fila, o servidor

envia uma resposta com a entidade; se não houver, o servidor envia uma resposta sem nenhuma entidade. Em qualquer um dos casos, o servidor retornará imediatamente.
- Com um pedido de pin, o cliente envia um pedido para uma partição e o servidor aguarda até que uma entidade esteja disponível. Se houver uma entidade na fila, o servidor envia uma resposta com a entidade imediatamente; se não houver, o servidor aguarda na fila até que uma entidade esteja disponível ou o pedido atinja o tempo limite.

A seguir, está um exemplo de como uma entidade é recuperada para uma fila de consulta que é implementada em todas as partições (n):

1. Quando um método QueryQueue.getNextEntity ou QueryQueue.getNextEntities é chamado, o cliente seleciona um número de partição aleatório de 0 a n-1.
2. O cliente envia o pedido de peek para a partição aleatória.
   - Se uma entidade estiver disponível, o método QueryQueue.getNextEntity ou QueryQueue.getNextEntities sai retornando a entidade.
   - Se uma entidade não estiver disponível e não for a última partição não-visitada, o cliente envia um pedido de peek para a próxima partição.
   - Se uma entidade não estiver disponível e for a última partição não-visitada, o cliente envia um pedido de pin.
   - Se o pedido de pin para a última partição atingir o tempo limite e ainda não houver dados disponíveis, o cliente fará um último esforço enviado o pedido de peek para todas as partições serialmente um ciclo a mais. Portanto, se alguma entidade estiver disponível nas partições anteriores, o cliente estará a obtê-la.

Suporte a Entidade e Não-entidade de Subconjunto

A seguir está o método para criar um objeto QueryQueue no entity manager:

```
public QueryQueue createQueryQueue(String qlString, Class entityClass);
```

O resultado na fila de consulta deve ser projetado para o objeto definido pelo segundo parâmetro para o método, Class entityClass.

Se este parâmetro for especificado, a classe deve ter o mesmo nome da entidade conforme especificado na cadeia de consultas. Isto é útil se você desejar projetar uma entidade em uma entidade de subconjunto. Se um valor nulo é utilizado com a classe de entidade, então, o resultado não será projetado. O valor armazenado no mapa estará em um formato de tupla da entidade.

Colisão de Chaves do Lado do Cliente

No ambiente eXtreme Scale distribuído, a fila de consulta é suportada apenas para mapas do eXtreme Scale com o modo de bloqueio pessimista. Portanto, não há um cache local no lado do cliente. Entretanto, um cliente poderia ter dados (chave e valor) no mapa transacional. Isto potencialmente poderia levar a uma colisão de chaves quando uma entidade recuperada do servidor compartilha a mesma chave que uma entrada já no mapa da transação.

Quando ocorre uma colisão de chaves, o tempo de execução do cliente do eXtreme Scale utiliza a seguinte regra para emitir uma exceção ou substituir os dados silenciosamente.

1. Se a chave colidida for a chave da entidade especificada na consulta de entidade associada com a fila de consulta, então, uma exceção é lançada. Neste caso, ocorre o rollback da transação e o bloqueio U nesta entidade será liberado no lado do servidor.
2. Caso contrário, se a chave colidida for a chave de uma associação de entidade, os dados no mapa transacional serão substituídos sem aviso.

A colisão de chaves acontece apenas quando há dados no mapa transacional. Em outras palavras, isto ocorre apenas quando uma chamada getNextEntity ou getNextEntities é chamada em uma transação que já foi suja (um novo dado foi inserido ou um dado foi atualizado). Se um aplicativo não deseja que aconteça uma colisão de chaves, ele deve sempre chamar getNextEntity ou getNextEntities em uma transação que não foi suja.

Falhas do Cliente

Após um cliente enviar um pedido getNextEntity ou getNextEntities para o servidor, o cliente poderia falhar da seguinte maneira:

1. O cliente envia um pedido para o servidor e, então, fica inativo.
2. O cliente obtém uma ou mais entidades do servidor e, então, fica inativo.

No primeiro caso, o servidor descobre que o cliente está ficando inativo quando ele tenta enviar de volta a resposta para o cliente. No segundo caso, quando o cliente obtém uma ou mais entidades do servidor, um bloqueio X é colocado nestas entidades. Se o cliente fica inativo, a transação eventualmente atingirá o tempo limite e o bloqueio X será liberado.

Consulta com a cláusula ORDER BY

Geralmente, as filas de consulta não honram a cláusula ORDER BY. Se você chamar getNextEntity ou getNextEntities a partir da fila de consulta, não há garantia de que as entidades serão retornadas de acordo com a ordem. O motivo é que as entidades não podem ser ordenadas entre partições. No caso em que a fila de consulta é implementada em todas as partições, quando uma chamada getNextEntity ou getNextEntities é executada, uma partição aleatória é selecionada para processar o pedido. Portanto, a ordem não é garantida.

ORDER BY será honrado se uma fila de consulta for implementada em uma partição única.

Para obter mais informações, consulte “API de Consulta EntityManager” na página 448.

Uma Chamada Por Transação

Cada chamada QueryQueue.getNextEntity ou QueryQueue.getNextEntities recupera entidades correspondentes de uma partição aleatória. Os aplicativos devem chamar exatamente uma QueryQueue.getNextEntity ou QueryQueue.getNextEntities em uma transação. Caso contrário, o eXtreme Scale pode encerrar o toque a entidades de várias partições, fazendo com que uma exceção seja lançada na hora da confirmação.

Tarefas relacionadas:

Java "Tutorial: Armazenando Informações de Pedido nas Entidades" na página 9
Este tutorial do gerenciador de entidade mostra como utilizar o WebSphere eXtreme Scale para armazenar informações de pedido em um Web site. É possível criar um aplicativo Java Platform, Standard Edition 5 simples que utiliza um eXtreme Scale local e de memória. As entidades utilizam anotações e genéricos do Java SE 5.

"Colocando Diversos Objetos de Cache na Mesma Partição" na página 429
Ao definir dados relacionados em conjuntos de mapas que são organizados na mesma partição, você pode evitar a duplicação de dados e permitir o acesso a dados de baixa granularidade.

Referências relacionadas:

Java "Agente de Instrumentação de Desempenho da Entidade" na página 762
É possível melhorar o desempenho de entidades de acesso ao campo ativando o agente de instrumentação do WebSphere eXtreme Scale ao usar o Java Development Kit (JDK) Versão 6 ou posterior.

Java "Definindo um Esquema de Entidade" na página 391
Um ObjectGrid pode ter inúmeros esquemas de entidade lógicos. As entidades são definidas usando as classes Java anotadas, o XML ou uma combinação de classes XML e Java. Entidades definidas são registradas com um servidor eXtreme Scale e ligadas a BackingMaps, índices e outros plug-ins.

Java "Listeners de Entidade e Métodos de Retorno de Chamada" na página 408
Os aplicativos podem ser notificados quando o estado de uma entidade é alterado de estado para estado. Dois mecanismos de retorno de chamada existem para os eventos de mudança de estado: os métodos de retorno de chamada do ciclo de vida que são definidos em uma classe de entidade e são chamados sempre que o estado da entidade é alterado e os listeners de entidade, que são mais gerais porque o listener da entidade pode ser registrado em várias entidades.

Java "Exemplos do Listener de Entidade" na página 414
É possível gravar EntityListeners com base em seus requisitos. Veja a seguir vários scripts de exemplo.

Java "Interface EntityTransaction"
É possível utilizar a interface EntityTransaction para demarcar transações.

Informações relacionadas:

Java Amostra: Executando as Consultas em Paralelo Usando um ReduceGridAgent

Interface EntityTransaction: Java

É possível utilizar a interface EntityTransaction para demarcar transações.

Propósito

Para demarcar uma transação, é possível utilizar a interface EntityTransaction, que é associada com uma instância do gerenciador de entidades. Utilize o método EntityManager.getTransaction para recuperar a instância do EntityTransaction para o gerenciador de entidades. Cada instância do EntityManager e do EntityTransaction é associada com o objeto Session. É possível demarcar transações com EntityTransaction ou Session. Os métodos na interface EntityTransaction não

possuem nenhuma exceção verificada. Apenas as exceções de tempo de execução do tipo PersistenceException ou seu resultado de subclasses.

Para obter mais informações sobre a interface EntityTransaction, consulte Documentação da API.

Conceitos relacionados:

Java "Ajustando o Desempenho da Interface EntityManager" na página 760
A interface EntityManager separa aplicativos do estado de suspensão no armazenamento de dados da grade do servidor.

Java "Objetos de Armazenamento em Cache e seus Relacionamentos (API EntityManager)" na página 388
A maioria dos produtos de cache utiliza APIs baseadas em mapa para armazenar dados como pares de chave-valor. A API ObjectMap e o cache dinâmico no WebSphere Application Server, entre outros, usam essa abordagem. Entretanto, APIs baseadas em mapas têm limitações. A API EntityManager simplifica a interação com a grade de dados ao fornecer uma maneira fácil de declarar e interagir com um gráfico complexo de objetos relacionados.

Java "Entity Manager em um Ambiente Distribuído" na página 401
É possível usar a API EntityManager com um ObjectGrid local ou em um ambiente distribuído do eXtreme Scale . A principal diferença é como você se conecta a esse ambiente remoto. Após você estabelecer uma conexão, não existe diferença entre o uso de um objeto Session ou uma API do EntityManager.

Java "Interagindo com EntityManager" na página 405
Geralmente os aplicativos primeiro obtêm uma referência do ObjectGrid e, depois, uma Sessão dessa referência para cada encadeamento. As sessões não podem ser compartilhadas entre encadeamentos. Um método extra em Session, o método getEntityManager, está disponível. Este método retorna uma referência para um gerenciador de entidades para uso para este encadeamento. A interface de EntityManager pode substituir as interfaces de Session e ObjectMap para todos os aplicativos. É possível utilizar essas APIs de EntityManager se o cliente tiver acesso às classes de entidade definidas.

Java "Suporte ao Plano de Carregamento do EntityManager" na página 417
Um FetchPlan é a estratégia que o gerenciador de entidade usa para recuperar objetos associados se o aplicativo precisar acessar relacionamentos.

Java "Filas de Consulta da Entidade" na página 421
Filas de consulte permitem que aplicativos criem uma fila qualificada por uma consulta no lado do servidor ou eXtreme Scale local sobre uma entidade. As entidades do resultado da consulta são armazenadas nesta fila. Atualmente, a fila de consulta é suportada apenas em um mapa que está utilizando a estratégia de bloqueio pessimista.

Java "Roteando os Objetos de Cache para a Mesma Partição" na página 432
Quando a configuração do eXtreme Scale usa a estratégia de colocação de partição fixa, ela dependerá do hash da chave para uma partição inserir, obter, atualizar ou remover o valor. O método hashCode é chamado na chave e ele deverá ser bem definido se uma chave customizada for criada. No entanto, outra opção é usar a interface PartitionableKey. Com a interface PartitionableKey, será possível usar um objeto diferente da chave para efetuar hash de uma partição.

Tarefas relacionadas:

Java "Tutorial: Armazenando Informações de Pedido nas Entidades" na página 9
Este tutorial do gerenciador de entidade mostra como utilizar o WebSphere eXtreme Scale para armazenar informações de pedido em um Web site. É possível criar um aplicativo Java Platform, Standard Edition 5 simples que utiliza um eXtreme Scale local e de memória. As entidades utilizam anotações e genéricos do Java SE 5.

"Colocando Diversos Objetos de Cache na Mesma Partição" na página 429

Ao definir dados relacionados em conjuntos de mapas que são organizados na mesma partição, você pode evitar a duplicação de dados e permitir o acesso a dados de baixa granularidade.

Informações relacionadas:

Java Amostra: Executando as Consultas em Paralelo Usando um ReduceGridAgent

Colocando Diversos Objetos de Cache na Mesma Partição

Ao definir dados relacionados em conjuntos de mapas que são organizados na mesma partição, você pode evitar a duplicação de dados e permitir o acesso a dados de baixa granularidade.

Sobre Esta Tarefa

Definindo os mapas no mesmo conjunto de mapas, você pode facilmente armazenar os dados em uma única partição. Os dados que são armazenados em uma partição podem fazer referência a dados relacionados nessa mesma partição armazenando a chave da entrada de cache relacionada no outro mapa ou no mesmo mapa. Utilize a interface mixin PartitionableKey ou a API do DataGrid, que ignora o roteamento da chave nativa das chaves de cache. Os dados também podem ser armazenados como dados de referência, onde eles são duplicados em cada partição, em vez de particionados sozinhos.

Quando você utilizou o roteamento de partição fixa, os dados são roteados para a partição apropriada com base no código hash da chave. Para organizar dados na mesma partição, o WebSphere eXtreme Scale fornece os seguintes métodos:

Procedimento

1. Implemente a interface PartitionableKey para colocar dados relacionados em vários mapas na mesma partição. A interface mixin PartitionableKey é usada para classes-chave customizadas. A chave que você utiliza para roteamento de partição é integrada na chave e retornada pelo método PartitionableKey.ibmGetPartition(). Para obter informações adicionais, consulte “Roteando os Objetos de Cache para a Mesma Partição” na página 432.

   Replice manualmente a referência, dados nativamente particionados que não possuem a interface ParititonableKey definida.

2. Java .NET Implemente a anotação @PartitionKey para identificar um ou mais atributos em uma classe de chave customizada que é utilizada em um mapa configurado de formato de dados eXtreme (XDF). Se você estiver usando uma grade de dados corporativos, você deverá ativar o XDF para que Java e .NET possam acessar os mesmos objetos da grade de dados. Portanto, a anotação Partitionkey fornece uma alternativa para a interface ParittionableKey e permite a interoperabilidade com o cliente eXtreme Scale .NET Framework.
3. Utilize APIs de acesso a dados para gerenciar dados relacionais implementando a API EntityManager. A API EntityManager impinge o roteamento da partição, desenvolvendo um relacionamento de árvore restrito onde todas as entidades devem fornecer um caminho para a raiz da árvore e a chave raiz é utilizada para roteamento da partição e é integrada em cada chave relacionada.

   Utilize a opção de configuração schemaRoot para especificar uma raiz de um esquema de árvore restrito. Para obter informações adicionais, consulte “Objetos de Armazenamento em Cache e seus Relacionamentos (API EntityManager)” na página 388.

Exemplo

Os dados podem ser roteados para partições específicas com a API do DataGrid, permitindo armazenar dados de referência e outros padrões avançados nos quais o roteamento de chave tradicional não funciona. A API do DataGrid é útil, por exemplo, para armazenar dados de referência em cada partição, permitindo que consultas sempre sejam colocadas com conjuntos de dados particionados maiores.

No exemplo a seguir, um cliente na grade de dados tem um ou mais endereços. No entanto, um endereço tem apenas um cliente e um endereço tem um país.

```
CustomerKey <-->  AddressKey
Address ->  CountryKey
```

CustomerKey no mapa Customer é um relacionamento de um para muitos bidirecional com AddressKey no mapa Address. AddressKey pode implementar a interface PartitionableKey, integrando CustomerKey dentro dele e retornando o CustomerKey a partir do método ibmGetParittion(). Como alternativa, você pode anotar o campo CustomerKey integrado no AddressKey com a anotação @PartitionKey quando o XDF é ativado.

CountryKey pode ser integrado no valor Address e o valor de CountryKey e Country pode ser armazenado em cada partição com a API do DataGrid ou um carregador, substituindo o roteamento baseado na chave padrão.

Conceitos relacionados:

Java "Roteando os Objetos de Cache para a Mesma Partição" na página 432
Quando a configuração do eXtreme Scale usa a estratégia de colocação de partição fixa, ela dependerá do hash da chave para uma partição inserir, obter, atualizar ou remover o valor. O método hashCode é chamado na chave e ele deverá ser bem definido se uma chave customizada for criada. No entanto, outra opção é usar a interface PartitionableKey. Com a interface PartitionableKey, será possível usar um objeto diferente da chave para efetuar hash de uma partição.

Java "Ajustando o Desempenho da Interface EntityManager" na página 760
A interface EntityManager separa aplicativos do estado de suspensão no armazenamento de dados da grade do servidor.

Java "Objetos de Armazenamento em Cache e seus Relacionamentos (API EntityManager)" na página 388
A maioria dos produtos de cache utiliza APIs baseadas em mapa para armazenar dados como pares de chave-valor. A API ObjectMap e o cache dinâmico no WebSphere Application Server, entre outros, usam essa abordagem. Entretanto, APIs baseadas em mapas têm limitações. A API EntityManager simplifica a interação com a grade de dados ao fornecer uma maneira fácil de declarar e interagir com um gráfico complexo de objetos relacionados.

Java "Entity Manager em um Ambiente Distribuído" na página 401
É possível usar a API EntityManager com um ObjectGrid local ou em um ambiente distribuído do eXtreme Scale . A principal diferença é como você se conecta a esse ambiente remoto. Após você estabelecer uma conexão, não existe diferença entre o uso de um objeto Session ou uma API do EntityManager.

Java "Interagindo com EntityManager" na página 405
Geralmente os aplicativos primeiro obtêm uma referência do ObjectGrid e, depois, uma Sessão dessa referência para cada encadeamento. As sessões não podem ser compartilhadas entre encadeamentos. Um método extra em Session, o método getEntityManager, está disponível. Este método retorna uma referência para um gerenciador de entidades para uso para este encadeamento. A interface de EntityManager pode substituir as interfaces de Session e ObjectMap para todos os aplicativos. É possível utilizar essas APIs de EntityManager se o cliente tiver acesso às classes de entidade definidas.

Java "Suporte ao Plano de Carregamento do EntityManager" na página 417
Um FetchPlan é a estratégia que o gerenciador de entidade usa para recuperar objetos associados se o aplicativo precisar acessar relacionamentos.

Java "Filas de Consulta da Entidade" na página 421
Filas de consulte permitem que aplicativos criem uma fila qualificada por uma consulta no lado do servidor ou eXtreme Scale local sobre uma entidade. As entidades do resultado da consulta são armazenadas nesta fila. Atualmente, a fila de consulta é suportada apenas em um mapa que está utilizando a estratégia de bloqueio pessimista.

Referências relacionadas:

Java "Agente de Instrumentação de Desempenho da Entidade" na página 762
É possível melhorar o desempenho de entidades de acesso ao campo ativando o agente de instrumentação do WebSphere eXtreme Scale ao usar o Java Development Kit (JDK) Versão 6 ou posterior.

Java "Definindo um Esquema de Entidade" na página 391
Um ObjectGrid pode ter inúmeros esquemas de entidade lógicos. As entidades são definidas usando as classes Java anotadas, o XML ou uma combinação de classes XML e Java. Entidades definidas são registradas com um servidor eXtreme Scale e

ligadas a BackingMaps, índices e outros plug-ins.

Java "Listeners de Entidade e Métodos de Retorno de Chamada" na página 408
Os aplicativos podem ser notificados quando o estado de uma entidade é alterado de estado para estado. Dois mecanismos de retorno de chamada existem para os eventos de mudança de estado: os métodos de retorno de chamada do ciclo de vida que são definidos em uma classe de entidade e são chamados sempre que o estado da entidade é alterado e os listeners de entidade, que são mais gerais porque o listener da entidade pode ser registrado em várias entidades.

Java "Exemplos do Listener de Entidade" na página 414
É possível gravar EntityListeners com base em seus requisitos. Veja a seguir vários scripts de exemplo.

Java "Interface EntityTransaction" na página 426
É possível utilizar a interface EntityTransaction para demarcar transações.

Informações relacionadas:

Java Amostra: Executando as Consultas em Paralelo Usando um ReduceGridAgent

Roteando os Objetos de Cache para a Mesma Partição: Java

Quando a configuração do eXtreme Scale usa a estratégia de colocação de partição fixa, ela dependerá do hash da chave para uma partição inserir, obter, atualizar ou remover o valor. O método hashCode é chamado na chave e ele deverá ser bem definido se uma chave customizada for criada. No entanto, outra opção é usar a interface PartitionableKey. Com a interface PartitionableKey, será possível usar um objeto diferente da chave para efetuar hash de uma partição.

É possível usar a interface PartitionableKey em situações em que houver vários mapas e os dados que você consolidar serão relatados e, assim, deverão ser colocados na mesma partição. WebSphere eXtreme Scale não suporta two-phase commit, portanto, várias transações de mapa não deverão ser confirmadas se incluírem várias partições. Se o PartitionableKey efetuar hash para a mesma partição para as chaves em mapas diferentes no mesmo conjunto de mapas, eles poderão ser consolidados em conjunto.

Também é possível usar a interface PartitionableKey quando grupos de chaves tiverem que ser colocados na mesma partição, mas não necessariamente durante uma única transação. Se as chaves tiverem que ser submetidas a hash com base no local, departamento, tipo de domínio ou algum outro tipo de identificador, as chaves filha poderão receber um PartitionableKey pai.

Por exemplo, os funcionários devem efetuar hash para a mesma partição do seu departamento. Cada chave de funcionário terá um objeto PartitionableKey que pertence ao mapa do departamento. Então, o funcionário e o departamento devem executar hash para a mesma partição.

A interface PartitionableKey fornece um método, chamado ibmGetPartition. O objeto retornado desse método deve implementar o método hashCode. O resultado retornado do uso de um hashCode alternativo será usado para rotear as chaves para uma partição.

Exemplo

Consulte a chave de exemplo a seguir que demonstra como usar a interface PartitionableKey e o método hashCode para clonar uma chave existente e rotear as chaves resultantes para a mesma partição.

```
package com.ibm.websphere.cjtester;

import java.io.Serializable;

import com.ibm.websphere.objectgrid.plugins.PartitionableKey;

public class RoutableKey implements Serializable, Cloneable, PartitionableKey {
    private static final long serialVersionUID = 1L;

    // The data that makes up the actual data object key.
    public final String realKey;

    // The key of the data object you want to use for routing.
    // This is typically the key of a parent object.
    public final Object keyToRouteWith;

    public RoutableKey(String realKey, Object keyToRouteWith) {
        super();
        this.realKey = realKey;
        this.keyToRouteWith = keyToRouteWith;
    }

    /**
     * Return the hashcode of the key we are using for routing.
     * If not supplied, eXtreme Scale will use the hashCode of THIS key.
     */
    public Object ibmGetPartition() {
        return new Integer(keyToRouteWith.hashCode());
    }

    @Override
    public RoutableKey clone() throws CloneNotSupportedException {
        return (RoutableKey) super.clone();
    }

    @Override
    public int hashCode ()  {
        final int prime = 31;
        int result = 1;
        result = prime * result + ((keyToRouteWith == null) ? 0 : keyToRouteWith.hashCode());
        result = prime * result + ((realKey == null) ? 0 : realKey.hashCode());
        return result;
    }

    @Override
    public boolean equals(Object obj) {
        if (this == obj) return true;
        if ( obj == null ) return false;
        if (getClass() != obj.getClass()) return false;
        RoutableKey other = (RoutableKey) obj;
        if (keyToRouteWith == null) {
            if (other.keyToRouteWith != null) return false;
        } else if (!keyToRouteWith.equals(other.keyToRouteWith)) return false;
        if (realKey == null) {
            if (other.realKey != null) return false;
        } else if (!realKey.equals(other.realKey)) return false;
        return true;
    }
}
```

Tarefas relacionadas:

"Colocando Diversos Objetos de Cache na Mesma Partição" na página 429
Ao definir dados relacionados em conjuntos de mapas que são organizados na mesma partição, você pode evitar a duplicação de dados e permitir o acesso a dados de baixa granularidade.

Referências relacionadas:

Java "Agente de Instrumentação de Desempenho da Entidade" na página 762
É possível melhorar o desempenho de entidades de acesso ao campo ativando o agente de instrumentação do WebSphere eXtreme Scale ao usar o Java Development Kit (JDK) Versão 6 ou posterior.

Java "Definindo um Esquema de Entidade" na página 391
Um ObjectGrid pode ter inúmeros esquemas de entidade lógicos. As entidades são definidas usando as classes Java anotadas, o XML ou uma combinação de classes XML e Java. Entidades definidas são registradas com um servidor eXtreme Scale e ligadas a BackingMaps, índices e outros plug-ins.

Java "Listeners de Entidade e Métodos de Retorno de Chamada" na página 408
Os aplicativos podem ser notificados quando o estado de uma entidade é alterado de estado para estado. Dois mecanismos de retorno de chamada existem para os eventos de mudança de estado: os métodos de retorno de chamada do ciclo de vida que são definidos em uma classe de entidade e são chamados sempre que o estado da entidade é alterado e os listeners de entidade, que são mais gerais porque o listener da entidade pode ser registrado em várias entidades.

Java "Exemplos do Listener de Entidade" na página 414
É possível gravar EntityListeners com base em seus requisitos. Veja a seguir vários scripts de exemplo.

Java "Interface EntityTransaction" na página 426
É possível utilizar a interface EntityTransaction para demarcar transações.

Informações relacionadas:

Java Amostra: Executando as Consultas em Paralelo Usando um ReduceGridAgent

Definindo Anotações ClassAlias e FieldAlias para Correlacionar Classes Java

Java

Para ativar o compartilhamento de objetos na grade de dados entre diferentes classes Java, use anotações ClassAlias e FieldAlias. Quando duas classes são correlacionadas, os campos e tipos de campo são correspondidos entre as classes, mesmo se os nomes de classe são diferentes.

Antes de Iniciar

- Você deve ter o IBM eXtremeIO configurado. Para obter informações adicionais, consulte "Configurando o IBM eXtremeIO (XIO)" na página 119.
- Seu atributo copyMode em seu arquivo XML do descritor do ObjectGrid deve ser configurado como COPY_TO_BYTES. Para obter informações adicionais, consulte "Configurando Grades de Dados para Utilizar o eXtreme Data Format (XDF)" na página 121.
- Use as anotações ClassAlias e FieldAlias quando estiver executando duas classes diferentes dentro de escopos do aplicativo diferentes ou tempos de execução. Os dados que são armazenados na grade de dados podem ser compartilhados e

reutilizados entre dois tempos de execução de aplicativos diferentes. Como resultado, você não precisa manter dois descritores de metadados diferentes. Se suas classes estiverem dentro do mesmo escopo do aplicativo, ou tempo de execução, poderá ser confuso do ponto de vista do provedor do aplicativo ou do desenvolvimento ter duas classes correlacionadas.

Sobre Esta Tarefa

Para obter mais informações sobre as anotações ClassAlias e FieldAlias, consulte "Anotações ClassAlias e FieldAlias" na página 125.

Procedimento

1. Java Utilize as anotações ClassAlias e FieldAlias para correlacionar objetos entre duas classes Java diferentes. Nas classes de exemplo a seguir, a anotação Java `@ClassAlias("ACME_Customer")` é especificada. Alguns campos possuem uma anotação `@FieldAlias("")`. Como ambas as classes possuem a mesma anotação ClassAlias e as definições de FieldAlias, os objetos são mantidos com o mesmo ID do tipo de classe, por XDF. Os mesmos metadados XDF são usados quando estes objetos são serializados ou desserializados durante as operações get e put.

```
@ClassAlias("ACME_Customer")
class Customer1 {
    @FieldAlias("Employee ID")
    int empId = -1;

    @FieldAlias("Department No.")
    int deptId = -1;

    @FieldAlias("Year Salary")
    float salary = 0;

    String sex = "M";

    int age = -1;

    String homeAddress = "";

    public Customer1(int empId, int deptId, float salary, String sex, int age, String homeAddress) {
        this.empId = empId;
        this.deptId = deptId;
        this.salary = salary;
        this.sex = sex;
        this.age = age;
        this.homeAddress = homeAddress;
    }
}
```

Figura 34. Classe Customer1 com Anotações @ClassAlias e @FieldAlias

```
@ClassAlias("ACME_Customer")
   class Customer2 {
       @FieldAlias("Employee ID")
       int empId = -1;

       @FieldAlias("Department No.")
       int deptId = -1;

       @FieldAlias("Year Salary")
       float salary = 0;


       String sex = "M";

       int age = -1;

       String homeAddress = "";

       public Customer2(int empId, int deptId, float salary, String sex, int age, String homeAddress) {
           this.empId = empId;
           this.deptId = deptId;
           this.salary = salary;
           this.sex = sex;
           this.age = age;
           this.homeAddress = homeAddress;
       }

   }
```

Figura 35. Classe Customer2 com Anotações @ClassAlias e @FieldAlias

2. Opcional: Especifique o caminho de descoberta do alias de classe, de forma que o alias de classe possa ser utilizado para correlacionar com uma classe equivalente no caminho de classe do cliente. Configure o caminho de descoberta se o processo de desserialização não localizar a classe equivalente a partir do cliente. Configure o caminho de descoberta se você tiver outra classe em seu cliente que define o mesmo alias de classe, mas não é carregada em seu carregador de classe atual.

   - Java Ative um aplicativo Java para varrer e carregar classes que correspondem ao valor de ClassAlias especificado a partir do caminho de classe do aplicativo.

     Ao iniciar o aplicativo, especifique o argumento da Java virtual machine (JVM) `-Dwxs.classalias.discovery.path`. A lista de arquivos Java archive (JAR) ou pastas específicas que contêm as classes Java para corresponder com um alias de classe que é definido nas classes definidas pelo usuário são varridas.

     Por exemplo, você pode especificar: `-Dwxs.classalias.discovery.path=c:\myApp\lib\customer1.jar;c:\myApp\lib\customer2.jar;c:\myApp\classes` A operação de varredura varre todos os arquivos JAR especificados e pastas de caminho da classe para localizar todas as classes Java disponíveis. A classe Java que é correspondida primeiro no ambiente do aplicativo cliente é baseada no alias de classe carregado durante a operação get.

Anotações ClassAlias e FieldAlias:

Use as anotações ClassAlias e FieldAlias para ativar o compartilhamento de dados da grade de dados entre classes. É possível compartilhar dados entre duas classes Java ou entre uma classe Java e uma .NET.

Se você definir duas classes com o mesmo nome e campos, os dados da grade de dados serão automaticamente compartilhados entre as classes. Por exemplo, se você tiver uma classe Customer1 em seu aplicativo Java e uma classe Customer1 em seu aplicativo .NET que tenha os mesmos campos, os dados serão compartilhados entre as classes. Isso supõe que o nome de classe também inclui o

qualificador de classe, que também é o nome do pacote em Java e namespace em C#. O nome do pacote e o namespace são compartilhados automaticamente porque o namespace e os nomes de pacotes correspondem. Consulte o exemplo a seguir, em que ambos os nomes não fazem distinção entre maiúsculas e minúsculas:

```
Java:
package com.mycompany.app
public class SampleClass {
int field1;
String field2;
}

C#
namespace Com.MyCompany.App
public class SampleClass {
int field1;
string field2;
}
```

No entanto, você também pode correlacionar dados entre as classes que possuem nomes diferentes. Para correlacionar dados a serem armazenados na grade de dados entre os nomes de classe diferentes, utilize as anotações ClassAlias ou FieldAlias.

Entre dois aplicativos Java: É possível definir duas classes diferentes com nomes diferentes em ambientes de aplicativos Java separados. Marcando as classes com a mesma anotação de ClassAlias, e todos os campos e tipos de campo são correspondidos entre estas duas classes, as classes são correlacionadas com o mesmo ID de tipo de classe, embora tenham os nomes de classe diferentes. O mesmo ID de tipo de classe e os metadados podem, então, ser reutilizados entre as classes nos diferentes tempos de execução de aplicativos Java.

Entre um aplicativo Java e um aplicativo .NET: É possível usar anotações semelhantes em seu aplicativo C# para correlacionar a classe C# com uma classe Java. Os atributos ClassAlias definidos para a classe C# e os campos são correspondidos a uma classe Java com a mesma anotação de ClassAlias.

Tarefas relacionadas:

8.6+ "Definindo Anotações ClassAlias e FieldAlias para Correlacionar Classes Java e .NET" na página 124
Use as anotações ClassAlias e FieldAlias para ativar o compartilhamento de dados da grade de dados entre suas classes Java e .NET.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Informações relacionadas:

8.6+ "Lição 2.3: Criando um Aplicativo de Grade de Dados Corporativos" na página 243
Para criar um aplicativo de grade de dados corporativos no qual clientes Java e .NET podem atualizar a mesma grade de dados, você deve tornar suas classes compatíveis. Nos aplicativos de amostra de introdução, o aplicativo de amostra .NET tem aliases para corresponderem aos padrões Java.

Recuperando Entidades e Objetos (API de Consulta)

Java

O WebSphere eXtreme Scale fornece um mecanismo de consulta flexível para recuperar entidades usando a API do EntityManager e objetos Java usando a API do ObjectQuery.

Recursos de Consulta do WebSphere eXtreme Scale

Com o mecanismo de consulta do eXtreme Scale, é possível executar consultas do tipo SELECT sobre uma entidade ou esquema baseado em objeto usando a linguagem de consulta do eXtreme Scale.

Esta linguagem de consulta fornece os seguintes recursos:

- Resultados únicos e com diversos valores
- Funções agregadas
- Classificação e agrupamento
- Junções
- Expressões condicionais com subconsultas
- Parâmetros nomeados e posicionais
- Uso de índice do eXtreme Scale
- Sintaxe da expressão de caminho para navegação de objetos
- Paginação

Interface de Consulta

Utilize a interface de consulta para controlar a execução da consulta da entidade de controle.

Utilize o método EntityManager.createQuery(String) para criar uma Query. É possível usar cada instância de consulta múltiplas vezes com a instância de EntityManager na qual ela foi recuperada.

Cada resultado da consulta produz uma entidade na qual a chave da entidade é o ID da linha (do tipo longo) e o valor da entidade contém os resultados do campo da cláusula SELECT. É possível usar cada resultado da consulta em consultas subsequentes.

Os seguintes métodos estão disponíveis na interface com.ibm.websphere.objectgrid.em.Query.

public ObjectMap getResultMap()

O método getResultMap executa uma consulta SELECT e retorna os resultados em um objeto ObjectMap com os resultados na ordem especificada pela consulta. O ObjectMap resultante é válido apenas para a transação atual.

A chave do mapa é o número de resultado, do tipo long, iniciando em 1. O valor do mapa é do tipo com.ibm.websphere.projector.Tuple, em que cada atributo e associação é nomeado com base em sua posição ordinal dentro da cláusula select da consulta. Utilize o método para recuperar o EntityMetadata para o objeto Tupla armazenado dentro do mapa.

O método getResultMap é o mais rápido para recuperar dados do resultado da consulta nas qual múltiplos resultados podem existir. É possível recuperar o nome da entidade resultante usando os métodos ObjectMap.getEntityMetadata() e EntityMetadata.getName().

Exemplo: A seguinte consulta retorna duas linhas.

```
String ql = SELECT e.name, e.id, d from Employee e join e.dept d WHERE d.number=5
 Query q = em.createQuery(ql);
 ObjectMap resultMap = q.getResultMap();
 long rowID = 1; // starts with index 1
 Tuple tResult = (Tuple) resultMap.get(new Long(rowID));
 while(tResult != null) {
     // The first attribute is name and has an attribute name of 1
     // But has an ordinal position of 0.
     String name = (String)tResult.getAttribute(0);
     Integer id = (String)tResult.getAttribute(1);

     // Dept is an association with a name of 3, but
     // an ordinal position of 0 since it's the first association.
     // The association is always a OneToOne relationship,
     // so there is only one key.
     Tuple deptKey = tResult.getAssociation(0,0);
     ...
     ++rowID;
     tResult = (Tuple) resultMap.get(new Long(rowID));

 }
```

public Iterator getResultIterator

O método getResultIterator executa uma consulta SELECT e retorna os resultados da consulta usando um Agente iterativo no qual cada resultado é um Objeto para uma consulta com valor único, ou uma matriz de Objetos para uma consulta com múltiplos valores. Os valores no resultado são armazenados na ordem da consulta. O Iterator de resultado é válido apenas para a transação atual.

Este método é preferencial para recuperar resultados da consulta dentro do contexto de EntityManager. É possível utilizar o método setResultEntityName(String) opcional para nomear a entidade resultante, para que ela possa ser utilizada em consultas adicionais.

Exemplo: A seguinte consulta retorna duas linhas.

```
String ql = SELECT e.name, e.id, e.dept from Employee e WHERE e.dept.number=5
 Query q = em.createQuery(ql);
 Iterator results = q.getResultIterator();
 while(results.hasNext()) {
     Object[] curEmp = (Object[]) results.next();
     String name = (String) curEmp[0];
     Integer id = (Integer) curEmp[1];
     Dept d = (Dept) curEmp[2];
     ...
 }
```

public Iterator getResultIterator(Class resultType)

O método getResultIterator(Class resultType) executa uma consulta SELECT e retorna os resultados da consulta usando um Agente Iterativo da entidade. O tipo de entidade é determinado pelo parâmetro resultType. O Iterator de resultado é válido apenas para a transação atual.

Utilize esse método quando você quiser utilizar as APIs EntityManager para acessar as entidades resultantes.

Exemplo: A consulta a seguir retorna todos os funcionários e o departamento ao qual pertencem para uma divisão, com classificação por salário. Para imprimir os cinco funcionários com os salários mais altos e, então, selecionar o trabalho com funcionários de apenas um departamento no mesmo conjunto de trabalhos, utilize o seguinte código.

```
String string_ql = "SELECT e.name, e.id, e.dept from Employee e WHERE e.dept.division='Manufacturi
Query query1 = em.createQuery(string_ql);
query1.setResultEntityName("AllEmployees");
Iterator results1 = query1.getResultIterator(EmployeeResult.class);
int curEmployee = 0;
```

```
System.out.println("Highest paid employees");
while (results1.hasNext() && curEmployee++ < 5) {
 EmployeeResult curEmp = (EmployeeResult) results1.next();
 System.out.println(curEmp);
 // Remove the employee from the resultset.
 em.remove(curEmp);
}

// Flush the changes to the result map.
em.flush();

// Run a query against the local working set without the employees we
// removed
String string_q2 = "SELECT e.name, e.id, e.dept from AllEmployees e WHERE e.dept.name='Hardware'";
Query query2 = em.createQuery(string_q2);
Iterator results2 = query2.getResultIterator(EmployeeResult.class);
System.out.println("Subset list of Employees");
while (results2.hasNext()) {
 EmployeeResult curEmp = (EmployeeResult) results2.next();
 System.out.println(curEmp);
}
```

public Object getSingleResult

O método getSingleResult executa uma consulta SELECT que retorna um único resultado.

Se a cláusula SELECT tiver mais de um campo definido, então o resultado é uma matriz de objetos, na qual cada elemento na matriz se baseia em sua posição original dentro da cláusula SELECT da consulta.

```
String ql = SELECT e from Employee e WHERE e.id=100"
 Employee e = em.createQuery(ql).getSingleResult();

 String ql = SELECT e.name, e.dept from Employee e WHERE e.id=100"
 Object[] empData = em.createQuery(ql).getSingleResult();
 String empName= (String) empData[0];
 Department empDept = (Department) empData[1];
```

public Query setResultEntityName(String entityName)

O método setResultEntityName(String entityName) especifica o nome da entidade do resultado da consulta.

Toda vez que os métodos getResultIterator ou getResultMap são chamados, uma entidade com um ObjectMap é dinamicamente criada para manter os resultados da consulta. Se a entidade não for especificada, ou estiver nula, a entidade e o nome do ObjectMap serão automaticamente gerados.

Como todos os resultados da consulta estão disponíveis para a duração de uma transação, um nome de consulta não pode ser reutilizado em uma única transação.

public Query setPartition(int partitionId)

Configure a partição para onde é roteada a consulta.

Este método é necessário se os mapas na consulta estão particionados e se o gerenciador de entidades não tem afinidade com uma partição da entidade-raiz do esquema único.

Use a Interface PartitionManager para determinar o número de partições para o mapa de apoio de uma determinada entidade.

A tabela a seguir fornece descrições dos outros métodos que estão disponíveis por meio da interface da consulta.

Tabela 12. Outros Métodos

Método	Resultado
public Query setMaxResults(int maxResult)	Configure o número máximo de resultados para recuperar.
public Query setFirstResult(int startPosition)	Configure a posição do primeiro resultado para recuperar.
public Query setParameter(String name, Object value)	Ligue um argumento a um parâmetro nomeado.
public Query setParameter(int position, Object value)	Ligue um argumento a um parâmetro posicional.
public Query setFlushMode(FlushModeType flushMode)	Configure o tipo de modo de limpeza a ser utilizado quando a consulta for executada, substituindo esse tipo de modo configurado no EntityManager.

Elementos de Consulta do eXtreme Scale

Com o mecanismo de consulta do eXtreme Scale, é possível utilizar uma linguagem de consulta única para procurar o cache do eXtreme Scale. Esta linguagem de consulta pode consultar objetos Java que são armazenados em objetos ObjectMap e objetos Entity. Utilize a sintaxe a seguir para criar uma cadeia de consultas.

Uma consulta do eXtreme Scale é uma cadeia que contém os seguintes elementos:

- Uma cláusula SELECT que especifica os objetos ou valores a retornar.
- Uma cláusula FROM que nomeia as coletas de objeto.
- Uma cláusula WHERE opcional que contém predicados de procura sobre as coletas.
- Uma cláusula GROUP BY e HAVING (consulte as funções de agregação de consulta do eXtreme Scale).
- Uma cláusula ORDER BY opcional que especifica a classificação da coleta de resultados.

Conjuntos de objetos Java são identificados em consultas por meio do uso de seu nome na cláusula FROM da consulta.

Os elementos da linguagem de consulta são discutidos em mais detalhes nos tópicos relacionados a seguir:

- Sintaxe do “Backus-Naur Form de Consulta do ObjectGrid” na página 461
- “Referência para Consultas do eXtreme Scale” na página 452

Os tópicos a seguir descrevem os meios para usar a API de Consulta:

- “API de Consulta EntityManager” na página 448
- “Uso da API ObjectQuery” na página 443

Consultando Dados em vários Fusos Horários: Java

Em um cenário distribuído, consultas são realmente executadas em servidores. Ao consultar dados com predicados do tipo calendar, java.util.Date e timestamp, o valor de data / hora especificado em uma consulta é baseado no fuso horário local do servidor.

Em um sistema de fuso horário único no qual todos os clientes e servidores são executados no mesmo fuso horário, você não precisa considerar os problemas relacionados aos tipos de predicado com calendar, java.util.Date e timestamp. Entretanto, quando clientes e servidores estão em fusos horários diferentes, o valor de data / hora especificado nas consultas é baseado no fuso horário do servidor e pode retornar dados indesejados para o cliente. Sem saber o fuso horário do servidor, o valor de data / hora especificado não tem sentido. Portanto, o valor de data / hora especificado deve considerar a diferença do deslocamento de fuso horário entre o fuso horário de destino e o fuso horário do servidor.

Deslocamento de Fuso Horário

Por exemplo, suponha que um cliente esteja em um fuso horário [GMT-0] e que o servidor esteja em um fuso horário [GMT-6]. O fuso horário do servidor está 6 horas atrás do cliente. O cliente gostaria de executar a seguinte consulta:

```
SELECT e FROM Employee
e WHERE e.birthDate='1999-12-31 06:00:00'
```

Supondo que a entidade Employee tenha um atributo birthDate do tipo java.util.Date, o cliente está no fuso horário [GMT-0] e quer recuperar Employees com o valor de birthDate de '1999-12-31 06:00:00 [GMT-0]' com base em seu fuso horário.

A consulta será executada no servidor e o valor de birthDate utilizado pelo mecanismo de consulta será '1999-12-31 06:00:00 [GMT-6]', que é igual a '1999-12-31 12:00:00 [GMT-0]'. Employees com valor de birthDate igual a '1999-12-31 12:00:00 [GMT-0]' serão retornados ao cliente. Além disso, o cliente não obterá Employees desejados com valor de birthDate de '1999-12-31 06:00:00 [GMT-0]'.

O problema descrito ocorre devido à diferença de fuso horário entre cliente e servidor. Para resolver esse problema, uma abordagem é calcular o deslocamento de fuso horário entre cliente e servidor e aplicar esse deslocamento no valor de data / hora de destino na consulta. No exemplo de consulta anterior, o deslocamento de fuso horário é de -6 horas, e o predicado birthDate ajustado deve ser “birthDate='1999-12-31 00:00:00'” se o cliente pretende recuperar Employees com valor de birthDate de '12-31 06:00:00 [GMT-0]'. Com o valor de birthDate ajustado, o servidor utilizará '1999-12-31 00:00:00 [GMT-6]' que é igual ao valor de destino '12-31 06:00:00 [GMT-0]', e Employees necessários serão retornados ao cliente.

Implementação Distribuída em vários Fusos Horários

Se a grade do eXtreme Scale distribuída for implementada em vários servidores ObjectGrid em vários fusos horários, a abordagem de ajuste do deslocamento de fuso horário não funcionará porque o cliente não saberá qual servidor executará a consulta e, assim, não poderá determinar o deslocamento de fuso horário a ser utilizado. A única solução é utilizar o sufixo ‘Z' (sem distinção de maiúsculas e minúsculas) no formato de escape de data e hora do JDBC para indicar o uso do fuso horário GMT com base no valor de data e hora. O sufixo ‘Z' (sem distinção de maiúsculas e minúsculas) indica o uso do fuso horário GMT com base no valor de

data e hora. Sem o sufixo ‘Z', o valor de data e hora baseado no fuso horário local será utilizado no processo que executa a consulta.

A consulta a seguir é equivalente ao exemplo anterior, mas utiliza o sufixo ‘Z':

```
SELECT e FROM Employee e WHERE e.birthDate='1999-12-31 06:00:00Z'
```

A consulta deve localizar Employees com valor de birthDate de ‘1999-12-31 06:00:00'. O sufixo ‘Z' indica que o valor de birthDate especificado é baseado no fuso horário GMT, portanto, o valor de birthDate ‘1999-12-31 06:00:00 [GMT-0]' baseado no fuso horário GMT será utilizado pelo mecanismo de consulta para o valor do critério de correspondência. Employees com valor de atributo birthDate igual a esse valor de birthDate baseado em GMT ‘1999-12-31 06:00:00 [GMT-0]' serão incluídos no resultado da consulta. O uso do sufixo ‘Z' no formato de escape de data e hora do JDBC em qualquer consulta é crucial para tornar o fuso horário dos aplicativos seguro. Sem essa abordagem, o valor de data e hora é baseado no fuso horário do servidor e não tem sentido a partir da perspectiva do cliente quando clientes e servidores estão em fusos horários diferentes.

Para obter informações adicionais, consulte “Dados para Diferentes Fusos Horários” na página 335.

Dados para Diferentes Fusos Horários: Java

Ao inserir dados com os atributos calendar, java.util.Date e timestamp em um ObjectGrid, você deve garantir que esses atributos de data e hora sejam criados com base no mesmo fuso horário, principalmente quando implementados em vários servidores em vários fusos horários. Usar o mesmo objeto de data e hora baseado em fuso horário pode garantir que o aplicativo esteja protegido por fuso horário e que os dados possam ser consultados pelos predicados calendar, java.util.Date e timestamp.

Sem especificar explicitamente um fuso horário ao criar objetos de data e hora, o Java usa o fuso horário local e pode causar valores de data e hora inconsistentes nos clientes e servidores.

Considere um exemplo em uma implementação distribuída na qual o client1 está no fuso horário [GMT-0] e o client2 está no [GMT-6], e ambos querem criar um objeto java.util.Date com o valor '1999-12-31 06:00:00'. Então, o client1 criará o objeto java.util.Date com o valor '1999-12-31 06:00:00 [GMT-0]' e o client2 criará o objeto java.util.Date com o valor '1999-12-31 06:00:00 [GMT-6]'. Os objetos java.util.Date não são iguais porque o fuso horário é diferente. Um problema semelhante ocorre quando você pré-carrega os dados nas partições que residem em servidores em fusos horários diferentes se o fuso horário local for utilizado para criar objetos de data e hora.

Para evitar o problema descrito, o aplicativo pode escolher um fuso horário como [GMT-0] como fuso horário base para criar objetos calendar, java.util.Date e timestamp.

Uso da API ObjectQuery: Java

A API ObjectQuery fornece métodos para consulta de dados no ObjectGrid que são armazenados usando a API ObjectMap. Quando um esquema é definido na

instância do ObjectGrid, a API do ObjectQuery pode ser usada para criar e executar consultas sobre os objetos heterogêneos armazenados nos mapas de objetos.

Consulta e Mapas de Objetos

Você pode usar uma capacidade de consulta avançada para objetos que são armazenados usando a API do ObjectMap. Essas consultas permitem que os objetos sejam recuperados utilizando os atributos não-chave e executem agregações simples, como sum, avg, min e max junto a todos os dados que correspondem a uma consulta. Os aplicativos podem construir uma consulta usando o método Session.createObjectQuery. Ese método retorna um objeto ObjectQuery que pode ser então interrogado para se obter os resultados da consulta. O objeto de consulta também permite que a consulta seja customizada antes de executá-la. A consulta é executada automaticamente quando qualquer método que retorna o resultado é chamado.

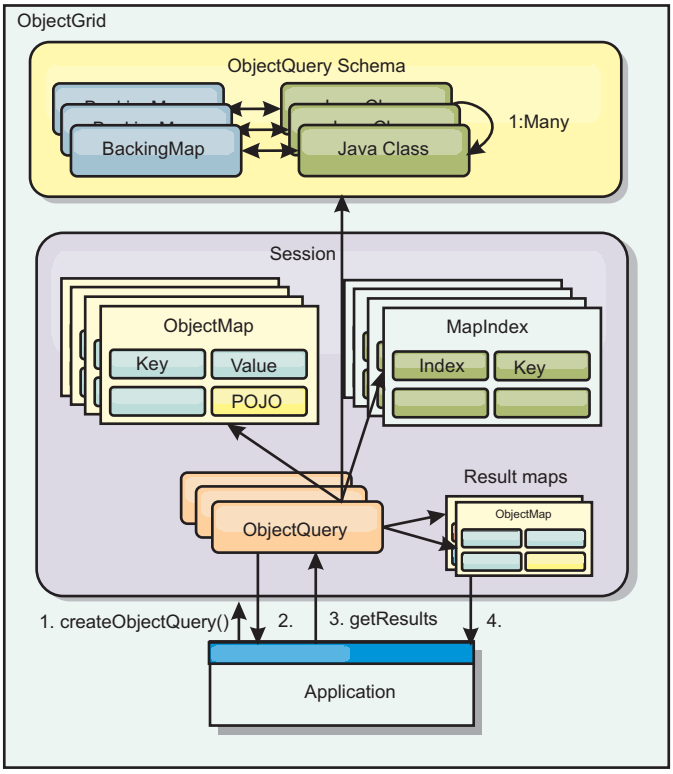


Figura 36. A interação da consulta com os mapas de objetos e como um esquema é definido para classes e associado a um mapa ObjectGrid

Definindo um Esquema do ObjectMap

Os mapas de objetos são usados para armazenar objetos em várias formas e são largamente livres de formatos. Um esquema deve ser definido no ObjectGrid que define o formato dos dados. Um esquema é composto das seguintes partes:

- O tipo de objeto armazenado no ObjectMap
- Relacionamentos entre ObjectMaps
- O método ao qual cada consulta acessa os atributos de dados nos objetos (campos e métodos de propriedade)
- O nome do atributo da chave primária no objeto.

Consulte o esquema Configurando um ObjectQuery para obter detalhes.

Para obter um exemplo sobre a criação de um esquema programaticamente ou usando o arquivo XML descritor do ObjectGrid, consulte “Tutorial do ObjectQuery - Etapa 3” na página 3.

Consultando Objetos com a API do ObjectQuery

A interface ObjectQuery permite a consulta de objetos de não-entidade, que sejam objetos heterogêneos e estejam armazenados nos ObjectMaps do ObjectGrid. A API ObjectQuery fornece uma maneira fácil de localizar os objetos ObjectMap sem usar o mecanismo de índice diretamente.

Há dois métodos para recuperação de resultados de um ObjectQuery: getResultIterator e getResultMap.

Recuperando resultados da consulta utilizando getResultIterator

Basicamente, os resultados de consultas são uma lista de atributos. Suponha que a consulta for selecionar a,b,c de X, em que y=z. Esta consulta retorna uma lista de linhas contendo a, b e c. Esta lista é armazenada em um Mapa com escopo em transação, o que significa que você deve associar uma chave artificial a cada linha e utilizar um número inteiro que aumenta a cada linha. Este mapa é obtido utilizando o método ObjectQuery.getResultMap(). É possível acessar os elementos de cada linha utilizando o código semelhante ao seguinte:

```
ObjectQuery q = session.createQuery(
    "select c.id, c.firstName, c.surname from Customer c where c.surname=?1");

  q.setParameter(1, "Claus");

  Iterator iter = q.getResultIterator();
  while(iter.hasNext())
  {
    Object[] row = (Object[])iter.next();
    System.out.println("Found a Claus with id "
      + row[objectgrid: 0 ] + ", firstName: "
      + row[objectgrid: 1 ] + ", surname: "
      + row[objectgrid: 2 ]);
  }
```

Recuperando resultados da consulta utilizando getResultMap

Os resultados da consulta também podem ser recuperados utilizando diretamente o mapa de resultados. O exemplo a seguir mostra uma consulta recuperando partes específicas dos Clientes correspondentes e demonstra como acessar as linhas resultantes. Observe que, se você utilizar o objeto ObjectQuery para acessar os dados, então o identificador de linha longa gerado será ocultado. A linha longa é visível somente ao utilizar o ObjectMap para acessar o resultado.

Quando a transação é concluída, este mapa desaparece. O mapa também está visível apenas na sessão utilizada, ou seja, geralmente apenas no encadeamento que o criou. O mapa utiliza uma chave do tipo Long que representa o ID da linha. Os valores armazenados no mapa são do tipo Object ou Object[], em que cada elemento corresponde ao tipo do elemento na cláusula select da consulta.

```
ObjectQuery q = em.createQuery(
      "select c.id, c.firstName, c.surname from Customer c where c.surname=?1");
  q.setParameter(1, "Claus");
  ObjectMap qmap = q.getResultMap();
```

```
for(long rowId = 0; true; ++rowId)
{
  Object[] row = (Object[]) qmap.get(new Long(rowId));
  if(row == null) break;
  System.out.println(" I Found a Claus with id " + row[0]
    + ", firstName: " + row[1]
    + ", surname: " + row[2]);
}
```

Para obter exemplos sobre o uso do ObjectQuery, consulte “Tutorial: Consultando uma Grade de Dados na Memória Local” na página 1.

Configurando um Esquema ObjectQuery: Java

O ObjectQuery conta com o esquema ou informações de formato para executar a verificação semântica e avaliar expressões de caminho. Esta seção descreve como definir o esquema no XML ou programaticamente.

Definindo o Esquema

O esquema do ObjectMap é definido no XML do descritor de implementação do ObjectGrid ou programaticamente utilizando as técnicas de configuração normais do eXtreme Scale. Para obter um exemplo sobre como criar um esquema, consulte “Tutorial do ObjectQuery - Etapa 4” na página 5.

As informações do esquema descrevem os POJOs (Plain Old Java Objects): cujos atributos que os compõem e quais os tipos de atributos que podem ter, sejam os atributos de campos de chave primária, relacionamentos de um único valor ou de múltiplos valores, ou relacionamentos bidirecionais. As informações do esquema conduzem o ObjectQuery a utilizar acesso de campo ou acesso de propriedade.

Atributos que Podem Ser Consultados

Quando o esquema é definido no ObjectGrid, os objetos no esquema são examinados automaticamente utilizando reflexão para determinar quais atributos estão disponíveis para consulta. Você pode consultar os tipos de atributos a seguir:

- Os tipos primitivos Java incluindo wrappers
- java.lang.String
- java.math.BigInteger
- java.math.BigDecimal
- java.util.Date
- java.sql.Date
- java.sql.Time
- java.sql.Timestamp
- java.util.Calendar
- byte[]
- java.lang.Byte[]
- char[]
- java.lang.Character[]
- Enum J2SE

Tipos serializáveis integrados que não aqueles indicados anteriormente também podem ser incluídos em um resultado da consulta, mas não podem ser incluídos na cláusula WHERE ou FROM da consulta. Atributos serializáveis não são navegáveis.

Os tipos de atributo podem ser excluídos do esquema se o tipo não for serializável, o campo ou propriedade é estática, ou o campo é temporário. Como todos os objetos de mapa devem ser serializáveis, o ObjectGrid inclui somente atributos que podem ser persistidos a partir do objeto. Outros objetos são ignorados.

Atributos de campo

Quando um esquema é configurado para acessar o objeto utilizando campos, todos serializáveis, os campos não-temporários são incorporados automaticamente no esquema. Para selecionar um atributo de campo em uma consulta, utilize o nome identificador de campo como ele existe na definição de classe.

Todos os campos público, privado, protegido e de pacote protegido são incluídos no esquema.

Atributos de propriedade

Quando o esquema está configurado para acessar o objeto usando propriedades, todos os métodos serializáveis que seguem as convenções de nomenclatura da propriedade JavaBeans serão automaticamente incorporadas no esquema. Para selecionar um atributo de propriedade para a consulta, use as convenções de nome de propriedade de estilo JavaBeans.

Todas as propriedades pública, privada, protegida e de pacote protegido são incluídas no esquema.

Na classe a seguir, os seguintes atributos são incluídos no esquema: name, birthday, valid.

```
public class Person {
  public String getName(){}
  private java.util.Date getBirthday(){}
  boolean isValid(){}
  public NonSerializableObject getData(){}
}
```

Ao utilizar um CopyMode de COPY_ON_WRITE, o esquema da consulta deve sempre utilizar o acesso baseado em propriedade. COPY_ON_WRITE cria objetos proxy sempre que os objetos são recuperados do mapa e podem acessar apenas aqueles objetos utilizando métodos de propriedade. A falha ao fazer isso resultará em cada resultado da consulta sendo configurado como nulo.

Relacionamentos

Cada relacionamento deve ser definido explicitamente na configuração do esquema. A cardinalidade do relacionamento é determinada automaticamente pelo tipo do atributo. Se o atributo implementa a interface java.util.Collection, então o relacionamento é um relacionamento de um-para-muitos ou de muitos-para-muitos.

Diferente das consultas de entidade, os atributos que se referem a outros objetos de cache não podem armazenar diretamente referências no objeto. As referências a

outros objetos são serializadas como parte dos dados do objeto que as contém. Em vez disso, armazene a chave no objeto relacionado.

Por exemplo, se houver relacionamento de muitos-para-um entre um Cliente e o Pedido:

Incorrect. Storing an object reference.

```
public class Customer {
  String customerId;
  Collection<Order> orders;
}

public class Order {
  String orderId;
  Customer customer;
}
```

Correto. A chave para o objeto relacionado.

```
public class Customer {
  String customerId;
  Collection<String> orders;
}

public class Order {
  String orderId;
  String customer;
}
```

Quando uma consulta é executada de modo a unir os dois objetos de mapa, a chave será automaticamente aumentada. Por exemplo, a seguinte consulta retorna objetos de Cliente:

```
SELECT c FROM Order o JOIN Customer c WHERE orderId=5
```

Utilizando Índices

O ObjectGrid utiliza plugins de índice para incluir índices nos mapas. O mecanismo de consulta incorpora automaticamente todos os índices definidos em um elemento de mapa do esquema do tipo: com.ibm.websphere.objectgrid.plugins.index.HashIndex e a propriedade rangeIndex é configurada para true. Se o tipo do índice não for HashIndex e a propriedade rangeIndex não estiver configurada para true, então o índice é ignorado pela consulta. Consulte “Tutorial do ObjectQuery - Etapa 2” na página 2 para obter um exemplo de como incluir um índice no esquema.

API de Consulta EntityManager: Java

A API do EntityManager fornece métodos para consultar dados no ObjectGrid armazenado utilizando a API do EntityManager. A API de Consulta EntityManager é usada para criar e executar consultas sobre uma ou mais entidades definidas no eXtreme Scale.

Consulta e ObjectMaps para Entidades

O WebSphere Extended Deployment v6.1 introduziu um recurso de consulta avançado para entidades armazenadas no eXtreme Scale. Essas consultas permitem que os objetos sejam recuperados utilizando os atributos não-chave e executem agregações simples, como sum, average, minimum e maximum junto a todos os dados que correspondem a uma consulta. Os aplicativos constroem uma consulta

utilizando a API EntityManager.createQuery. Isso retorna um objeto de consulta e pode, então, ser interrogado para obter os resultados da consulta. O objeto de consulta também permite que a consulta seja customizada antes de executá-la. A consulta é executada automaticamente quando qualquer método que retorna o resultado é chamado.

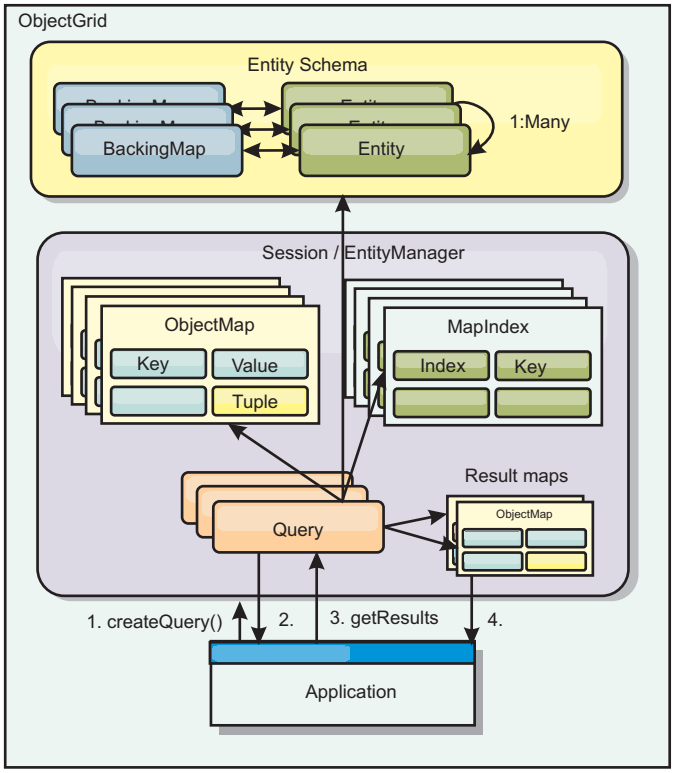


Figura 37. A interação da consulta com os mapas de objetos ObjectGrid e como o esquema da entidade é definido e associado com um mapa ObjectGrid.

Recuperando resultados da consulta usando o método getResultIterator

Os resultados da consulta são uma lista de atributos. Se uma consulta foi selecionar a,b,c de X, em que y=z, então, uma lista de linhas contendo a, b e c é retornada. Essa lista é armazenada em um Mapa de transações com escopo definido, o que significa que é necessário associar uma chave artificial com cada linha e utilizar um inteiro que aumenta com cada linha. Este mapa é obtido usando o método Query.getResultMap. O mapa possui EntityMetaData, que descreve cada linha no Mapa associado a ele. É possível acessar os elementos de cada linha utilizando o código semelhante ao seguinte:

```
Query q = em.createQuery("select c.id, c.firstName, c.surname from Customer c where c.surname=?1");

  q.setParameter(1, "Claus");

  Iterator iter = q.getResultIterator();
  while(iter.hasNext())
  {
    Object[] row = (Object[])iter.next();
    System.out.println("Found a Claus with id "  + row[objectgrid: 0 ]
      + ", firstName: " + row[objectgrid: 1 ]
      + ", surname: " + row[objectgrid: 2 ]);
  }
```

Recuperando Resultados da Consulta Utilizando getResultMap

O código a seguir mostra a recuperação de partes específicas dos Clientes correspondentes e mostra como acessar as linhas resultantes. Se você utilizar o objeto Query para acessar os dados, então o identificador de linha longa gerado será ocultado. O Long é visível somente ao utilizar o ObjectMap para acessar o resultado. Quando a transação é concluída, este mapa desaparece. O Mapa está visível apenas na Session utilizada, ou seja, geralmente apenas no encadeamento que o criou. O Mapa utiliza uma Tupla para a chave com um único atributo, um Long com o ID da linha. O valor é uma outra tupla com um atributo para cada coluna no conjunto de resultados.

O código de amostra a seguir demonstra isto:

```
Query q = em.createQuery("select c.id, c.firstName, c.surname from
Customer c where c.surname=?1");
q.setParameter(1, "Claus");
ObjectMap qmap = q.getResultMap();
Tuple keyTuple = qmap.getEntityMetadata().getKeyMetadata().createTuple();
for(long i = 0; true; ++i)
{
  keyTuple.setAttribute(0, new Long(i));
  Tuple row = (Tuple)qmap.get(keyTuple);
  if(row == null) break;
  System.out.println(" I Found a Claus with id "  + row.getAttribute(0)
    + ", firstName: " + row.getAttribute(1)
    + ", surname: " + row.getAttribute(2));
}
```

Recuperando Resultados da Consulta Utilizando um Agente Iterativo de Resultado da Entidade

O código a seguir mostra a consulta e o loop que recupera cada linha resultante utilizando as APIs de mapas normais. A chave para o Mapa é uma Tupla. Portanto, construa uma dos tipos corretos utilizando o resultado do método createTuple em keyTuple. Tente recuperar todas as linhas com rowIds de 0 em diante. Quando você obtém retornos de nulo (indicando que a chave não foi localizada), então o loop é finalizado. Configure o primeiro atributo de keyTuple como o long que deseja localizar. O valor retornado por get também é uma Tupla com um atributo para cada coluna no resultado da consulta. Em seguida, empurre cada atributo da Tupla de valor utilizando getAttribute.

A seguir está o próximo trecho de código:

```
Query q2 = em.createQuery("select c.id, c.firstName, c.surname from Customer c where c.surname=?1");
q2.setResultEntityName("CustomerQueryResult");
q2.setParameter(1, "Claus");

Iterator iter2 = q2.getResultIterator(CustomerQueryResult.class);
while(iter2.hasNext())
{
  CustomerQueryResult row = (CustomerQueryResult)iter2.next();
  // firstName is the id not the firstName.
  System.out.println("Found a Claus with id " + row.id
    + ", firstName: " + row.firstName
    + ", surname: " + row.surname);
}

em.getTransaction().commit();
```

Um valor de ResultEntityName está especificado na consulta. Este valor informa ao mecanismo de consulta que você deseja projetar cada linha para um objeto específico, CustomerQueryResult, neste caso. A classe é a seguinte:

```
@Entity
public class CustomerQueryResult {
 @Id long rowId;
```

```
 String id;
 String firstName;
 String surname;
};
```

No primeiro snippet, observe que cada linha da consulta é retornada como um objeto CustomerQueryResult em vez de um Object[]. As colunas resultantes da consulta são projetadas para o objeto CustomerQueryResult. Projetar o resultado é ligeiramente mais lento no tempo de execução, porém mais legível. O resultado da consulta Entities não deve ser registrado com o eXtreme Scale na inicialização. Se as entidades são registradas, então um Mapa global com o mesmo nome é criado, e a consulta falha com um erro indicando nome de Mapa duplicado.

Consultas Simples com EntityManager: Java

WebSphere eXtreme Scale é fornecido com a API de consulta de EntityManager.

A API de consulta EntityManager é muito semelhante a outros mecanismos de consulta SQL que pesquisam sobre objetos. Uma consulta é definida, então o resultado é recuperado da consulta utilizando vários métodos getResult.

Os exemplos a seguir referem-se às entidades usadas no tutorial do EntityManager na Visão Geral do Produto.

Executando uma Consulta Simples

Neste exemplo, os clientes com o sobrenome Claus são consultados:

```
em.getTransaction().begin();

  Query q = em.createQuery("select c from Customer c where c.surname='Claus'");

  Iterator iter = q.getResultIterator();
  while(iter.hasNext())
  {
    Customer c = (Customer)iter.next();
    System.out.println("Found a claus with id " + c.id);
  }

  em.getTransaction().commit();
```

Utilizando Parâmetros

Como você quer localizar todos os clientes com um sobrenome Claus, um parâmetro para especificar o sobrenome é utilizado, visto que você pode utilizar essa consulta mais de uma vez.

Exemplo de Parâmetro Posicional

```
Query q = em.createQuery("select c from Customer c where c.surname=?1");
  q.setParameter(1, "Claus");
```

O uso de parâmetros é muito importante quando a consulta é utilizada mais de uma vez. O EntityManager precisa analisar a cadeia de consultas e construir um plano para a consulta, o qual é caro. Utilizando um parâmetro, o EntityManager armazena em cache o plano para a consulta, reduzindo, assim, o tempo que leva para executar uma consulta.

Os parâmetros posicionais e nomeados são utilizados:

Exemplo de Parâmetro Nomeado

```
Query q = em.createQuery("select c from Customer c where c.surname=:name");
  q.setParameter("name", "Claus");
```

Utilizando um Índice para Melhorar o Desempenho

Se houver milhões de clientes, a consulta anterior precisará varrer sobre todas as linhas no Mapa do Cliente. Isso não é muito eficiente. Mas o eXtreme Scale fornece um mecanismo para definição de índices sobre atributos individuais em uma entidade. A consulta automaticamente utiliza este índice quando apropriado, o que pode acelerar as consultas dramaticamente.

Você pode especificar quais atributos relacionar muito simples, utilizando a anotação @Index no atributo entity:

```
@Entity
public class Customer
{
  @Id String id;
  String firstName;
  @Index String surname;
  String address;
  String phoneNumber;
}
```

O EntityManager cria um índice ObjectGrid apropriado para o atributo surname na entidade Customer e o mecanismo de consulta utiliza automaticamente o índice, o qual diminui bastante o tempo da consulta.

Utilizando a Paginação para Melhorar o Desempenho

Se houver um milhão de clientes chamados Claus, provavelmente você não vai querer exibir uma página que mostra um milhão de clientes. É mais provável que você queira exibir 10 ou 25 clientes de uma vez.

Os métodos Query setFirstResult e setMaxResults ajudam apenas a retornar um subconjunto dos resultados.

Exemplo de Paginação

```
Query q = em.createQuery("select c from Customer c where c.surname=:name");
  q.setParameter("name", "Claus");
  // Display the first page
  q.setFirstResult=1;
  q.setMaxResults=25;
  displayPage(q.getResultIterator());

  // Display the second page
  q.setFirstResult=26;
  displayPage(q.getResultIterator());
```

Referência para Consultas do eXtreme Scale: Java

WebSphere eXtreme Scale tem sua própria linguagem por meio da qual o usuário pode consultar dados.

Cláusula FROM de Consulta do ObjectGrid

A cláusula FROM especifica as coleções de objetos aos quais a consulta deve ser aplicada. Cada coleta é identificada ou por um nome de esquema abstrato e uma

variável de identificação, chamada uma variável de intervalo, ou por uma declaração de membro de coleta que identifica um relacionamento com valor único e com vários valores e uma variável de identificação.

Conceitualmente, a semântica da consulta serve para primeiro formar uma coleta temporária de tuplas, referidas como R. As tuplas são compostas de elementos das coletas que são identificadas na cláusula FROM. Cada tupla contém um elemento de cada uma das coleções na cláusula FROM. Todas as combinações possíveis são formadas sujeitas às restrições impostas pelas declarações de membros da coleta. Se algum nome de esquema identificar uma coleta para a qual não existem registros no armazenamento persistente, a coleta temporária R será vazia.

Exemplos utilizando FROM

O objeto DeptBean contém os registros 10, 20 e 30. O objeto EmpBean contém os registros 1, 2 e 3 que são relacionados ao departamento 10 e os registros 4 e 5 que são relacionados ao departamento 20. O departamento 30 não possui funcionários.

```
FROM DeptBean d, EmpBean e
```

Essa cláusula forma uma coleta temporária R que contém 15 tuplas.

```
FROM  DeptBean d,  DeptBean d1
```

Essa cláusula forma uma coleta temporária R que contém 9 tuplas.

```
FROM  DeptBean d,  IN (d.emps) AS e
```

Essa cláusula forma uma coleta temporária R que contém 5 tuplas. O departamento 30 não está na coleta temporária R porque não contém funcionários. O departamento 10 estará contido na coleta temporária R três vezes e o departamento 20 estará contido em R duas vezes.

Em vez de utilizar IN(d.emps) como e, será possível utilizar um predicado JOIN:

```
FROM DeptBean d JOIN d.emps as e
```

Depois de formar a coleta temporária, as condições de procura da cláusula WHERE serão aplicadas à coleta temporária R e isso produzirá uma nova coleta temporária R1. As cláusulas ORDER BY e SELECT são aplicadas a R1 para resultar no conjunto de resultados final.

Uma variável de identificação é uma variável declarada na cláusula FROM utilizando o operador IN ou o operador AS opcional.

```
FROM DeptBean AS d,  IN (d.emps) AS e
```

é equivalente a:

```
FROM DeptBean d, IN (d.emps) e
```

Uma variável de identificação que é declarada para ser um nome de esquema abstrato é chamada uma variável de faixa. Na consulta anterior, "d" é uma variável de intervalo. Uma variável de identificação que é declarada para ser uma

expressão de caminho com diversos valores é chamada uma declaração de membro de coleta. Os valores "d" e "e" no exemplo anterior são declarações do membro de coleta.

A seguir, está um exemplo de utilização de uma expressão de caminho com valor único na cláusula FROM:

```
FROM EmpBean e, IN(e.dept.mgr) as m
```

Cláusula SELECT de Consulta do ObjectGrid

A sintaxe da cláusula SELECT é ilustrada no seguinte exemplo:

```
SELECT { ALL | DISTINCT }  [ seleção , ]*  seleção
selection  ::= {single_valued_path_expression |
                identification_variable |
                OBJECT ( identification_variable) |
        aggregate_functions } [[ AS ] id ]
```

A cláusula SELECT consiste em um ou mais dos seguintes elementos: uma única variável de identificação, definida na cláusula FROM, ou uma expressão de caminho com valor único que é avaliada para referências ou valores do objeto e uma função agregada. É possível utilizar a palavra-chave DISTINCT para eliminar as referências duplicadas.

Uma subseleção-escalar é uma subseleção que retorna um único valor.

Exemplos utilizando SELECT

Localizar todos os funcionários que ganham mais que João:

```
SELECT OBJECT(e) FROM EmpBean ej, EmpBean eWHERE  ej.name = 'John'  and
e.salary > ej.salary
```

Localizar todos os departamentos que têm um ou mais funcionários que ganham menos de 20000:

```
SELECT DISTINCT e.dept  FROM EmpBean e where e.salary < 20000
```

Uma consulta que pode ter uma expressão de caminho que seja avaliada para um valor arbitrário:

```
SELECT e.dept.name  FROM EmpBean e where e.salary < 20000
```

A consulta anterior retorna uma coleta de valores de nomes para os departamentos que possuem funcionários que ganham menos de 20000.

Uma consulta pode retornar um valor agregado:

```
SELECT  avg(e.salary)  FROM EmpBean e
```

Uma consulta que recupera os nomes e as referências do objeto para funcionário não remunerados a seguir:

```
SELECT e.name as name, object(e) as emp from EmpBean e where e.salary <
50000
```

Cláusula WHERE de Consulta do ObjectGrid

A cláusula WHERE contém condições de procura que são compostos dos elementos apresentados abaixo. Quando uma condição de procura é avaliada como TRUE, a tupla é incluída no conjunto de resultados.

Literais de Consulta do ObjectGrid

Um literal de cadeia é delimitado por aspas simples. Uma aspa simples que ocorre dentro de uma cadeia literal é representada por duas aspas simples, por exemplo: 'Tom''s'.

Um literal numérico pode ser qualquer um dos seguintes valores:

- Um valor exato como 57, -957 ou +66
- Qualquer valor suportado pelo tipo long Java
- Um literal decimal como 57,5 ou -47,02
- Um valor numérico aproximado como 7E3 ou -57.4E-2
- Tipos float devem incluir o qualificador "F", por exemplo, 1.0F
- Tipos long devem incluir o qualificador "L", por exemplo, 123L

Os literais booleanos são TRUE e FALSE.

Os literais temporais seguem a sintaxe de escape JDBC baseada no tipo de atributo:

- java.util.Date: aaaa-mm-ss
- java.sql.Date: aaaa-mm-ss
- java.sql.Time: hh-mm-ss
- java.sql.Timestamp: aaaa-mm-dd hh:mm:ss.f...
- java.util.Calendar: aaaa-mm-dd hh:mm:ss.f...

Os literais de enumeração são expressos usando a sintaxe de literal de enumeração Java com um nome de classe de enumeração completo.

Parâmetros de Entrada de Consulta do ObjectGrid

É possível especificar parâmetros de entrada utilizando uma posição ordinal ou um nome de variável. A gravação de consultas que utilizam parâmetros de entrada é bastante incentivada, porque o uso de parâmetros de entrada aumenta o desempenho, permitindo que o ObjectGrid capture o plano da consulta entre ações em execução.

Um parâmetro de entrada pode ser um dos seguintes tipos: Byte, Short, Integer, Long, Float, Double, BigDecimal, BigInteger, String, Boolean, Char, java.util.Date, java.sql.Date, java.sql.Time, java.sql.Timestamp, java.util.Calendar, uma enumeração Java SE 5, uma Entity ou POJO Object ou uma cadeia de dados binários no formato Java byte[].

Um parâmetro de entrada não pode ter um valor NULL. Para procurar pela ocorrência de um valor NULL, utilize o predicado NULL.

Parâmetros Posicionais

Os parâmetros de entrada posicionais são definidos utilizando um ponto de interrogação seguido por um número positivo:

```
?[inteiro positivo].
```

Parâmetros de entrada posicionais são numerados iniciando em 1 e correspondem aos argumentos da consulta; portanto, uma consulta não deve conter um parâmetro de entrada que exceda o número de argumentos de entrada.

Exemplo: `SELECT e FROM Employee e WHERE e.city = ?1 and e.salary >= ?2`

Parâmetros Denominados

Os parâmetros de entrada denominados são definidos utilizando um nome de variável no formato: :[nome do parâmetro].

Exemplo: `SELECT e FROM Employee e WHERE e.city = :city and e.salary >= :salary`

Predicado BETWEEN de Consulta do ObjectGrid

O predicado BETWEEN determina se um valor dado está entre dois outros valores dados.

```
expressão  [NOT]  BETWEEN expressão-2  AND expressão-3
```

Exemplo 1

```
e.salary BETWEEN 50000 AND 60000
```

é equivalente a:

```
e.salary >= 50000  AND e.salary <= 60000
```

Exemplo 2

```
e.name NOT BETWEEN 'A' AND 'B'
```

é equivalente a:

```
e.name < 'A'  OR e.name > 'B'
```

Predicado IN de Consulta do ObjectGrid

O predicado IN compara um valor a um conjunto de valores. É possível utilizar o predicado IN em um dos dois formatos:

```
expression [NOT] IN ( subselect )expression [NOT] IN  ( value1, value2,
.... )
```

O valor ValorN pode ser um valor literal ou um parâmetro de entrada. A expressão não pode ser avaliada para um tipo de referência.

Exemplo 1

```
e.salary IN ( 10000, 15000 )
```

é equivalente a

```
( e.salary = 10000  OR  e.salary = 15000 )
```

Exemplo 2

```
e.salary IN ( select  e1.salary from EmpBean e1 where e1.dept.deptno = 10)
```

é equivalente a

```
e.salary = ANY   ( select  e1.salary from EmpBean e1 where e1.dept.deptno =
10)
```

Exemplo 3

```
e.salary NOT IN ( select  e1.salary from EmpBean e1 where e1.dept.deptno =
10)
```

é equivalente a

```
e.salary <> ALL    ( select  e1.salary from EmpBean e1 where e1.dept.deptno
= 10)
```

Predicado LIKE de Consulta do ObjectGrid

O predicado LIKE pesquisa um valor de cadeia para um certo padrão.

```
expressão-de-cadeia   [NOT]  LIKE  padrão    [ ESCAPE caractere-de-escape ]
```

O valor padrão é uma cadeia literal ou marcador de parâmetro do tipo string no qual o sublinhado (_) representa qualquer caractere único e o símbolo de percentual (%) representa qualquer sequência de caracteres, incluindo uma sequência vazia. Qualquer outro caractere significa ele próprio. O caractere de escape pode ser utilizado para pesquisar os caracteres _ e %. O caractere de escape pode ser especificado como um literal de cadeia ou um parâmetro de entrada.

Se a expressão-de-cadeia for nula, o resultado será desconhecido.

Se a expressão-de-cadeia e o padrão forem ambos vazios, o resultado será true.

Exemplo

```
'' LIKE '' is true
'' LIKE '%' is true
e.name LIKE '12%3' is true for '123' '12993' and false for '1234'
e.name LIKE 's_me' is true for 'some' and 'same', false for 'soome'
e.name LIKE '/_foo' escape '/' is true for '_foo', false for 'afoo'
e.name LIKE '//_foo' escape '/' is true for '/afoo' and for '/bfoo'
e.name LIKE '///_foo' escape '/' is true for '/_foo' but false for '/afoo'
```

Predicado NULL de Consulta do ObjectGrid

O predicado NULL testa a ocorrência de valores nulos.

```
{expressão-de-caminho-com-valor-único | parâmetro_de_entrada} IS [NOT] NULL
```

Exemplo

```
e.name IS NULL
e.dept.name IS NOT NULL
e.dept IS NOT NULL
```

Predicado de Coleta EMPTY de Consulta do ObjectGrid

Utilize o predicado de coleta EMPTY para testar uma coleta vazia.

Para testar se um relacionamento com vários valores é vazio, utilize a seguinte sintaxe:

```
expressão-de-caminho-com-valor-de-coleção  IS [NOT]  EMPTY
```

Exemplo

Predicado de coleta vazio para localizar todos os departamentos que não possuem funcionários:

```
SELECT OBJECT(d) FROM DeptBean d  WHERE  d.emps IS EMPTY
```

Predicado MEMBER OF de Consulta do ObjectGrid

A expressão a seguir testa se a referência de objeto especificada pela expressão de caminho com valor único ou parâmetro de entrada é um membro da coleta designada. Se a expressão de caminho com valor da coleta designar uma coleta vazia o valor da expressão MEMBER OF será FALSE.

```
{ expressão-de-caminho-com-valor-único | parâmetro_de_entrada } [ NOT ]
MEMBER [ OF ] expressão-de-caminho-com-valor-de-coleção
```

Exemplo

Localizar funcionários que não são membros de um número de departamento dado:

```
SELECT OBJECT(e) FROM EmpBean e , DeptBean d
WHERE e NOT MEMBER OF d.emps AND d.deptno = ?1
```

Localizar funcionários cujo gerente é um membro de um número de departamento dado:

```
SELECT OBJECT(e) FROM EmpBean e, DeptBean d
WHERE e.dept.mgr MEMBER  OF d.emps  and d.deptno=?1
```

Predicado EXISTS de Consulta do ObjectGrid

O predicado EXISTS testa a presença ou ausência de uma condição especificada por uma subseleção.

```
EXISTS ( subseleção )
```

O resultado de EXISTS será true se a subseleção retornar pelo menos um valor; caso contrário, o resultado será false.

Para negar um predicado EXISTS, preceda-o com o operador lógico NOT.

Exemplo

Retornar departamentos que têm pelo menos um funcionário ganhando mais que 1000000:

```
SELECT OBJECT(d) FROM DeptBean d
WHERE EXISTS ( SELECT  e  FROM IN (d.emps) e WHERE  e.salary > 1000000 )
```

Retornar departamentos que não têm funcionários

```
SELECT OBJECT(d) FROM DeptBean d
WHERE NOT EXISTS  ( SELECT e FROM IN (d.emps) e)
```

É possível reescrever a consulta anterior como no exemplo a seguir:

```
SELECT OBJECT(d) FROM DeptBean d WHERE SIZE(d.emps)=0
```

Cláusula ORDER BY de Consulta do ObjectGrid

A cláusula ORDER BY especifica uma ordenação dos objetos na coleta de resultados. Este é um exemplo:

ORDER BY [order_element ,]* order_element order_element ::={ path-expression }[ASC | DESC]

A expressão de caminho deve especificar um campo de valor único que é um tipo primitivo de byte, short, int, long, float, double, char, ou um tipo de wrapper de Byte, Short, Integer, Long, Float, Double, BigDecimal, String, Character, java.util.Date, java.sql.Date, java.sql.Time, java.sql.Timestamp e java.util.Calendar. O elemento de ordem ASC especifica que os resultados são exibidos em ordem crescente, que é o padrão. Um elemento de ordem DESC especifica que os resultados são exibidos em ordem decrescente.

Exemplo

Retornar objetos do departamento. Exibir os números de departamento em ordem decrescente:

```
SELECT  OBJECT(d) FROM  DeptBean d ORDER BY  d.deptno DESC
```

Retornar objetos de funcionário, classificados por número de departamento e nome:

```
SELECT  OBJECT(e) FROM EmpBean e ORDER BY e.dept.deptno ASC,  e.name DESC
```

Funções de Agregação de Consulta do ObjectGrid

As funções de agregação operam em um conjunto de valores para retornar um valor escalar único. É possível utilizar essas funções nos métodos select e subselect. O exemplo a seguir ilustra uma agregação:

```
SELECT  SUM (e.salary) FROM EmpBean e WHERE e.dept.deptno =20
```

Essa agregação calcula o salário total para o departamento 20.

As funções de agregação são: AVG, COUNT, MAX, MIN e SUM. A sintaxe de uma função de agregação é ilustrada no exemplo a seguir:

```
função-de-agregação  (    [ ALL |  DISTINCT ]  expressão )
```

ou:

```
COUNT( [ ALL |  DISTINCT ] variável de identificação )
```

A opção DISTINCT elimina valores duplicados antes de aplicar a função. A opção ALL é a opção padrão e não elimina valores duplicados. Os valores nulos são

ignorados no cálculo da função agregada, exceto quando você utiliza a função COUNT(identification-variable), que retorna uma contagem de todos os elementos no conjunto.

Definindo o Tipo de Retorno

As funções MAX e MIN podem se aplicar a qualquer tipo de dados numéricos, de cadeia ou de data-hora e retornam o tipo de dados correspondente. As funções SUM e AVG pegam um tipo numérico como entrada. A função AVG retorna um tipo double. A função SUM retorna um tipo long se o tipo de entrada for um tipo integer, exceto quando a entrada for um tipo Java BigInteger, e, em seguida, a função retornar um tipo Java BigInteger. A função SUM retorna um tipo double se o tipo de entrada não for um tipo integer, exceto quando a entrada for um tipo Java BigDecimal, e, em seguida, a função retornar um tipo Java BigDecimal. A função COUNT pode tomar qualquer tipo de dados, exceto coletas, e retorna um tipo long.

Quando aplicadas a um conjunto vazio, as funções SUM, AVG, MAX e MIN podem retornar um valor nulo. A função COUNT retorna zero (0) quando aplicada a um conjunto vazio.

Utilizando cláusulas GROUP BY e HAVING

O conjunto de valores utilizado para a função agregada é determinado pela coleta que resulta da cláusula FROM e WHERE da consulta. É possível dividir o conjunto em grupos e aplicar a função de agregação a cada grupo. Para executar essa ação, utilize uma cláusula GROUP BY na consulta. A cláusula GROUP BY define os membros do agrupamento que compreendem uma lista de expressões de caminho. Cada expressão de caminho especifica um campo que é um tipo primitivo de byte, short, int, long, float, double, boolean, char ou um tipo de wrapper de Byte, Short, Integer, Long, Float, Double, BigDecimal, String, Boolean, Character, java.util.Date, java.sql.Date, java.sql.Time, java.sql.Timestamp e java.util.Calendar ou um Java SE 5 enum.

O exemplo a seguir ilustra a utilização da cláusula GROUP BY em uma consulta que calcula o salário médio para cada departamento:

```
SELECT e.dept.deptno,  AVG ( e.salary) FROM EmpBean e GROUP BY
e.dept.deptno
```

Na divisão de um conjunto em grupos, um valor NULL é considerado igual a outro valor NULL.

Os grupos podem ser filtrados utilizando uma cláusula HAVING, que testa as propriedades de grupo antes de envolver funções agregadas ou membros do agrupamento. Essa filtragem é similar a como a cláusula WHERE filtra tuplas (isto é, registros dos valores de coleta de retorno) da cláusula FROM. Um exemplo da cláusula HAVING é o seguinte:

```
SELECT e.dept.deptno,  AVG ( e.salary) FROM EmpBean e
GROUP BY e.dept.deptno
HAVING COUNT(e) > 3 AND e.dept.deptno > 5
```

Essa consulta retorna o salário médio para departamentos que possuem mais de três funcionários e o número de departamentos é maior que cinco.

É possível utilizar a cláusula HAVING sem uma cláusula GROUP BY. Nesse caso, todo o conjunto é tratado como um único grupo, ao qual a cláusula HAVING é aplicada.

Backus-Naur Form de Consulta do ObjectGrid: Java

A seguir, está um resumo da Notação Backus-Naur Form (BNF) de Consulta do ObjectGrid.

Tabela 13. Chave para o Resumo BNF

Representação	Descrição
{...}	Agrupamento
[...]	Construções opcionais
negrito	Palavras-Chave
*	Zero ou mais
|	Alternativas

```
ObjectGrid QL ::=select_clause from_clause [where_clause]
[group_by_clause] [having_clause] [order_by_clause]

from_clause
::=FROM identification_variable_declaration [,identification_variable_declaration]*

identification_variable_declaration::=collection_member_declaration |
  range_variable_declaration

collection_member_declaration
::=IN ( collection_valued_path_expression | single_valued_navigation)
[AS] identifier | [LEFT [OUTER] | INNER] JOIN collection_valued_path_expression
| single_valued_navigation [AS] identifier

range_variable_declaration
::=abstract_schema_name [AS] identifier

single_valued_path_expression
::={single_valued_navigation | identification_variable}.
  { state_field
| state_field.value_object_attribute } | single_valued_navigation

single_valued_navigation
::=identification_variable.[ single_valued_association_field. ]*
  single_valued_association_field

collection_valued_path_expression
::=identification_variable.[ single_valued_association_field. ]* collection_valued_association_field

select_clause
::= SELECT [DISTINCT] [ selection , ]* selection

selection
::= {single_valued_path_expression |identification_variable | OBJECT (
identification_variable) |aggregate_functions } [[ AS ] id
]

order_by_clause ::= ORDER BY [ {identification_variable.[
single_valued_association_field.
  ]*state_field} [ASC|DESC],]*
{identification_variable.[ single_valued_association_field. ]*state_field}[ASC|DESC]

where_clause
::= WHERE conditional_expression

conditional_expression
::= conditional_term | conditional_expression OR conditional_term

conditional_term
::= conditional_factor | conditional_term AND conditional_factor

conditional_factor
::= [NOT] conditional_primary

conditional_primary::=simple_cond_expression | (conditional_expression)

simple_cond_expression
::= comparison_expression | between_expression | like_expression |
in_expression | null_comparison_expression | empty_collection_comparison_expression
| exists_expression | collection_member_expression
```

```
between_expression
::= numeric_expression [NOT] BETWEEN numeric_expression AND numeric_expression
| string_expression [NOT] BETWEEN string_expression AND string_expression
| datetime_expression [NOT] BETWEEN datetime_expression AND datetime_expression

in_expression
::= identification_variable.[ single_valued_association_field. ]state_field
[*NOT] IN { (subselect) | ( atom ,]* atom) }

atom
::= { string_literal | numeric_literal | input_parameter }

like_expression
::=string_expression [NOT] LIKE {string_literal | input_parameter}
[ESCAPE {string_literal | input_parameter}]

null_comparison_expression
::= {single_valued_path_expression | input_parameter} IS [ NOT ] NULL

empty_collection_comparison_expression
::= collection_valued_path_expression IS [NOT] EMPTY

collection_member_expression
::={ ssingle_valued_path_expression | input_parameter }[ NOT ] MEMBER [
OF ]collection_valued_path_expression

exists_expression ::= EXISTS {(subselect)}

subselect
::= SELECT [{ ALL | DISTINCT }] subselection
from_clause [where_clause] [group_by_clause] [having_clause]

subselection
::= {single_valued_path_expression |identification_variable | aggregate_functions
}

group_by_clause ::= GROUP BY[single_valued_path_expression,]*
single_valued_path_expression

having_clause ::= HAVING conditional_expression

comparison_expression
::= numeric_ expression comparison_operator { numeric_expression |
{SOME | ANY | ALL}(subselect) } | string_expression
comparison_operator {

string_expression | {SOME | ANY | ALL}(subselect)
} |

datetime_expression comparison_operator {

datetime_expression
{SOME | ANY | ALL}(subselect) } |

boolean_expression
{=|<>} {

boolean_expression {SOME | ANY | ALL}(subselect)
} |

entity_expression {=|<>} {

entity_expression {SOME| ANY | ALL}(subselect)
}

comparison_operator ::= = | > | >= | < | <= | <>

string_expression
::= string_primary | (subselect)

string_primary ::=state_field_path_expression
|string_literal | input_parameter | functions_returning_strings

datetime_expression
::= datetime_primary |(subselect)

datetime_primary ::=state_field_path_expression
| string_literal | long_literal | input_parameter | functions_returning_datetime

boolean_expression
::= boolean_primary |(subselect)

boolean_primary ::=state_field_path_expression
| boolean_literal | input_parameter

entity_expression ::=single_valued_association_path_expression |
  identification_variable | input_parameter

numeric_expression
::= simple_numeric_expression |(subselect)

simple_numeric_expression
::= numeric_term | numeric_expression {+|-} numeric_term
```

```
numeric_term
::= numeric_factor | numeric_term {*|/} numeric_factor

numeric_factor
::= {+|-} numeric_primary

numeric_primary ::= single_valued_path_expression
| numeric_literal | ( numeric_expression ) | input_parameter | functions

aggregate_functions :=

AVG([ALL|DISTINCT] identification_variable.[
single_valued_association_field. ]*state_field) |

COUNT([ALL|DISTINCT]
{single_valued_path_expression | identification_variable}) |

MAX([ALL|DISTINCT]
identification_variable.[ single_valued_association_field. ]*state_field) |

MIN([ALL|DISTINCT] identification_variable.[
single_valued_association_field. ]*state_field) |

SUM([ALL|DISTINCT]
identification_variable.[ single_valued_association_field. ]*state_field)

functions ::=

ABS (simple_numeric_expression) |

CONCAT (string_primary
, string_primary) |

LOWER (string_primary) |

LENGTH(string_primary)
|

LOCATE(string_primary, string_primary [, simple_numeric_expression])
|

MOD (simple_numeric_expression, simple_numeric_expression)
|

SIZE (collection_valued_path_expression) |

SQRT (simple_numeric_expression)
|

SUBSTRING (string_primary, simple_numeric_expression[,
simple_numeric_expression]) |

UPPER (string_primary)
|

TRIM ([[LEADING | TRAILING | BOTH]
[trim_character] FROM] string_primary)
```

Notificando Clientes de Atualizações do Mapa Utilizando a Consulta Contínua

É possível ser notificado em sua Java virtual machine (JVM) do cliente quando objetos ou entradas são inseridas ou atualizadas na grade de dados.

Antes de Iniciar

Se desejar utilizar a consulta contínua, você deverá ativar o IBM eXtremeIO, que é um mecanismo de transporte, utilizado para comunicação entre os servidores de contêiner e clientes. Para obter mais informações sobre como ativar o eXtremeIO, consulte "Configurando o IBM eXtremeIO (XIO)" na página 119.

Sobre Esta Tarefa

Ao desenvolver aplicativos clientes que interagem com a grade de dados, você pode requerer consultas que recuperam resultados automáticos em tempo real quando entradas que correspondem aos critérios de filtragem são inseridas, atualizadas ou excluídas. Por exemplo, você desenvolve um aplicativo de cotação de ações que requer atualizações frequentes. Essas atualizações refletem mudanças que ocorrem no mercado de ações. Portanto, é crítico que seu aplicativo seja notificado sobre alterações instantaneamente, para que você possa fornecer

resultados precisos e oportunos. A consulta continua tem uma área de cobertura de memória baixa que pode notificar clientes proativamente conforme as alterações na grade de dados ocorrem.

Utilize o seguinte procedimento para programar seus aplicativos clientes para utilizar a consulta contínua.

Procedimento

1. Chame o gerenciador de consulta contínua no aplicativo cliente. Por exemplo, insira a seguinte linha de código:

   ```
   ContinuousQueryManager cqMan = ContinuousQueryManagerFactory.getManager(og);
   ```

2. Defina um filtro ou uma cadeia de filtros. É possível implementar seus próprios filtros, ou você pode usar os seguintes filtros básicos que são fornecidos: `AND`, `OR`, `LT`, `GT`, `EQ`, e assim por diante. Os filtros e cadeias de filtros instanciados recebem identificações exclusivas. Para obter mais informações sobre todos os filtros suportados, consulte "Acessando a Documentação da API Java" na página 338 para localizar as APIs de consulta contínua.

   O exemplo de código a seguir demonstra uma maneira de utilizar o filtro básico equals (EQ). Suponha que a grade de dados contém objetos Customer com o campo `firstName`. O filtro retornará `true` quando `firstName` for igual a `Larry`.

   ```
   EQFilter<String, String> equalsFilter = new EQFilter<String, String>("firstName", "Larry");
   ```

3. Defina uma consulta utilizando o filtro que você criou na etapa anterior; por exemplo:

   ```
   ContinuousQueryTopicImpl<String, Customer> topic =
     cqMan.<String, Customer> defineContinuousQuery("myMapName", equalsFilter, true, true, true);
   ```

4. Opcional: Obtenha o cache de consulta contínua para acessar os resultados do lado do cliente da consulta contínua. Se a consulta for definida como uma consulta somente de chaves, apenas as chaves que satisfazem a consulta estarão no cache de consulta contínua; por exemplo:

   ```
   ContinuousQueryCache cache = topic.getCache();
   ```

5. Opcional: Além disso, você pode registrar uma classe que implementa a interface ContinuousQueryListener com uma instância ContinuousQueryTopic para receber notificações quando os resultados da consulta contínua são alterados. Chame o método addListener para registrar o listener; por exemplo:

   ```
   ContinuousQueryListener<String, Customer> listener = new MyCQListener<String, Customer>();
   topic.addListener(listener);
   ```

O que Fazer Depois

Consulte Documentação da API: Pacote com.ibm.websphere.objectgrid.continuousquery para obter informações adicionais sobre a API de consulta contínua.

Programação para Transações

Java

Os aplicativos que requerem transações introduzem considerações como bloqueios de manipulação, colisões de manipulação e isolamento de transação.

Visão Geral do Processamento de Transações: Java

O WebSphere eXtreme Scale usa transações de acordo com seu mecanismo de interação com os dados.

Para interagir com os dados, o encadeamento em seu aplicativo precisa de sua própria sessão. Quando o aplicativo desejar usar o ObjectGrid em um encadeamento, chame um dos métodos ObjectGrid.getSession para obter uma sessão. Com a sessão, o aplicativo pode trabalhar com dados que são armazenados nos mapas ObjectGrid.

Quando um aplicativo usa um objeto de Sessão, a sessão deve estar no contexto de uma transação. Uma transação inicia e é consolidada ou inicia e é recuperada usando os métodos begin, commit e rollback no objeto de Sessão. Os aplicativos também podem trabalhar em modo de auto-consolidação, no qual a Sessão inicia e consolida automaticamente uma transação sempre que uma operação é executada no mapa. O modo de auto-confirmação não pode agrupar várias operações em uma única transação, assim, ele é a opção mais lenta se você estiver criando um lote de várias operações em uma única transação. Porém, para transações que contêm uma operação, a auto-consolidação é a opção mais rápida.

Quando seu aplicativo for finalizado com a Sessão, use o método opcional Session.close() para fechar a sessão. O fechamento da Sessão faz a liberação do heap e permite que chamadas subsequentes para o método getSession() sejam reutilizadas, melhorando o desempenho.

Tarefas relacionadas:

Java "Resolvendo Exceções de Tempo Limite do Bloqueio" na página 892
Usando o comando **xscmd -c listindoubt**, é possível visualizar o estado de uma transação e determinar um curso de ação.

Java "Resolução de Problemas de Exceções de Tempo Limite do Bloqueio para uma Transação Multipartição" na página 890
O cenário que é descrito é um exemplo de uma transação multipartição que está causando uma exceção de tempo limite de bloqueio. Dependendo do estado da transação, as soluções ilustram como você pode resolver esse problema manualmente.

Acesso a Dados e Transações: Java

Após um aplicativo fazer uma referência a uma instância ObjectGrid ou uma conexão do cliente com uma grade de dados remota, é possível acessar e interagir com os dados em sua grade de dados. Com a API do ObjectGridManager, é possível criar uma instância local ou estabelecer uma conexão do cliente com uma instância distribuída. Para criar uma instância local, use um dos métodos createObjectGrid. Para estabelecer uma conexão do cliente com uma grade de dados remota, use o método getObjectGrid.

Um encadeamento em um aplicativo precisa de sua própria Sessão. Quando você desejar que seu aplicativo use o ObjectGrid em um encadeamento, chame um dos métodos getSession para obter uma Sessão. Após o aplicativo ser concluído com a Sessão, chame o método Session.close(). Esse método fecha a sessão retornando-a para o conjunto e liberando seus recursos. Fechar a sessão é opcional, mas melhora o desempenho das chamadas subsequentes para o método getSession(). Se o aplicativo estiver usando uma estrutura de injeção independente como Spring, é possível injetar uma Sessão em um bean de aplicativo quando necessário.

Após obter uma Sessão, o aplicativo pode acessar dados armazenados em mapas no ObjectGrid. Se o ObjectGrid usar entidades, é possível usar a API de EntityManager, que pode ser obtida com o método Session.getEntityManager. Porque ele está mais próxima das especificações Java, a interface EntityManager é mais simples que a API baseada em mapa. Porém, a API de EntityManager

transporta um gasto adicional de desempenho porque controla as alterações em objetos. A API baseada em mapa é obtida usando o método Session.getMap.

O WebSphere eXtreme Scale usa transações. Quando um aplicativo interage com Session, ele deve estar no contexto de uma transação. Uma transação é iniciada e consolidade ou retrocedida usando os métodos Session.begin, Session.commit e Session.rollback no objeto Sessão. Os aplicativos também podem funcionar no modo auto-commit, no qual Session inicia automaticamente e executa o commit de uma transação sempre que o aplicativo interagem com Mapas. Entretanto, o modo de auto-consolidação é mais lento.

A Lógica de Utilização de Transações

As transações parecem estar lentas. Você deve usar as transações pelas razões a seguir:

1. Para permitir o retrocesso das alterações se uma exceção ocorrer ou se a lógica de negócios precisar desfazer alterações de estado.
2. Para manter bloqueios nos dados e liberar bloqueios dentro do ciclo de vida de uma transação, permitindo que um conjunto de alterações seja feito atomicamente, ou seja, todas as alterações ou nenhuma alteração nos dados.
3. Para produzir uma unidade atômica de replicação.

É possível customizar o quanto é necessário o suporte a transações. Seu aplicativo pode desligar o suporte ao retrocesso e bloqueio, mas ele faz isso com prejuízo para o aplicativo. O aplicativo deve manipular a falta desses recursos.

Por exemplo, um aplicativo pode desligar o bloqueio configurando a estratégia de bloqueio de BackingMap para que seja NONE. Esta estratégia é rápida, mas transações simultâneas agora podem modificar os mesmos dados sem nenhuma proteção uma da outra. O aplicativo é responsável por todos os bloqueios e consistências de dados quando NONE é utilizado.

Um aplicativo também pode alterar a maneira como os objetos são copiados quando acessados pela transação. O aplicativo pode especificar como os objetos são copiados com o método ObjectMap.setCopyMode. Com este método, é possível desligar CopyMode. Desligar CopyMode normalmente é usado para transações somente de leitura se diferentes valores podem ser retornados para o mesmo objeto dentro de uma transação. Valores diferentes podem ser retornados para o mesmo objeto dentro de uma transação.

Por exemplo, se a transação chamou o método ObjectMap.get para o objeto em T1, ela obtém o valor naquele ponto no tempo. Se ela chamar o método get novamente dentro dessa transação em um tempo posterior T2, outro encadeamento pode ter alterado o valor. Em razão do valor ter sido alterado por outro encadeamento, o aplicativo vê um valor diferente. Se o aplicativo modifica um objeto recuperado usando um valor de CopyMode NONE, ele está alterando a cópia consolidada desse objeto diretamente. A recuperação da transação não faz sentido neste modo. Você está alterando a única cópia no ObjectGrid. Apesar do uso de CopyMode NONE ser rápido, esteja ciente de suas consequências. Um aplicativo que usa o CopyMode NONE nunca deve retroceder a transação. Se o aplicativo retroceder a transação, os índices não são atualizados com as alterações *e* as alterações não são replicadas se a replicação estiver desativada. Os valores padrão são fáceis de usar e menos propensos a erros. Se você começar a trocar desempenho por dados menos confiáveis, o aplicativo precisará estar ciente do que está fazendo para evitar problemas indesejados.

CUIDADO:
Tome cuidado ao alterar os valores de bloqueio ou de CopyMode. Se você alterar os valores, ocorre um comportamento imprevisível do aplicativo.

Interação de Dados Armazenados

Após obter uma sessão, é possível usar o fragmento de código a seguir para usar a API do Mapa para inserir dados.

```
Session session = ...;
ObjectMap personMap = session.getMap("PERSON");
session.begin();
Person p = new Person();
p.name = "John Doe";
personMap.insert(p.name, p);
session.commit();
```

O mesmo exemplo usando a API do EntityManager está a seguir. Esta amostra de código supõe que o objeto Pessoal é mapeado para uma Entidade.

```
Session session = ...;
EntityManager em = session.getEntityManager();
session.begin();
Person p = new Person();
p.name = "John Doe";
em.persist(p);
session.commit();
```

O padrão é projetado para obter referências aos ObjectMaps para os Mapas com os quais o encadeamento trabalha, inicia uma transação, trabalha com os dados e depois consolida a transação.

A interface ObjectMap tem as operações de Mapa comuns, como put, get e remove. Porém, use os nomes de operação mais específicos como: get, getForUpdate, insert, update e remove. Esses nomes de métodos expressam o intento mais precisamente que as APIs de Mapa tradicionais.

Nota: 8.6+ Os métodos upsert e upsertAll substituem os métodos put e putAll do ObjectMap. Use o método upsert para informar ao BackingMap e carregador que uma entrada na grade de dados precisa colocar a chave e o valor na grade. O BackingMap e carregador executam uma inserção ou uma atualização para colocar o valor na grade e no carregador. Se você executar a API upsert dentro de seus aplicativos, o carregador obterá um tipo UPSERT de LogElement, que permite que carregadores façam a mesclagem do banco de dados ou chamadas upsert em vez de usar insert ou update.

Também é possível usar o suporte à indexação, que é flexível.

Consulte o exemplo a seguir para atualização de um Objeto:

```
session.begin();
Person p = (Person)personMap.getForUpdate("John Doe");
p.name = "John Doe";
p.age = 30;
personMap.update(p.name, p);
session.commit();
```

Normalmente o aplicativo usa o método getForUpdate em vez de um get simples para bloquear o registro. O método update deve ser chamado para fornecer o valor atualizado para o mapa. Se o método update não for chamado, então o mapa não é alterado. O código a seguir é o mesmo fragmento usando a API de EntityManager:

```
session.begin();
Person p = (Person)em.findForUpdate(Person.class, "John Doe");
p.age = 30;
session.commit();
```

A API de EntityManager é mais simples que a abordagem de Mapa. Neste caso, o eXtreme Scale localiza a Entidade e retorna um objeto gerenciado para o aplicativo. O aplicativo modifica o objeto e consolida a transação, e o eXtreme Scale controla as alterações para objetos gerenciados automaticamente no tempo de consolidação e executa as atualizações necessárias.

Transações e Partições

Transações do WebSphere eXtreme Scale podem atualizar uma partição única ou diversas partições, no entanto, a atualização de uma partição única é o comportamento padrão. É possível ativar um protocolo two-phase commit chamando o método a seguir:
`session.setTxCommitProtocol(Session.TxCommitProtocol.TWOPHASE);`
`session.begin();` O fragmento de código a seguir ilustra como criar, recuperar, atualizar e excluir operações em uma grade com um protocolo two-phase commit:

```
Session session = og.getSession();
Objectmap map1 = session.getMap("Map1");
Objectmap map2 = session.getMap("Map2");
Objectmap map3 = session.getMap("Map3");
session.setTxCommitProtocol(Session.TxCommitProtocol.TWOPHASE);
session.begin();
map1.insert("randKey345", "HelloMap1");
map2.insert("randKey58901", "HelloMap2");
map3.insert("randKey58", "HelloMap3");
session.commit();
```

Utilize a nova API de Sessão TxCommitProtocol configurada para ativar o suporte a transações multipartição para o WebSphere eXtreme Scale em um ambiente independente. A nova API fornece as duas opções a seguir:

- TxCommitProtocol.ONEPHASE: Este é o padrão. As transações de um cliente podem ler de múltiplas partições, mas podem atualizar uma partição única. Tentativas feitas para atualizar várias partições falharão.
- TxCommitProtocol.TWOPHASE: Transação a partir de um cliente pode ler e atualizar várias partições. A transação utiliza o protocolo two-phase commit para assegurar que os dados gravados nas partições sejam automaticamente confirmados ou recuperados. Se a transação grava apenas em uma única partição, um protocolo one-phase commit é utilizado. O recurso depende do novo protocolo eXtremeIO.

É necessário ativar e configurar o eXtremeIO antes de configurar múltiplas transações com o WebSphere eXtreme Scale. Para obter informações adicionais, consulte “Configurando o IBM eXtremeIO (XIO)” na página 119.

Consultas e Partições

Se uma transação já buscou por uma Entidade, a transação é associada com a partição para essa Entidade. Quaisquer consultas que executam em uma transação que está associada com uma Entidade são roteadas para a partição associada.

Se uma consulta é executada em uma transação antes de ser associada com uma partição, você deve configurar o ID da partição a ser usado para a consulta. O ID

da partição é um valor de número inteiro. A consulta é, então, roteada para essa partição. Isto se aplica apenas se a transação for configurada para utilizar um protocolo one-phase commit.

As consultas pesquisam somente dentro de uma única partição. No entanto, se a sessão for configurada utilizando um protocolo two-phase commit, configure o ID de partição para a consulta como -1. Isto busca resultados de todas as partições. É possível utilizar as APIs do DataGrid para executar a mesma consulta em paralelo em todas as partições ou em um subconjunto de partições. Use as APIs do DataGrid para localizar uma entrada que podem estar em qualquer partição.

O serviço de dados REST permite que qualquer cliente HTTP acesse uma grade de dados, além de ser compatível com WCF Data Services no Microsoft .NET Framework 3.5 SP1. Para obter informações adicionais, consulte Configurando Serviços de Dados REST.

.

Tarefas relacionadas:

Java "Desenvolvendo Aplicativos para Gravar Transações de Múltiplas Partições para o WebSphere eXtreme Scale em um Ambiente Independente" na página 487
É possível gravar um aplicativo para uma grade de dados distribuídos com várias partições em seu ambiente independente do WebSphere eXtreme Scale.

Transações: Java

As transações possuem muitas vantagens para o armazenamento e a manipulação de dados. É possível usar transações para proteger a grade de dados contra mudanças simultâneas, para aplicar diversas mudanças como uma unidade simultânea, para replicar dados e para implementar um ciclo de vida para bloqueios em mudanças.

Quando uma transação inicia, o WebSphere eXtreme Scale aloca um mapa de diferença especial para conter as alterações atuais ou cópias dos pares chave e valor que a transação utiliza. Normalmente, quando um par de chave e valor é acessado, o valor é copiado antes de o aplicativo receber o valor. O mapa de diferenças controla todas as alterações de operações, como inserir, atualizar, obter, remover e assim por diante. As chaves não são copiadas porque elas são assumidas como imutáveis. Se um objeto ObjectTransformer for especificado, então, ele será utilizado para copiar o valor. Se a transação estiver utilizando o bloqueio optimistic, as imagens anteriores dos valores também serão rastreadas para comparação quando a transação for confirmada.

Se uma transação for recuperada, as informações do mapa de diferenças serão descartadas e os bloqueios nas entradas serão liberados. Quando uma transação é consolidada, as alterações são aplicadas nos mapas e os bloqueios são liberados. Se o bloqueio otimista estiver sendo utilizado, o eXtreme Scale compara as versões de imagens anteriores dos valores com os valores que estão no mapa. Esses valores devem corresponder para que a transação seja confirmada. Essa comparação permite um esquema de bloqueio de várias versões, mas a um custo de duas cópias sendo feitas quando a transação acessa a entrada. Todos os valores são copiados novamente e a nova cópia é armazenada no mapa. O WebSphere eXtreme Scale executa esta cópia para se proteger do aplicativo alterando a referência do aplicativo para o valor após um commit.

É possível evitar o uso de diversas cópias das informações. O aplicativo pode salvar uma cópia, utilizando o bloqueio pessimistic em vez do bloqueio optimistic como o custo da limitação da simultaneidade. A cópia do valor no momento da confirmação também pode ser evitada se o aplicativo concordar em não alterar um valor após uma confirmação.

Vantagens das Transações

Utilize as transações pelos seguintes motivos:

Usando as transações, você pode:

- Recuperar alterações se ocorrer uma exceção ou a lógica de negócios precisar desfazer mudanças de estado.
- Para aplicar várias alterações como uma unidade atômica no momento commit.
- Mantém e libera bloqueios em dados para aplicar múltiplas alterações como uma unidade atômica no momento da consolidação.
- Protege um encadeamento de alterações concorrentes.
- Implementar um ciclo de vida para bloqueios em mudanças.
- Produz uma unidade atômica de replicação.

Tamanho da Transação

Transações maiores são mais eficientes, especificamente para replicação. No entanto, as transações maiores podem causar impacto adverso na simultaneidade porque os bloqueios nas entradas são retidos por um período maior de tempo. Se você usar transações maiores, é possível aumentar o desempenho de replicação. Este aumento de desempenho é importante quando você estiver pré-carregando um Mapa. Experimente diferentes tipos de batch para determinar qual funciona melhor para o seu cenário.

Transações maiores também ajudam com os utilitários de carga. Se estiver sendo usado um utilitário de carga que possa executar SQL em lote, então ganhos consideráveis no desempenho são possíveis dependendo da transação e de reduções significativas de carga no lado do banco de dados. Esse ganho no desempenho depende da implementação do Carregador.

Modo de Commit Automático

Se nenhuma transação for ativamente iniciada, então quando um aplicativo interage com um objeto ObjectMap, uma operação automática é iniciada e uma consolidação é executada em nome do aplicativo. Esta operação automática de início e consolidação funciona, mas evita que a recuperação e o bloqueio funcionem efetivamente. A velocidade de replicação síncrona sofre um impacto devido ao tamanho de transação muito reduzido. Se estiver usando um aplicativo gerenciador de entidades, então não use o modo de consolidação automática pois os objetos que estiverem bloqueados com o método EntityManager.find se tornarão imediatamente não gerenciados no retorno do método e inutilizáveis.

Coordenadores de Transação Externos

Normalmente, as transações iniciam com o método session.begin e terminam com o método session.commit. Porém, quando o eXtreme Scale está incorporado, as transações podem ser iniciadas e encerradas por um coordenador externo de transações. Se você estiver usando um coordenador de transação externo, não é

necessário chamar o método session.begin e terminar com o método session.commit. Se você estiver usando o WebSphere Application Server, será possível usar o plug-in WebSphereTranscationCallback.

Integração da Transação Java EE

O eXtreme Scale inclui um adaptador de recursos compatível com Java Connector Architecture (JCA) 1.5 que suporta as conexões do cliente em uma grade de dados remotos e o gerenciamento de transação local. Os aplicativos Java Platform, Enterprise Edition (Java EE) como servlets, arquivos JavaServer Pages (JSP) e componentes Enterprise JavaBeans (EJB) podem demarcar as transações do eXtreme Scale usando a interface padrão javax.resource.cci.LocalTransaction ou a interface de sessão do eXtreme Scale.

Ao fazer a execução no WebSphere Application Server com o último suporte participante ativado no aplicativo, é possível relacionar a transação eXtreme Scale em uma transação global com outros recursos transacionais do two-phase commit.

Atributo CopyMode: Java

É possível ajustar o número de cópias ao definir o atributo CopyMode do BackingMap ou objetos ObjectMap no arquivo XML do descritor do ObjectGrid.

É possível ajustar o número de cópias definindo o atributo CopyMode do BackingMap ou objetos ObjectMap. O modo de cópia possui os seguintes valores:

- COPY_ON_READ_AND_COMMIT
- COPY_ON_READ
- NO_COPY
- COPY_ON_WRITE
- COPY_TO_BYTES
- COPY_TO_BYTES_RAW

O valor COPY_ON_READ_AND_COMMIT é o padrão. O valor COPY_ON_READ copia os dados iniciais recuperados, mas não copia no momento da consolidação. Este modo é seguro se o aplicativo não modificar um valor depois de consolidar uma transação. O valor NO_COPY não copia os dados, que são seguros apenas para dados de leitura. Se ele nunca for alterado, não será necessário copiá-lo por motivos de isolamento.

Seja cauteloso ao usar o valor do atributo NO_COPY com mapas que possam ser atualizados. O WebSphere eXtreme Scale utiliza a cópia no primeiro acesso para permitir o retrocesso da transação. O aplicativo alterou apenas a cópia e, como resultado, o eXtreme Scale descarta a cópia. Se o valor de atributo NO_COPY for utilizado e o aplicativo modificar o valor confirmado, não será possível concluir a recuperação. Modificar o valor confirmado conduz a problemas nos índices, replicação e assim por diante porque os índices e as réplicas são atualizadas quando a transação é confirmada. Se você modificar os dados confirmados e, em seguida, recuperar a transação, o que na realidade não é recuperada, os índices não serão atualizados e a replicação não ocorrerá. Os outros encadeamentos podem ver as alterações não confirmadas imediatamente, mesmo se tiverem bloqueios. Utilize o valor de atributo NO_COPY apenas para mapas somente leitura ou para aplicativos que concluem a cópia apropriada antes de modificar o valor. Se você utilizar o valor de atributo NO_COPY e chamar o suporte IBM com um problema de integridade de dados, será necessário reproduzir o problema com o modo de cópia definido como COPY_ON_READ_AND_COMMIT.

O valor COPY_TO_BYTES armazena os valores no mapa de maneira serializada. No tempo de leitura, o eXtreme Scale aumenta o valor de um formato serializado e, no tempo de consolidação, ele armazena o valor em um formato serializado. Com esse método, uma cópia é feita no tempo de leitura e de consolidação.

Restrição: 8.6+

Ao usar o bloqueio otimista com COPY_TO_BYTES, você pode experienciar exceções ClassNotFoundException durante operações comuns, tal como invalidar entradas de cache. Estas exceções ocorrem porque o mecanismo de bloqueio otimista deve chamar o método "equals(...)" do objeto de cache para detectar quaisquer mudanças antes de a transação ser confirmada. Para chamar o método equals(...), o servidor eXtreme Scale deve poder desserializar o objeto em cache, o que significa que eXtreme Scale deve carregar a classe de objetos.

Para resolver estas exceções, você pode empacotar as classes de objeto em cache para que o servidor eXtreme Scale possa carregar as classes em ambientes independentes. Portanto, você deve colocar as classes no caminho de classe.

Se seu ambiente incluir a estrutura OSGi, empacote as classes em um fragmento do pacote configurável `objectgrid.jar`. Se estiver executando servidores do eXtreme Scale no Perfil do Liberty, empacote as classes como um pacote configurável OSGi e exporte os pacotes Java para essas classes. Em seguida, instale o pacote configurável copiando-o no diretório `grids`.

No WebSphere Application Server, empacote as classes no aplicativo ou em uma biblioteca compartilhada que o aplicativo pode acessar.

Como alternativa, é possível usar serializadores customizados que podem comparar as matrizes de bytes que são armazenadas no eXtreme Scale para detectar quaisquer mudanças.

O modo de cópia padrão para um mapa pode ser configurado no objeto BackingMap. Também é possível alterar o modo de cópia antes de iniciar uma transação usando o método ObjectMap.setCopyMode.

A seguir há um exemplo de um fragmento de mapa de apoio de um arquivo `objectgrid.xml` que mostra como configurar o modo de cópia para um determinado mapa de apoio. Este exemplo assume que você esteja utilizando `cc` como o espaço de nomes `objectgrid/config`.

```
<cc:backingMap name="RuntimeLifespan" copyMode="NO_COPY"/>
```

Referências relacionadas:

Arquivo XML descritor do ObjectGrid
Para configurar o WebSphere eXtreme Scale, utilize um arquivo XML descritor do ObjectGrid e a API do ObjectGrid.

Gerenciador de Bloqueio: Java

Quando configurar uma estratégia de bloqueio, um gerenciador de bloqueio é criado para o mapa de apoio para manter a consistência da entrada de cache.

Configuração do Gerenciador de Bloqueios

Quando a estratégia de bloqueio pessimista ou otimista for utilizada, será criado um gerenciador de bloqueios para o BackingMap. O gerenciador de bloqueios

utiliza um mapa hash para controlar entradas bloqueadas por uma ou mais transações. Se existirem muitas entradas de mapa no mapa hash, mais depósitos de bloqueio podem resultar em melhor desempenho. O risco de colisões de sincronização Java é inferior conforme a quantidade de depósitos aumenta. Mais depósitos de bloqueios também resultam em maior simultaneidade. Os exemplos anteriores mostram como um aplicativo pode configurar o número de depósitos de bloqueio para utilizar para uma determinada instância de BackingMap.

Para evitar uma exceção java.lang.IllegalStateException, o método setNumberOfLockBuckets deve ser chamado antes de chamar os métodos initialize ou getSession na instância do ObjectGrid. O parâmetro do método setNumberOfLockBuckets é um inteiro primitivo Java que especifica a quantidade de depósitos de bloqueio para uso. Utilizar um número primo permite uma distribuição uniforme de entradas do mapa sobre os depósitos de bloqueios. Um bom ponto de partida para obter melhor desempenho é configurar o número de depósitos de bloqueios para aproximadamente dez por cento do número esperado de entradas do BackingMap.

Estratégias de Bloqueio: Java

As estratégias de bloqueio incluem pessimista, otimista e nenhum. Para escolher uma estratégia de bloqueio, é necessário considerar questões como a porcentagem de cada tipo de operações que você tem, se você utiliza um utilitário de carga, entre outras.

Os bloqueios são limitados pelas transações. É possível especificar as seguintes configurações de bloqueio:

- **Ausência de bloqueio**: Executar sem a configuração de bloqueio é a opção mais rápida. Se estiver utilizando dados de leitura, você talvez não precise do bloqueio.
- **Bloqueio pessimistic**: Adquire bloqueios em entrada e, em seguida, contém o bloqueio até o momento do commit. Essa estratégia de bloqueio fornece boa consistência à custa do rendimento.
- **Bloqueio optimistic**: Obtém uma imagem anterior de cada registro que a transação acessa e compara a imagem com os valores de entrada atuais quando ocorre o commit da transação. Se os valores de entrada forem alterados, a transação será recuperada. Nenhum bloqueio será retido até o momento da confirmação. Esta estratégia de bloqueio fornece melhor simultaneidade do que a estratégia pessimista, no risco da transação sendo recuperada e no custo da memória de criar a cópia extra da entrada.

Configure a estratégia de bloqueio no BackingMap. Não é possível alterar a estratégia de bloqueio para cada transação. A seguir há um exemplo de fragmento XML que mostra como configurar o modo de bloqueio em um mapa utilizando o arquivo XML, assumindo que `cc` é o espaço de nomes para o espaço de nomes `objectgrid/config`.

```
<cc:backingMap name="RuntimeLifespan" lockStrategy="PESSIMISTIC" />
```

Bloqueio Pessimista

Use a estratégia de bloqueio pessimista para ler e gravar mapas quando outras estratégias de bloqueio não foram possíveis. Quando um mapa do ObjectGrid map é configurado para utilizar a estratégia de bloqueio pessimista, um bloqueio de transação pessimista para uma entrada de mapa é obtido quando uma transação primeiro obtém a entrada do BackingMap. O bloqueio pessimistic fica retido até

que o aplicativo conclua a transação. Geralmente, a estratégia de bloqueio pessimistic é utilizada nas seguintes situações:

- Quando o BackingMap é configurado com ou sem um utilitário de carga e as informações de controle de versões não estão disponíveis.
- Quando o BackingMap é utilizado diretamente por um aplicativo que precisa de ajuda do eXtreme Scale para controle de simultaneidade.
- Quando as informações de controle de versões estão disponíveis, mas as transações de atualização colidem frequentemente nas entradas de suporte, resultando em falhas de atualização otimistas.

Como a estratégia de bloqueio pessimista tem o maior impacto no desempenho e escalabilidade, esta estratégia deve ser utilizada apenas para ler e gravar mapas quando outras estratégias de bloqueio não são viáveis. Por exemplo, essas situações incluem quando ocorrem falhas de atualização otimista com frequência ou quando a recuperação da falha otimista é difícil para um aplicativo manipular.

8.6+ Ao usar o bloqueio pessimista, é possível usar o método de bloqueio para bloquear dados, ou chaves, sem retornar nenhum valor dos dados. Com o método de bloqueio, é possível bloquear a chave na grade ou bloquear a chave e determinar se o valor existe na grade. Em liberações anteriores, você usava as APIs get e getForUpdate para bloquear chaves na grade de dados. No entanto, se você não precisou de dados do cliente, o desempenho é degradado pela recuperação em potencial de objetos de valores grandes no cliente. Além disso, containsKey não contém atualmente nenhum bloqueio, portanto, você foi forçado a usar get e getForUpdate para obter bloqueios apropriados ao usar bloqueio pessimista. A API de bloqueio agora fornece a você uma semântica containsKey enquanto mantém o bloqueio. Verifique os seguintes exemplos:

- `boolean ObjectMap.lock(Object key, LockMode lockMode);`

  Bloqueia a chave no mapa, retornando true se a chave existir e retornando false se a chave não existir.
- `List<Boolean> ObjectMap.lockAll(List keys, LockMode lockMode);`

  Bloqueia uma lista de chaves no mapa, retornando uma lista de valores true ou false; retornando `true` se a chave existir e retornando `false` se a chave não existir.

LockMode é uma enumeração com possíveis valores SHARED, UPGRADABLE e EXCLUSIVE, nos quais é possível especificar as chaves que você deseja bloquear. Consulte a tabela a seguir para entender o relacionamento entre estes valores de modo de bloqueio e o comportamento de métodos existentes:

Tabela 14. Valores de LockMode e Equivalentes do Método Existente

Modo de bloqueio	Equivalente do Método
SHARED	get()
UPGRADABLE	getForUpdate()
EXCLUSIVE	getNextKey() e commit()

Consulte o código de exemplo a seguir do parâmetro LockMode:

```
session.begin();
map.lock(key, LockMode.UPGRADABLE);
map.upsert();
session.commit()
```

Bloqueio Otimista

A estratégia de bloqueio otimista assume que nenhuma transação em execução simultânea pode tentar atualizar a mesma entrada de mapa. Devido a esta convicção, o modo de bloqueio não precisa ser retido pelo ciclo de vida da transação porque é improvável que mais de uma transação possa atualizar a entrada de mapa simultaneamente. A estratégia de bloqueio optimistic geralmente é utilizada nas seguintes situações:

- Quando um BackingMap é configurado com ou sem um utilitário de carga e as informações de controle de versões estão disponíveis.
- Quando um BackingMap possui em sua maior parte, transações que executam operações de leitura. As operações insert, update ou remove nas entradas de mapa não ocorrem com frequência no BackingMap.
- Quando um BackingMap é inserido, atualizado ou removido mais frequentemente do que é lido, mas as transações raramente colidem na mesma entrada do mapa.

Como a estratégia de bloqueio pessimistic, o métodos na interface ObjectMap determinam como o eXtreme Scale automaticamente tenta adquirir um modo de bloqueio para a entrada de mapa que está sendo acessada. Entretanto, existem as seguintes diferenças entre as estratégias pessimistic e optimistic:

- Como a estratégia de bloqueio pessimistic, um modo de bloqueio S é adquirido pelos métodos get e getAll quando o método é chamado. No entanto, com o bloqueio optimistic, o modo de bloqueio S não fica retido até que a transação seja concluída. Em vez disso, o modo de bloqueio S é liberado antes de o método retornar ao aplicativo. O propósito de adquirir o modo de bloqueio é para que o eXtreme Scale possa garantir que apenas dados com commit de outras transações fiquem visíveis para a transação atual. Após o eXtreme Scale ter verificado que ocorreu commit nos dados, o modo de bloqueio S é liberado. No momento do commit, uma verificação de versão optimistic é executada para garantir que nenhuma outra transação tenha alterado a entrada do mapa após a transação atual ter liberado seu modo de bloqueio S. Se uma entrada não for procurada a partir do mapa antes de ser atualizada, invalidada ou excluída, o tempo de execução do eXtreme Scale implicitamente procura a entrada a partir do mapa. Esta operação get implícita é desempenhada para obter o valor atual no momento em que foi solicitada a modificação da entrada.
- Diferente da estratégia de bloqueio pessimista, os métodos getForUpdate e getAllForUpdate são tratados exatamente como os métodos get e getAll quando a estratégia de bloqueio otimista é utilizada. Ou seja, um modo de bloqueio S é adquirido no início do método e o modo de bloqueio S é liberado antes de retornar para o aplicativo.

Todos os outros métodos ObjectMap são tratados exatamente como são tratados para a estratégia de bloqueio pessimistic. Ou seja, quando o método commit é chamado, um modo de bloqueio X é obtido para qualquer entrada do mapa que tenha sido inserida, atualizada, removida, tocada ou invalidada e o modo de bloqueio X é retido até que a transação tenha concluído o processamento de consolidação.

A estratégia de bloqueio optimistic assume que nenhuma transação em execução simultânea tenta atualizar a mesma entrada de mapa. Devido a esta suposição, o modo de bloqueio não precisa ser mantido pela duração da transação porque é improvável que mais de uma transação possa atualizar a entrada de mapa simultaneamente. Entretanto, como um modo de bloqueio não foi mantido, outra

transação simultânea poderia potencialmente atualizar a entrada do mapa após a transação atual ter liberado seu modo de bloqueio S.

Para tratar esta possibilidade, o eXtreme Scale obtém um bloqueio X no momento do commit e executa uma verificação de versão optimistic para verificar se nenhuma outra transação alterou a entrada do mapa após a transação atual ter lido a entrada do mapa a partir do BackingMap. Se outra transação alterar a entrada do mapa, a verificação de versão falhará e ocorrerá uma exceção OptimisticCollisionException. Esta exceção força a transação atual a ser retrocedida e o aplicativo deve tentar novamente a transação inteira. A estratégia de bloqueio optimistic é muito útil quando um mapa é lido em sua maior parte e é improvável que ocorram atualizações na mesma entrada do mapa.

Restrição: 8.6+

Ao usar o bloqueio otimista com COPY_TO_BYTES, você pode experienciar exceções ClassNotFoundException durante operações comuns, tal como invalidar entradas de cache. Estas exceções ocorrem porque o mecanismo de bloqueio otimista deve chamar o método "equals(...)" do objeto de cache para detectar quaisquer mudanças antes de a transação ser confirmada. Para chamar o método equals(...), o servidor eXtreme Scale deve poder desserializar o objeto em cache, o que significa que eXtreme Scale deve carregar a classe de objetos.

Para resolver estas exceções, você pode empacotar as classes de objeto em cache para que o servidor eXtreme Scale possa carregar as classes em ambientes independentes. Portanto, você deve colocar as classes no caminho de classe.

Se seu ambiente incluir a estrutura OSGi, empacote as classes em um fragmento do pacote configurável `objectgrid.jar`. Se estiver executando servidores do eXtreme Scale no Perfil do Liberty, empacote as classes como um pacote configurável OSGi e exporte os pacotes Java para essas classes. Em seguida, instale o pacote configurável copiando-o no diretório `grids`.

No WebSphere Application Server, empacote as classes no aplicativo ou em uma biblioteca compartilhada que o aplicativo pode acessar.

Como alternativa, é possível usar serializadores customizados que podem comparar as matrizes de bytes que são armazenadas no eXtreme Scale para detectar quaisquer mudanças.

Ausência de Bloqueio

Quando um BackingMap é configurado para usar nenhuma estratégia de bloqueio, nenhum bloqueio de transação para uma entrada de mapa é obtido.

Nota: 8.6+ BackingMaps configurados para usar uma estratégia sem bloqueio não podem participar de uma transação com múltiplas partições.

Não utilizar uma estratégia de bloqueio é útil quando um aplicativo é um gerenciador de persistência, como um contêiner Enterprise JavaBeans (EJB) ou quando um aplicativo utiliza Hibernate para obter dados persistentes. Neste cenário, o BackingMap é configurado sem um utilitário de carga e o gerenciador de persistência utiliza o BackingMap como um cache de dados. Neste cenário, o gerenciador de persistência fornece controle de simultaneidade entre transações que estão acessando as mesmas entradas de Mapa.

O WebSphere eXtreme Scale não precisa obter nenhum bloqueio de transação para o propósito de controle de simultaneidade. Essa situação presume que o gerenciador de persistência não libera os bloqueios da transação antes de atualizar o mapa ObjectGrid com as alterações confirmadas. Se o gerenciador de persistência libera seus bloqueios, então uma estratégia de bloqueio pessimistic ou optimistic deve ser utilizada. Por exemplo, suponha que o gerenciador de persistência de um contêiner EJB esteja atualizando o mapa do ObjectGrid com dados que foram confirmados na transação gerenciada por contêiner de EJB. Se a atualização do mapa do ObjectGrid ocorrer antes dos bloqueios de transação do gerenciador de persistência serem liberados, então é possível não utilizar nenhuma estratégia de bloqueio. Se o mapa do ObjectGrid ocorrer após os bloqueios de transação do gerenciador de persistência serem liberados, será necessário utilizar a estratégia de bloqueio otimista ou pessimista.

Outro cenário onde a ausência de estratégia de bloqueio pode ser utilizada é quando o aplicativo utiliza um BackingMap diretamente e um Utilitário de Carga é configurado para o mapa. Neste cenário, o utilitário de carga utiliza o suporte de controle de simultaneidade que é fornecido por um Relational Database Management System (RDBMS) utilizando Java Database Connectivity (JDBC) ou Hibernate para acessar dados em um banco de dados relacional. A implementação do utilitário de carga pode utilizar uma abordagem optimistic ou pessimistic. Um utilitário de carga que utiliza um bloqueio optimistic ou uma abordagem de controle de versões ajuda a obter a maior quantidade de simultaneidade e desempenho. Para obter mais informações sobre como implementar uma abordagem de bloqueio otimista, consulte a seção OptimisticCallback em “Configurando Carregadores de Banco de Dados” na página 604. Se estiver usando um utilitário de carga que usa suporte de bloqueio pessimistic de um backend subjacente, é possível querer usar o parâmetro forUpdate que é transmitido no método get da interface do utilitário de carga. Configure este parâmetro como true se o método getForUpdate da interface ObjectMap foi utilizado pelo aplicativo para obter os dados. O utilitário de carga pode utilizar esse parâmetro para determinar se solicitará um bloqueio atualizável na linha que está sendo lida. Por exemplo, o DB2 obtém um bloqueio atualizável quando uma instrução select SQL contém uma cláusula `FOR UPDATE`. Esta abordagem oferece a mesma prevenção de conflito que está descrita em “Bloqueio Pessimista” na página 473.

Para obter mais informações, consulte o “Bloqueios” na página 493 ou o “Gerenciador de Bloqueio” na página 472.

Tarefas relacionadas:

Java "Resolução de Problemas de Exceções de Tempo Limite do Bloqueio para uma Transação Multipartição" na página 890
O cenário que é descrito é um exemplo de uma transação multipartição que está causando uma exceção de tempo limite de bloqueio. Dependendo do estado da transação, as soluções ilustram como você pode resolver esse problema manualmente.

Java "Resolvendo Exceções de Tempo Limite do Bloqueio" na página 892
Usando o comando **xscmd -c listindoubt**, é possível visualizar o estado de uma transação e determinar um curso de ação.

Java "Desenvolvendo Aplicativos para Gravar Transações de Múltiplas Partições para o WebSphere eXtreme Scale em um Ambiente Independente" na página 487
É possível gravar um aplicativo para uma grade de dados distribuídos com várias partições em seu ambiente independente do WebSphere eXtreme Scale.

Distribuindo Transações: Java

Use Java Message Service (JMS) para mudanças de transação distribuída entre diferentes camadas ou em ambientes em plataformas mistas.

O JMS é um protocolo ideal para alterações distribuídas entre diferentes camadas ou em ambientes em plataformas mistas. Por exemplo, alguns aplicativos que usam o eXtreme Scale podem ser implementados noIBM WebSphere Application Server Community Edition, Apache Geronimo ou Apache Tomcat, considerando que outros aplicativos podem executar no WebSphere Application Server Versão 6.x. O JMS é ideal para alterações distribuídas entre peers do eXtreme Scale nesses diferentes ambientes. O transporte de mensagens do gerenciador de alta disponibilidade é muito rápido, mas pode apenas distribuir alterações para as Java Virtual Machines que estão em um grupo principal único. O JMS é mais lento, mas permite que conjuntos maiores e mais diversos de aplicativos clientes compartilhem um ObjectGrid. O JMS é ideal no compartilhamento de dados em um ObjectGrid entre um cliente Swing rápido e um aplicativo implementado no WebSphere Extended Deployment.

O Mecanismo de Invalidação do Cliente e a Replicação Ponto a Ponto incorporados são exemplos da distribuição de alterações transacionais com base no JMS. Consulte o Configurando a Sincronização do Cliente Baseada no Serviço de Mensagens Java (JMS) e o Configurando Replicação Ponto a Ponto com o JMS para obter mais informações.

Implementando o JMS

O JMS é implementado para distribuir alterações de transação usando um objeto Java que se comporta como um ObjectGridEventListener. Este objeto pode propagar o estado nas quatro maneiras a seguir:

1. Invalidar: Qualquer entrada que é despejada, atualizada ou excluída é removida em todas as Java Virtual Machines peer quando elas recebem a mensagem.
2. Invalidar condicional: A entrada é despejada somente se a versão local for a mesma ou mais antiga que a versão no publicador.
3. Push: Qualquer entrada que foi despejada, atualizada, excluída ou inserida é incluída ou sobrescrita em todas as Java Virtual Machines peer quando elas recebem a mensagem JMS.

4. Push condicional: A entrada é atualizada ou incluída no lado de recebimento apenas se a entrada local for menos recente que a versão que está sendo publicada.

Atender Alterações de Publicação

O plug-in implementa a interface ObjectGridEventListener para interceptar o evento transactionEnd. Quando o eXtreme Scale chama este método, o plug-in tenta converter a lista LogSequence list para cada mapa que é acessado pela transação em uma mensagem JMS e, então, a publica. O plug-in pode ser configurado para publicar alterações para todos os mapas ou um subconjunto de mapas. Os objetos LogSequence são processados para os mapas com a publicação ativada. A classe LogSequenceTransformer do ObjectGrid serializa um LogSequence filtrado para cada mapa em um fluxo. Após todas as LogSequences serem serializadas para o fluxo, então, um ObjectMessage JMS é criado e publicado em um tópico bem conhecido.

Atender Mensagens JMS e Aplicá-las ao ObjectGrid Local

O mesmo plug-in também inicia um encadeamento que gira em um loop, recebendo todas as mensagens publicadas no tópico bem conhecido. Quando chega uma mensagem, ele transmite o conteúdo da mensagem para a classe LogSequenceTransformer para convertê-lo em um conjunto de objetos LogSequence. Em seguida, uma transação não-write-through é iniciada. Cada objeto LogSequence é fornecido ao método Session.processLogSequence, que atualiza os Mapas locais com as alterações. O método processLogSequence entende o modo de distribuição. A transação é confirmada e o cache local agora reflete as alterações. Para obter mais informações sobre como usar o JMS para distribuir as mudanças transacionais, consulte o Distribuindo Mudanças entre JVMs Peers.

Transações de Partição Única e entre Grade de Dados: Java

A maior diferença entre as soluções do WebSphere eXtreme Scale e de armazenamento de dados tradicional, como bancos de dados relacionais ou bancos de dados em memória, é o uso do particionamento, que permite que o cache seja escalado de maneira linear. Os tipos de transações importantes a serem considerados são transações de partição única e de cada partição (grade de dados cruzada).

Em geral, as interações com o cache podem ser categorizadas como transações de partição única ou transações de grade de dados cruzada, conforme abordado na seguinte seção.

Transações de Partição Única

As transações de partição única são o método preferido para interagir com os caches que são hospedados pelo WebSphere eXtreme Scale. Quando uma transação é limitada a uma única partição, por padrão, ela é limitada a uma única Java Virtual Machine e, portanto, a um único computador de servidor. Um servidor pode executar *M* número dessas transações por segundo e, se você tiver *N* computadores, poderá executar `M*N` transações por segundo. Se os negócios aumentarem e você precisar executar o dobro dessas transações por segundo, poderá dobrar *N* ao adquirir mais computadores. Em seguida, é possível atender as demandas de capacidade sem alterar o aplicativo, fazer upgrade de hardware ou até mesmo usar o aplicativo off-line.

Além de permitir que o cache seja escalado de maneira significativa, as transações de partição única também maximizam a disponibilidade do cache. Cada transação depende apenas de um computador. Qualquer um dos outros (N-1) computadores podem falhar sem afetar o sucesso ou o tempo de resposta da transação. Assim, se você estiver executando 100 computadores e um deles falhar, apenas 1% das transações em andamento no momento em que esse servidor falhou é recuperado. Depois que o servidor falhar, o WebSphere eXtreme Scale relocará as partições que são hospedadas pelo servidor com falha nos outros 99 computadores. Durante esse breve período, antes de concluir a operação, os outros 99 computadores ainda poderão concluir as transações. Apenas as transações que envolveriam as partições que estão sendo relocadas são bloqueadas. Depois que o processo de failover ser concluído, o cache poderá continuar executando, totalmente operacional, a 99% de sua capacidade de rendimento original. Depois que o servidor com falha for substituído e retornado para a grade de dados, o cache voltará para 100% da capacidade de rendimento.

Transações da Grade de Dados Cruzada

Em termos de desempenho, disponibilidade e escalabilidade, as transações de grade de dados cruzada são o oposto de transações de partição única. As transações de grade de dados cruzada acessam cada partição e, portanto, cada computador na configuração. Cada computador na grade de dados é instruído a procurar alguns dados e retornar o resultado. A transação não pode ser concluída até que cada computador tenha respondido e, dessa forma, o rendimento da grade de dados inteira ficará limitado em função do computador mais lento. Incluir computadores não agiliza o computador mais lento e, assim, não melhora o rendimento do cache.

As transações de grade de dados cruzada possuem um efeito semelhante em termos de disponibilidade. Estendendo o exemplo anterior, se você estiver executando 100 servidores e um deles falhar, então, 100% das transações que estão em andamento no momento em que esse servidor falhou será recuperado. Depois que o servidor falhar, o WebSphere eXtreme Scale relocará as partições que são hospedadas por esse servidor nos outros 99 computadores. Durante esse tempo, antes de o processo de failover ser concluído, a grade de dados não pode processar nenhuma dessas transações. Depois que o processo de failover ser concluído, o cache poderá continuar executando, porém com capacidade reduzida. Se cada computador na grade de dados atender 10 partições, então 10 dos 99 computadores restantes receberão, pelo menos, uma partição extra como parte do processo de failover. Incluir uma partição extra aumenta a carga de trabalho desse computador em pelo menos 10%. Como o rendimento da grade de dados é limitado ao rendimento do computador mais lento em uma transação de grade de dados cruzada, em média, o rendimento é reduzido em 10%.

As transações de partição única são preferidas para as transações de grade de dados cruzada para efetuar scale out com um cache de objeto distribuído e altamente disponível, como o WebSphere eXtreme Scale. Aumentar o desempenho desses tipos de sistemas requer o uso de técnicas que são diferentes das metodologias relacionais tradicionais, porém é possível transformar as transações de grade de dados cruzada em transações de partição única escalável.

Boas práticas para criar modelos de dados escaláveis

As boas práticas para construir aplicativos escaláveis com produtos como o WebSphere eXtreme Scale incluem duas categorias: princípios básicos e dicas de implementação. Os princípios básicos são ideias principais que precisam ser

capturadas no projeto dos próprios dados. Um aplicativo que não observa esses princípios podem não ser escalados tão bem, mesmo para as transações de linha principal. Por outro lado, as dicas de implementação são aplicadas em transações problemáticas em um aplicativo bem projetado que observa os princípios gerais para modelos de dados escaláveis.

Princípios Básicos

Algumas das maneiras importantes de otimizar a escalabilidade são conceitos ou princípios básicos que devem ser mantidos em mente.

Duplicar em vez de normalizar

O que mais deve-se ter em mente sobre os produtos como o WebSphere eXtreme Scale é que eles são designados para propagar dados entre um grande número de computadores. Se o objetivo é concluir a maioria ou todas as transações em uma única partição, o design do modelo de dados precisa garantir que todos os dados que a transação possa precisar estejam localizados na partição. Na maioria das vezes, a única maneira de fazer isso é duplicar os dados.

Por exemplo, considere um aplicativo, como um quadro de avisos. Duas transações muito importantes para um quadro de mensagens mostram todas as postagens de um determinado usuário e todas as postagens de um determinado tópico. Primeiro considere como essas transações trabalhariam com um modelo de dados normalizado que contenha um registro de usuário, um registro de tópico e um registro de postagem que contenha o texto real. Se as postagens forem particionadas com os registros do usuário, a exibição do tópico torna-se uma transação de grade cruzada e vice-versa. Os tópicos e os usuários não podem ser particionados juntos porque eles possuem um relacionamento muitos-para-muitos.

A melhor maneira de fazer com que esse quadro de avisos seja escalável é duplicar as postagens, armazenar uma cópia com o registro de tópico e uma cópia com o registro do usuário. Em seguida, a exibição das postagens de um usuário é uma transação de partição única, exibir as postagens em um tópico é uma transação de partição única e atualizar ou excluir uma postagem é uma transação de duas partições. Todas essas três transações serão escaladas de maneira linear já que o número de computadores na grade de dados aumenta.

Escalabilidade Em Vez de Recursos

O maior obstáculo a ser superado ao considerar os modelos de dados não-normalizados é o impacto que esse modelos causam nos recursos. Manter duas, três ou mais cópias de alguns dados pode parecer que muitos recursos usados são práticos. Ao se deparar com esse cenário, lembre-se dos seguintes fatos: os recursos de hardware se tornam mais baratos a cada dia. Segundo e o mais importante, o WebSphere eXtreme Scale elimina a maioria dos custos implícitos associados à implementação de mais recursos.

Os recursos devem ser medidos em termos de custo em vez de computador, como megabytes e processadores. Os armazenamentos de dados que trabalham com dados relacionais normalizados geralmente precisam estar localizados no mesmo computador. Essa colocação necessária significa que um único computador corporativo maior precisa ser adquirido em vez de vários computadores menores. Com o hardware corporativo, um computador que executa um milhão de transações por

segundo normalmente é bem mais barato que 10 computadores capazes de executar 100 mil transações por segundo cada um.

Incluir recursos também gera custos de negócios. Um negócio em crescimento normalmente pode ficar sem capacidade. Quando não houver capacidade, é necessário encerrar para mudar para um computador maior e mais rápido ou é necessário criar um segundo ambiente de produção para o qual você possa mudar. De uma das formas, custos adicionais serão acarretados na forma de negócios perdidos ou ao manter quase o dobro da capacidade necessária durante o período de transação.

Com o WebSphere eXtreme Scale, o aplicativo não precisa ser encerrado para incluir capacidade. Se seus projetos de negócios requererem 10% de capacidade a mais para o próximo ano, aumente 10% o número de computadores na grade de dados. É possível aumentar essa porcentagem sem ocorrer tempo de inatividade do aplicativo e sem adquirir capacidade em excesso.

Evitar transformações de dados

Quando estiver usando o WebSphere eXtreme Scale, os dados deverão ser armazenados em um formato que possa ser consumado diretamente pela lógica de negócios. Dividir os dados em um formato mais primitivo gera custos. A transformação precisa ser feita quando os dados forem gravados e lidos. Com os bancos de dados relacionais, essa transformação é feita sem necessidade porque os dados são definitivamente persistidos no disco muito frequentemente, mas com o WebSphere eXtreme Scale, essas transformações não precisam ser executadas. Na maioria das vezes os dados são armazenados na memória e podem, portanto, serem armazenados no formato exato em que o aplicativo precisa.

Observar essa regra de amostra ajuda a desnormalizar os dados de acordo com o primeiro princípio. O tipo mais comum de transformação dos dados de negócios é as operações JOIN que são necessárias para tornar os dados normalizados em um conjunto de resultados que se ajusta às necessidades do aplicativo. Armazenar os dados no formato correto implicitamente evita a execução dessas operações JOIN e produz um modelo de dados não-normalizado.

Eliminar consultas ilimitadas

Independente de como os seus dados são estruturados, as consultas ilimitadas não são bem escaladas. Por exemplo, não tenha uma transação que solicite uma lista de todos os itens classificados por valor. Essa transação pode funcionar inicialmente quando o número total de itens for 1.000, mas quando o número total de itens chegar a 10 milhões, a transação retornará todos os 10 milhões de itens. Se você executar essa transação, os dois resultados mais prováveis são o tempo limite da transação se esgotar ou o cliente receber um erro de falta de memória.

A melhor opção é alterar a lógica de negócios para que apenas os 10 ou 20 itens principais possam ser retornados. Essa mudança de lógica mantém o tamanho da transação gerenciável, independente de quantos itens estão no cache.

Definir esquema

A principal vantagem de normalizar os dados é que o sistema de banco de dados controla a consistência de dados em segundo plano. Quando os dados são desnormalizados para escalabilidade, esse gerenciamento de consistência de dados automático já não existe mais. É necessário

implementar um modelo de dados que funcione na camada de aplicativos ou como um plug-in para a grade de dados distribuída para garantir a consistência dos dados.

Considere o exemplo do quadro de mensagens. Se uma transação remover uma postagem de um tópico, a postagem duplicada no registro do usuário precisará ser removida. Sem um modelo de dados, um desenvolvedor pode gravar o código do aplicativo para remover a postagem do tópico e se esquecer de remover a postagem do registro do usuário. Entretanto, se o desenvolvedor estiver usando um modelo de dados em vez de interagir diretamente com o cache, o método removePost no modelo de dados poderá extrair o ID do usuário da postagem, procurar pelo registro do usuário e remover a postagem duplicada em segundo plano.

Como alternativa, é possível implementar um listener que é executado na partição real que detecta a alteração no tópico e ajusta automaticamente o registro do usuário. Um listener pode ser benéfico porque o ajuste do registro do usuário pode ocorrer localmente caso a partição possua o registro do usuário ou, mesmo se o registro do usuário estiver em uma partição diferente, a transação ocorrerá entre os servidores em vez de ocorrer entre o cliente e o servidor. A conexão de rede entre os servidores provavelmente é mais rápida do que a conexão de rede entre o cliente e o servidor.

Evitar contenção

Evite cenários, como ter um contador global. A grade de dados não será escalável se um registro único estiver sendo usado por um número de vezes desproporcional, comparado com o restante dos registros. O desempenho da grade de dados será limitado pelo desempenho do computador que mantém o registro fornecido.

Nessas situações, tente dividir o registro para que ele seja gerenciado por partição. Por exemplo, considere uma transação que retorna o número total de entradas no cache distribuído. Em vez de fazer com que cada operação de inserção e remoção acesse um único registro que incrementa, faça com que o listener em cada partição controle as operações de inserção e remoção. Com o controle desse listener, a inserção e a remoção poderá se transformar nas operações de partição única.

A leitura do contador se transformará em uma operação de grade de dados cruzada, mas para a maior parte, isso já era ineficiente como uma operação de grade de dados cruzada porque o desempenho dependia do desempenho do computador que hospeda o registro.

Dicas de Implementação

Também é possível considerar as seguintes dicas para obter a melhor escalabilidade.

Índices de Procura Reversa

Considere um modelo de dados não-normalizado adequadamente em que os registros são particionados com base no número do ID do cliente. Esse método de particionamento é a opção lógica porque quase cada operação de negócios executada com o registro do cliente usa o número de ID do cliente. Entretanto, uma transação importante que não usa o número do ID do cliente é a transação de login. É mais comum ter nomes de usuário ou endereços de e-mail para login em vez de números do ID de cliente.

A abordagem simples com o cenário de login é usar uma transação de grade de dados cruzada para localizar o registro do cliente. Conforme explicado anteriormente, essa abordagem não é escalada.

A próxima opção pode ser uma partição no nome do usuário ou e-mail. Essa opção não é viável porque todas as operações baseadas no ID do cliente se transformam em transações de grade de dados cruzada. Além disso, os clientes do seu site podem alterar o nome do usuário ou o endereço de e-mail. Produtos como o WebSphere eXtreme Scale precisam do valor usado para particionar os dados que permanecerem constantes.

A solução correta é usar um índice de consulta reversa. Com o WebSphere eXtreme Scale, um cache pode ser criado na mesma grade distribuída que o cache que mantém todos os registros do usuário. Esse cache é altamente escalável, particionado e escalável. Esse cache pode ser usado para mapear um nome de usuário ou endereço de e-mail para um ID de cliente. Esse cache transforma o login em uma operação de duas partições em vez de uma operação de grade cruzada. Esse cenário não é tão bom quanto uma transação de partição única, mas o rendimento ainda pode ser escalado linearmente conforme o número de computadores aumenta.

Computar no Momento da Gravação

Valores normalmente calculados, como médias ou totais, podem ser despendiosos para serem produzidos porque essas operações normalmente requerem leitura de um grande número de entradas. Como as leituras são mais comuns do que as gravações na maioria dos aplicativos, é eficiente calcular esses valores no momento da gravação e, em seguida, armazenar o resultado no cache. Essa prática torna as operações mais rápidas e mais escaláveis.

Campos Opcionais

Considere um registro de usuário que mantém um número de negócios, doméstico e de telefone. Um usuário pode ter todos, nenhum ou qualquer combinação desses números definida. Se os dados forem normalizados, uma tabela do usuário e um número de telefone existirão. Os números de telefone para um determinado usuário pode ser localizado usando uma operação JOIN entre as duas tabelas.

Desnormalizar esse registro não requer duplicação de dados, porque a maioria dos usuários não compartilha números de telefone. Em vez disso, slots vazios no registro do usuário devem ser permitidos. Em vez de ter uma tabela de número de telefone, inclua três atributos em cada registro do usuário, um para cada tipo de número de telefone. Essa inclusão de atributos elimina a operação JOIN e torna uma procura por número de telefone de um usuário uma operação de partição única.

Colocação de relacionamentos muitos-para-muitos

Considere um aplicativo que controla os produtos e as lojas nas quais os produtos são vendidos. Um único produto é vendido em muitas lojas e uma única loja vende muitos produtos. Suponha que esse aplicativo controla 50 grandes varejistas. Cada produto é vendido em um máximo de 50 lojas, com cada uma vendendo milhares de produtos.

Mantenha uma lista de lojas dentro da entidade do produto (organização A), em vez de manter uma lista de produtos dentro de cada entidade de loja (organização B). Observar algumas das transações que esse aplicativo teria que executar mostra o porquê a organização A é mais escalável.

Primeiro observe as atualizações. Com a organização A, remover um produto do inventário de uma loja bloqueia a entidade do produto. Se a grade de dados mantiver 10.000 produtos, apenas 1/10.000 da grade de dados precisará ser bloqueada para executar a atualização. Com a organização B, a grade de dados contém apenas 50 lojas, de modo que 1/50 da grade deverá ser bloqueada para concluir a atualização. Portanto, embora os dois possam ser considerados operações de partição única, a organização A é escalada mais eficientemente.

Agora, considerando as leituras na organização A, observar as lojas nas quais um produto é vendido é uma transação de partição única que é escalada e é rápido porque a transação transmite apenas uma pequena quantia de dados. Com a organização B, essa transação se torna uma transação de grade de dados cruzada porque cada entidade de loja deve ser acessada para ver se o produto é vendido nessa loja, que revela uma enorme vantagem de desempenho para a organização A.

Escalando com Dados Normalizados

Um uso legítimo de transações de grade de dados cruzada é escalar o processamento de dados. Se uma grade de dados tiver 5 computadores e uma transação de grade de dados cruzada for despachada, que classifica cerca de 100.000 registros em cada computador, essa transação classificará entre 500.000 registros. Se o computador mais lento na grade de dados puder executar 10 dessas transações por segundo, a grade de dados poderá classificar cerca de 5.000.000 de registros por segundo. Se os dados da grade dobrarem, cada computador deverá classificar cerca de 200.000 registros e cada transação classificará cerca de 1.000.000 de registros. Esse aumento de dados diminui o rendimento do computador mais lento para 5 transações por segundo, reduzindo, assim, o rendimento da grade de dados para 5 transações por segundo. Além disso, a grade de dados classifica entre 5.000.000 de registros por segundo.

Neste cenário, dobrar o número de computadores permite que cada computador volte para o carregamento anterior de classificação de 100.000 registros, permitindo que o computador mais lento processe 10 dessas transações por segundo. O rendimento da grade de dados permanece o mesmo nas 10 solicitações por segundo, mas agora cada transação processa 1.000.000 de registros dobrando, assim, a capacidade da grade em processar 10.000.000 de registros por segundo.

Aplicativos, como um mecanismo de procura, que precisam ser escalados tanto em termos de processamento de dados para acomodar o tamanho crescente da Internet e de rendimento para acomodar o crescimento de usuários, requer a criação de diversas grades de dados, com um round robin das solicitações entre as grades. Se você precisar efetuar scale up do rendimento, inclua computadores e outra grade de dados para solicitações de serviço. Se for necessário efetuar scale up do processamento de dados, inclua mais computadores e mantenha o número de grades de dados constante.

Desenvolvendo Aplicativos que Atualizam Várias Partições em uma Única Transação: Java 8.6+

Se os dados forem distribuídos entre várias partições na grade de dados, você poderá ler e atualizar várias partições em uma única transação. Esse tipo de transação é chamado de transação com múltiplas partições e utiliza o protocolo two-phase commit para coordenar e recuperar a transação em caso de falha.

Two-phase Commit e Recuperação de Erro: Java

O protocolo two-phase commit coordena todas as partições que participam de uma transação distribuída para confirmar ou recuperar a transação.

Em uma grade de dados distribuídos, as partições são distribuídas através de várias Java virtual machines. Estas JVMs podem estar em mais de um sistema. Uma transação que grava em múltiplas partições pode envolver decisões transacionais que afetam mais de um sistema. Quando a transação é confirmada utilizando um protocolo two-phase commit, esse processamento de confirmação assegura que a transação inteira seja persistida, ou nenhuma transação seja persistida. O processo two-phase commit assegura este resultado apesar das falhas de partição, sistema ou de comunicação. Se ocorrer uma falha na segunda fase, o cliente do WebSphere eXtreme Scale tentará resolver a falha automaticamente, a menos que o erro atenda a determinados critérios nos quais você pode intervir manualmente.

Uma transação que é ativada para gravar em várias partições utiliza o protocolo two-phase commit. Um protocolo two-phase commit assegura que o processo de confirmação seja consistente em todas as partições e sistemas. O WebSphere eXtreme Scale age como o coordenador que controla o processo two-phase commit. As partições envolvidas na transação são chamadas de participantes ou gerenciadores de recursos (RM). Durante a segunda fase do protocolo de confirmação, o coordenador delega uma das partições para agir como o gerenciador de transações (TM). O TM é responsável por rastrear a decisão de cada transação e recuperar a transação se uma falha ocorrer.

Primeira fase:
Quando um aplicativo confirma uma transação, o cliente do WebSphere eXtreme Scale inicia a primeira fase enviando a solicitação para preparar para confirmação para cada partição identificada como um RM. Cada partição aplica as mudanças na transação nos mapas de apoio e mantém todos os bloqueios para assegurar a integridade dos dados. O RM notifica o cliente do WebSphere eXtreme Scale. Após todas as partições identificadas como RM responderem com sucesso, o cliente do WebSphere eXtreme Scale começa a segunda fase do protocolo de confirmação.

Segunda fase:
Se pelo menos uma partição falhar durante a primeira fase, o coordenador recuperará todas as partições durante a segunda fase. Se todas as partições de RM responderem com êxito, o cliente do WebSphere eXtreme Scale delegará uma das partições para atuar como a partição de TM. Como o coordenador, o WebSphere eXtreme Scale começa a segunda fase do protocolo de confirmação, enviando uma solicitação de confirmação ou de retrocesso para todas as partições que estão envolvidas na transação. Cada partição que é identificada como um RM aplica ou recupera as alterações no mapa de apoio e libera todos os bloqueios. O RM, então, notifica o cliente WebSphere eXtreme Scale. Se pelo menos uma partição falhou durante a segunda fase, a partição de TM delegada recuperará automaticamente a transação. A recuperação automática garante que todas as partições envolvidas na transação sejam consistentes.

Fase em dúvida:
A fase em dúvida é o período entre quando a partição de RM processa com sucesso a primeira fase e está esperando para iniciar a segunda fase. Durante o período em dúvida, a partição de RM não sabe se deve confirmar ou recuperar a transação. A partição de RM mantém os

bloqueios. A manutenção dos bloqueios pode resultar em outras transações experienciando um aumento na contenção de bloqueio.

Recuperação de Erro Durante uma Two-phase Commit

No caso de uma falha durante a primeira fase, o cliente do WebSphere eXtreme Scale recupera a transação. Se uma das partições falhar ao confirmar a transação, o TM assegura que a transação seja confirmada tentando periodicamente confirmar a transação. Você verá mensagens de log, como a seguinte:

```
00000099 TransactionLog I  CWOBJ8705I: Resolução automática da transação
WXS-40000139-DF01-216D-E002-
1CB456931719 em RM:TestGrid:TestSet2:20 ainda está esperando por uma decisão. Uma outra tentativa
```

Você deve permitir que o cliente do WebSphere eXtreme Scale resolva a transação. Você deve tentar intervir manualmente apenas se a transação não for recuperada dentro de 1 minuto ou o aplicativo estiver experimentando um alto volume de contenção de bloqueio, pois ele é uma transação pendente. Para obter mais informações sobre como recuperar manualmente uma transação, consulte "Resolução de Problemas de Exceções de Tempo Limite do Bloqueio para uma Transação Multipartição" na página 890.

Tarefas relacionadas:

Java "Resolvendo Exceções de Tempo Limite do Bloqueio" na página 892
Usando o comando **xscmd -c listindoubt**, é possível visualizar o estado de uma transação e determinar um curso de ação.

Java "Resolução de Problemas de Exceções de Tempo Limite do Bloqueio para uma Transação Multipartição" na página 890
O cenário que é descrito é um exemplo de uma transação multipartição que está causando uma exceção de tempo limite de bloqueio. Dependendo do estado da transação, as soluções ilustram como você pode resolver esse problema manualmente.

Desenvolvendo Aplicativos para Gravar Transações de Múltiplas Partições para o WebSphere eXtreme Scale em um Ambiente Independente: Java

É possível gravar um aplicativo para uma grade de dados distribuídos com várias partições em seu ambiente independente do WebSphere eXtreme Scale.

Antes de Iniciar

- Ative o protocolo eXtremeIO. Para obter informações adicionais, consulte "Configurando o IBM eXtremeIO (XIO)" na página 119.
- Não é possível utilizar a replicação multi-master com transações que gravam em várias partições.
- Não é possível utilizar várias partições em um WebSphere eXtreme Scale Client em um ambiente .NET.
- BackingMaps que são configurados com um plug-in Loader podem ler mas não podem gravar no mapa em uma transação de partição múltipla.
- BackingMaps que estiverem utilizando como estratégia de bloqueio NONE não poderão participar de transações com várias partições.

Sobre Esta Tarefa

Utilize a API de Sessão TxCommitProtocol configurada para ativar o suporte a transações multipartição para o WebSphere eXtreme Scale em um ambiente independente. A nova API fornece as duas opções a seguir:

- TxCommitProtocol.ONEPHASE: Uma constante do protocolo de confirmação de transação que indica que a transação deve ser confirmada com o one-phase commit padrão. Com essa opção, uma transação pode ler várias partições, mas pode gravar em uma partição única. Uma exceção TransactionException ocorre se a transação grava em várias partições.
- TxCommitProtocol.TWOPHASE: Uma constante do protocolo de confirmação da transação que indica que a transação deve ser confirmada com o one-phase commit ou two-phase commit. Se a transação gravar em uma única partição, o protocolo one-phase commit será usado. Caso contrário, o protocolo de duas fases será usado para confirmar a transação, envolvendo operações de gravação para várias partições.

Também é possível configurar o suporte de diversas transações para o WebSphere eXtreme Scale no WebSphere Application Server. Para obter informações adicionais, consulte "Desenvolvendo Componentes do Cliente eXtreme Scale para Usar Transações" na página 199.

Procedimento

1. Obtenha uma instância de sessão da grade de dados com o método ObjectGrid.getSession. Para obter informações adicionais, consulte "Uso de Sessões para Acessar Dados na Grade" na página 364.
2. Conecte-se à grade de dados. Para obter informações adicionais, consulte "Conectando-se às Instâncias do ObjectGrid Distribuído Programaticamente" na página 345.
3. Ative um protocolo two-phase commit, configurando o fragmento de código a seguir: `session.setTxCommitProtocol(Session.TxCommitProtocol.TWOPHASE); session.begin();` O fragmento de código a seguir ilustra como operações de criação, recuperação, atualização e exclusão em uma grade com o protocolo two-phase commit:

```
Session session = og.getSession();
Objectmap map1 = session.getMap("Map1");
Objectmap map2 = session.getMap("Map2");
Objectmap map3 = session.getMap("Map3");
session.setTxCommitProtocol(Session.TxCommitProtocol.TWOPHASE);
session.begin();
map1.insert("randKey345", "HelloMap1");
map2.insert("randKey58901", "HelloMap2");
map3.insert("randKey58", "HelloMap3");
session.commit();
```

O que Fazer Depois

É possível ativar o rastreio em transações de múltiplas partições. Para obter informações adicionais, consulte "Opções de Rastreio do Servidor" na página 860.

Conceitos relacionados:

Java "Estratégias de Bloqueio" na página 473
As estratégias de bloqueio incluem pessimista, otimista e nenhum. Para escolher uma estratégia de bloqueio, é necessário considerar questões como a porcentagem de cada tipo de operações que você tem, se você utiliza um utilitário de carga, entre outras.

Java "Acesso a Dados e Transações" na página 465
Após um aplicativo fazer uma referência a uma instância ObjectGrid ou uma conexão do cliente com uma grade de dados remota, é possível acessar e interagir com os dados em sua grade de dados. Com a API do ObjectGridManager, é possível criar uma instância local ou estabelecer uma conexão do cliente com uma instância distribuída. Para criar uma instância local, use um dos métodos createObjectGrid. Para estabelecer uma conexão do cliente com uma grade de dados remota, use o método getObjectGrid.

Desenvolvendo Componentes do Cliente eXtreme Scale para Usar Transações: Java

O adaptador de recursos WebSphere eXtreme Scale fornece suporte à transação local e gerenciamento de conexão do cliente. Com esse suporte, os aplicativos Java Platform, Enterprise Edition (Java EE) podem consultar as conexões do cliente eXtreme Scale e demarcar as transações locais com transações Java EE ou APIs eXtreme Scale.

Antes de Iniciar

Crie uma referência de recurso do connection factory do eXtreme Scale.

Sobre Esta Tarefa

Há várias opções para trabalhar com as APIs de acesso a dados do eXtreme Scale. Em todos os casos, o connection factory eXtreme Scale deve ser injetado no componente de aplicativo ou consultado no Java Naming Directory Interface (JNDI). Depois que o connection factory for consultado, você poderá demarcar as transações e criar conexões para acessar as APIs do eXtreme Scale.

Opcionalmente, você pode executar cast da instância javax.resource.cci.ConnectionFactory para um com.ibm.websphere.xs.ra.XSConnectionFactory que forneça opções adicionais para recuperar as manipulações de conexões. As manipulações de conexão resultante devem ser lançadas na interface com.ibm.websphere.xs.ra.XSConnection, que fornece o método getSession. O método getSession retorna uma manipulação de objeto com.ibm.websphere.objectgrid.Session que permite que os aplicativos usem algumas das APIs de acesso a dados eXtreme Scale, como a API ObjectMap e a API EntityManager.

A manipulação de Sessão e quaisquer objetos derivados são válidos pela duração da manipulação XSConnection.

Os procedimentos a seguir podem ser usados para demarcar as transações do eXtreme Scale. Não é possível combinar cada um dos procedimentos. Por exemplo, não é possível combinar demarcação de transação global e demarcação de transação local no mesmo contexto do componente de aplicativo.

Procedimento

- Use confirmação automática, transações locais. Use as etapas a seguir para confirmar automaticamente as operações de acesso a dados ou operações que não suportam uma transação ativa:
  1. Recupere uma conexão com.ibm.websphere.xs.ra.XSConnection fora do contexto de uma transação global.
  2. Recupere e use a sessão com.ibm.websphere.objectgrid.Session para interagir com a grade de dados.
  3. Chame qualquer operação de acesso a dados que suporte as transação de confirmação automática.
  4. Feche a conexão.
- Use uma sessão ObjectGrid para demarcar uma transação local. Use as etapas a seguir para demarcar uma transação ObjectGrid usando o objeto de Sessão:
  1. Recupere uma conexão com.ibm.websphere.xs.ra.XSConnection.
  2. Recupere a sessão com.ibm.websphere.objectgrid.Session.
  3. Use o método Session.begin() para iniciar a transação.
  4. Use a sessão para interagir com a grade de dados.
  5. Use os métodos Session.commit() ou rollback() para terminar a transação.
  6. Feche a conexão.
- Use uma transação javax.resource.cci.LocalTransction para demarcar uma transação local. Use as etapas a seguir para demarcar uma transação ObjectGrid usando a interface javax.resource.cci.LocalTransaction:
  1. Recupere uma conexão com.ibm.websphere.xs.ra.XSConnection.
  2. Recupere a transação javax.resource.cci.LocalTransaction usando o método XSConnection.getLocalTransaction().
  3. Use o método LocalTransaction.begin() para iniciar a transação.
  4. Recupere e use a sessão com.ibm.websphere.objectgrid.Session para interagir com a grade de dados.
  5. Use os métodos LocalTransaction.commit() ou rollback() para terminar a transação.
  6. Feche a conexão.
- Relacione a conexão em uma transação global. Esse procedimento também se aplica a transações gerenciadas por contêiner:
  1. Inicie a transação global por meio da interface javax.transaction.UserTransaction ou com uma transação gerenciada por contêiner.
  2. Recupere uma conexão com.ibm.websphere.xs.ra.XSConnection.
  3. Recupere e use a sessão com.ibm.websphere.objectgrid.Session.
  4. Feche a conexão.
  5. Confirme ou retroceda a transação global.
- **8.6+** Configure uma conexão para compor diversas partições em uma transação. Use as etapas a seguir para demarcar uma transação ObjectGrid usando o objeto de Sessão:
  1. Crie um novo objeto com.ibm.websphere.xs.ra.XSConnectionSpec.
  2. Chame o método XSConnectionSpec e o método setMultiPartitionSupportEnabled com um argumento igual a `true`.
  3. Recupere a conexão com.ibm.websphere.xs.ra.XSConnection para transmitir a XSConnectionSpec ao método ConnectionFactory.getConnection.

4. Recupere e use a sessão com.ibm.websphere.objectgrid.Session.

Exemplo

Consulte o exemplo de código a seguir, que demonstra as etapas anteriores para demarcar as transações eXtreme Scale.

```
// (C) Copyright IBM Corp. 2001, 2012.
// All Rights Reserved. Licensed Materials - Property of IBM.
package com.ibm.ws.xs.ra.test.ee;

import javax.naming.InitialContext;
import javax.resource.cci.Connection;
import javax.resource.cci.ConnectionFactory;
import javax.resource.cci.LocalTransaction;
import javax.transaction.Status;
import javax.transaction.UserTransaction;

import junit.framework.TestCase;

import com.ibm.websphere.objectgrid.ObjectMap;
import com.ibm.websphere.objectgrid.Session;
import com.ibm.websphere.xs.ra.XSConnection;

/**
* This sample requires that it runs in a J2EE context in your
* application server. For example, using the JUnitEE framework servlet.
*
* The code in these test methods would typically reside in your own servlet,
* EJB, or other web component.
*
* The sample depends on a configured WebSphere eXtreme Scale connection
* factory registered at of JNDI Name of "eis/embedded/wxscf" that defines
* a connection to a grid containing a Map with the name "Map1".
*
* The sample does a direct lookup of the JNDI name and does not require
* resource injection.
*/
public class DocSampleTests extends TestCase {
    public final static String CF_JNDI_NAME = "eis/embedded/wxscf";
    public final static String MAP_NAME = "Map1";

    Long                key = null;
    Long                value = null;
    InitialContext      ctx = null;
    ConnectionFactory cf = null;

    public DocSampleTests() {
    }
    public DocSampleTests(String name) {
        super(name);
    }
    protected void setUp() throws Exception {
        ctx = new InitialContext();
        cf = (ConnectionFactory)ctx.lookup(CF_JNDI_NAME);
        key = System.nanoTime();
        value = System.nanoTime();
    }
    /**
     * This example runs when not in the context of a global transaction
     * and uses autocommit.
     */
    public void testLocalAutocommit() throws Exception {
        Connection conn = cf.getConnection();
        try {
            Session    session = ((XSConnection)conn).getSession();
            ObjectMap  map = session.getMap(MAP_NAME);
            map.insert(key, value); // Or various data access operations
        }
        finally {
            conn.close();
        }
    }

    /**
     * This example runs when not in the context of a global transaction
     * and demarcates the transaction using session.begin()/session.commit()
```

```
 */
public void testLocalSessionTransaction() throws Exception {
    Session session = null;
    Connection conn = cf.getConnection();
    try {
        session = ((XSConnection)conn).getSession();
        session.begin();
        ObjectMap  map = session.getMap(MAP_NAME);
        map.insert(key, value); // Or various data access operations
        session.commit();
    }
    finally {
        if (session != null && session.isTransactionActive()) {
            try { session.rollback(); }
            catch (Exception e) { e.printStackTrace(); }
        }
        conn.close();
    }
}

/**
 * This example uses the LocalTransaction interface to demarcate
 * transações.
 */
public void testLocalTranTransaction() throws Exception {
    LocalTransaction tx = null;
    Connection conn = cf.getConnection();
    try {
        tx = conn.getLocalTransaction();
        tx.begin();
        Session    session = ((XSConnection)conn).getSession();
        ObjectMap  map = session.getMap(MAP_NAME);
        map.insert(key, value); // Or various data access operations
        tx.commit(); tx = null;
    }
    finally {
        if (tx != null) {
            try { tx.rollback(); }
            catch (Exception e) { e.printStackTrace(); }
        }
        conn.close();
    }
}

/**
 * This example depends on an externally managed transaction,
 * the externally managed transaction might typically be present in
 * an EJB with its transaction attributes set to REQUIRED or REQUIRES_NEW.
 * NOTE: If there is NO global transaction active, this example runs in auto-commit
 *       mode because it doesn't verify a transaction exists.
 */
public void testGlobalTransactionContainerManaged() throws Exception {
    Connection      conn = cf.getConnection();
    try {
        Session    session = ((XSConnection)conn).getSession();
        ObjectMap  map = session.getMap(MAP_NAME);
        map.insert(key, value); // Or various data access operations
    }
    catch (Throwable t) {
        t.printStackTrace();
        UserTransaction tx = (UserTransaction)ctx.lookup("java:comp/UserTransaction");
        if (tx.getStatus() != Status.STATUS_NO_TRANSACTION) {
            tx.setRollbackOnly();
        }
    }
    finally {
        conn.close();
    }
}

/**
 * This example demonstrates starting a new global transaction using the
 * UserTransaction interface. Typically the container starts the global
 * transaction (for example in an EJB with a transaction attribute of
 * REQUIRES_NEW), but this sample will also start the global transaction
 * using the UserTransaction API if it is not currently active.
 */
public void testGlobalTransactionTestManaged() throws Exception {
    boolean         started = false;
```

```
            UserTransaction tx = (UserTransaction)ctx.lookup("java:comp/UserTransaction");
            if (tx.getStatus() == Status.STATUS_NO_TRANSACTION) {
                tx.begin();
                started = true;
            }
            // else { called with an externally/container managed transaction }
            Connection conn  = null;
            try {
                conn = cf.getConnection(); // Get connection after the global tran starts
                Session    session = ((XSConnection)conn).getSession();
                ObjectMap  map = session.getMap(MAP_NAME);
                map.insert(key, value); // Or various data access operations
                if (started) {
                    tx.commit(); started = false; tx = null;
                }
            }
            finally {
                if (started) {
                    try { tx.rollback(); }
                    catch (Exception e) { e.printStackTrace(); }
                }
                if (conn != null) { conn.close(); }
            }
        }
/**
        /**
        * This example demonstrates a multi-partition transaction.
        */

   public void testGlobalTransactionTestManagedMultiPartition() throws Exception {
     boolean         started = false;
     XSConnectionSpec connSpec = new XSConnectionSpec();
     connSpec.setWriteToMultiplePartitions(true);
     UserTransaction tx = (UserTransaction)ctx.lookup("java:comp/UserTransaction");
     if (tx.getStatus() == Status.STATUS_NO_TRANSACTION) {
       tx.begin();
     started = true;
    }
   // else { called with an externally/container managed transaction }
     Connection conn  = null;
        try {
     conn = cf.getConnection(connSpec); // Get connection after the global tran starts
     Session    session = ((XSConnection)conn).getSession();
     ObjectMap  map = session.getMap(MAP_NAME);
     map.insert(key, value); // Or various data access operations
     if (started) {
       tx.commit(); started = false; tx = null;
       }
     }
     finally {
      if (started) {
        try { tx.rollback(); }
        catch (Exception e) { e.printStackTrace(); }
       }
      if (conn != null) { conn.close(); }
     }
    }
```

Informações relacionadas:

- Benefícios de Referência de Recurso
- Desenvolvendo Componentes para Usar Transações

Usando Bloqueio: Java

Bloqueios têm ciclos de vida e os tipos diferentes de bloqueios são compatíveis com outros de várias maneiras. Os bloqueios devem ser manipulados na ordem correta para evitar cenários de conflito.

Bloqueios: Java

Bloqueios têm ciclos de vida e os tipos diferentes de bloqueios são compatíveis com outros de várias maneiras. Os bloqueios devem ser manipulados na ordem correta para evitar cenários de conflito.

Bloqueios Compartilhados, Passíveis de Upgrade e Exclusivos

Quando um aplicativo chama qualquer método da interface ObjectMap, usa os métodos de localização em um índice ou faz uma consulta, o eXtreme Scale tenta automaticamente adquirir um bloqueio para a entrada de mapa que está sendo acessada.

8.6+ Ao usar o bloqueio pessimista, é possível usar o método de bloqueio para bloquear dados, ou chaves, sem retornar nenhum valor dos dados. Com o método de bloqueio, é possível bloquear a chave na grade ou bloquear a chave e determinar se o valor existe na grade. Em liberações anteriores, você usava as APIs get e getForUpdate para bloquear chaves na grade de dados. No entanto, se você não precisou de dados do cliente, o desempenho é degradado pela recuperação em potencial de objetos de valores grandes no cliente. Além disso, containsKey não contém atualmente nenhum bloqueio, portanto, você foi forçado a usar get e getForUpdate para obter bloqueios apropriados ao usar bloqueio pessimista. A API de bloqueio agora fornece a você uma semântica containsKey enquanto mantém o bloqueio. Verifique os seguintes exemplos:

- `boolean ObjectMap.lock(Object key, LockMode lockMode);`

  Bloqueia a chave no mapa, retornando true se a chave existir e retornando false se a chave não existir.
- `List<Boolean> ObjectMap.lockAll(List keys, LockMode lockMode);`

  Bloqueia uma lista de chaves no mapa, retornando uma lista de valores true ou false; retornando `true` se a chave existir e retornando `false` se a chave não existir.

LockMode é uma enumeração com possíveis valores SHARED, UPGRADABLE e EXCLUSIVE, nos quais é possível especificar as chaves que você deseja bloquear. Consulte a tabela a seguir para entender o relacionamento entre estes valores do modo de bloqueio e o comportamento de métodos existentes:

Tabela 15. Valores de LockMode e Equivalentes do Método Existente

Modo de bloqueio	Equivalente do Método
SHARED	get()
UPGRADABLE	getForUpdate()
EXCLUSIVE	getNextKey() e commit()

Consulte o código de exemplo a seguir do parâmetro LockMode:

```
session.begin();
map.lock(key, LockMode.UPGRADABLE);
map.upsert();
session.commit()
```

O WebSphereeXtreme Scale utiliza os seguintes modos de bloqueio com base no método em que o aplicativo chama na interface ObjectMap.

- Os métodos get e getAll na interface ObjectMap, os métodos de índice e as consultas adquirem um *bloqueio S* ou um modo de bloqueio compartilhado para a chave em uma entrada de mapa. A duração em que o bloqueio S é mantido depende do nível de isolamento da transação usado. Um modo de bloqueio S permite a simultaneidade entre transações que tentam adquirir um modo de

bloqueio S ou de bloqueio para upgrade (bloqueio U) para a mesma chave, mas bloqueia outras transações que tentam obter um modo de bloqueio exclusivo (bloqueio X) para a mesma chave.

- Os métodos getForUpdate e getAllForUpdate adquirem um *bloqueio U* ou um modo de bloqueio para upgrade para a chave de uma entrada do mapa. O bloqueio U fica retido até que a transação seja concluída. Um modo de bloqueio U permite a simultaneidade entre transações que adquirem um modo de bloqueio S para a mesma chave, mas bloqueia outras transações que tentam adquirir um modo de bloqueio U ou de bloqueio X para a mesma chave.
- Os métodos put, putAll, remove, removeAll, insert, update e touch adquirem um *bloqueio X* ou um modo de bloqueio exclusivo para a chave de uma entrada de mapa. O bloqueio X fica retido até que a transação seja concluída. Um modo de bloqueio X assegura que apenas uma transação esteja inserindo, atualizando ou removendo uma entrada do mapa de um valor de chave especificado. Um bloqueio X bloqueia todas as demais transações que tentam adquirir um modo de bloqueio S, U ou X para a mesma chave.

  Nota: 8.6+ Os métodos upsert e upsertAll substituem os métodos put e putAll do ObjectMap. Use o método upsert para informar ao BackingMap e carregador que uma entrada na grade de dados precisa colocar a chave e o valor na grade. O BackingMap e carregador executam uma inserção ou uma atualização para colocar o valor na grade e no carregador. Se você executar a API upsert dentro de seus aplicativos, o carregador obterá um tipo UPSERT de LogElement, que permite que carregadores façam a mesclagem do banco de dados ou chamadas upsert em vez de usar insert ou update.
- Os métodos global invalidate e global invalidateAll adquirem um bloqueio X para cada entrada do mapa que é invalidada. O bloqueio X fica retido até que a transação seja concluída. Não são adquiridos bloqueios para os métodos local invalidate e local invalidateAll, porque nenhuma das entradas de BackingMap é invalidada por chamadas de métodos locais invalidate.

Das definições anteriores, é óbvio que um modo de bloqueio S é mais fraco que um modo de bloqueio U, porque permite que mais transações sejam executadas simultaneamente durante o acesso à mesma entrada do mapa. O modo de bloqueio U é um pouco mais forte do que o modo de bloqueio S, porque bloqueia outras transações que estão solicitando um modo de bloqueio U ou X. O modo de bloqueio S bloqueia apenas outras transações que estão solicitando um modo de bloqueio X. Esta pequena diferença é importante na prevenção de alguns conflitos. O modo de bloqueio X é o modo de bloqueio mais forte, porque bloqueia todas as demais transações que estão tentando obter um modo de bloqueio S, U ou X para a mesma entrada do mapa. O efeito de rede de um modo de bloqueio X é para garantir que apenas uma transação possa inserir, atualizar ou remover uma entrada de mapa e para evitar que atualizações sejam perdidas quando mais de uma transação esteja tentando atualizar a mesma entrada de mapa.

A tabela a seguir é uma matriz de compatibilidade de modo de bloqueio que resume os modos de bloqueio descritos, que você pode utilizar para determinar quais modos de bloqueio são compatíveis com outros. Para ler esta matriz, a linha na matriz indica um modo de bloqueio já concedido. A coluna indica o modo de bloqueio solicitado por outra transação. Se Yes for exibido na coluna, então, o modo de bloqueio solicitado por outra transação é concedido porque é compatível com o modo de bloqueio que já foi concedido. No, indica que o modo de bloqueio não é compatível e a outra transação deve esperar a primeira transação liberar o bloqueio que ela possui.

Tabela 16. Matriz de Compatibilidade do Modo de Bloqueio

Bloqueio	Tipo de bloqueio S (compartilhado)	Tipo de bloqueio U (para upgrade)	Tipo de bloqueio X (exclusivo)	Força
S (compartilhado)	Sim	Sim	Não	mais fraco
U (para upgrade)	Sim	Não	Não	normal
X (exclusivo)	Não	Não	Não	mais forte

Conflitos de Bloqueio

Considere a seguinte sequência de pedidos de modo de bloqueio:

1. O bloqueio X é concedido à transação 1 para key1.
2. O bloqueio X é concedido à transação 2 para key2.
3. O bloqueio X é solicitado pela transação 1 para key2. (Transaction 1 blocks waiting for lock owned by transaction 2.)
4. O bloqueio X é solicitado pela transação 2 para key1. (Transaction 2 blocks waiting for lock owned by transaction 1.)

A sequência anterior é o exemplo clássico de conflito de duas transações que tentam adquirir mais de um bloqueio único e cada transação adquire os bloqueios em uma ordem diferente. Para evitar este conflito, cada transação deve obter vários bloqueios na mesma ordem. Se a estratégia de bloqueio OPTIMISTIC for utilizada e o método flush na interface ObjectMap nunca for utilizado pelo aplicativo, os modos de bloqueio serão solicitados pela transação apenas durante o ciclo de confirmação. Durante o ciclo de commit, o eXtreme Scale determina as chaves para as entradas de mapa que precisam ser bloqueadas e solicita os modos de bloqueio na sequência de chaves (comportamento determinístico). Com este método, o eXtreme Scale evita a grande maioria dos conflitos clássicos. Entretanto, o eXtreme Scale não evita e não pode evitar todos os cenários de conflito possíveis. Existem poucos cenários que o aplicativo precisa considerar. A seguir estão os cenários que o aplicativo deve considerar e executar uma ação preventiva contra.

Existe um cenário em que eXtreme Scale está apto a detectar um conflito sem precisar aguardar que um tempo limite de espera de bloqueio ocorra. Se este cenário ocorrer, isto resultará em uma exceção com.ibm.websphere.objectgrid.LockDeadlockException. Considere o seguinte exemplo de código:

```
Session sess = ...;
ObjectMap person = sess.getMap("PERSON");
sess.begin();
Person p = (IPerson)person.get("Lynn");
// Lynn had a birthday; so make her 1 year older.
p.setAge( p.getAge() + 1 );
person.put( "Lynn", p );
sess.commit();
```

8.6+ No mesmo cenário, é possível usar o método upsert no exemplo de código:

```
Session sess = ...;
ObjectMap person = sess.getMap("PERSON");
sess.begin();
Person p = (IPerson)person.get("Lynn");
// Lynn had a birthday; so make her 1 year older.
p.setAge( p.getAge() + 1 );
person.upsert( "Lynn", p );
sess.commit();
```

Nessa situação, o namorado de Lynn quer que ela seja mais velha do que sua idade atual e tanto Lynn quanto seu namorado executam essa transação simultaneamente. Nesta situação, as duas transações possuem um modo de bloqueio S na entrada Lynn do mapa PERSON como resultado da chamada de método person.get("Lynn"). Como resultado da chamada de método person.put ("Lynn", p), as duas transações tentam fazer upgrade do modo de bloqueio S para um modo de bloqueio X. As duas transações bloqueiam a espera para que a outra transação libere o modo de bloqueio S que ela possui. Como resultado, ocorre um conflito porque existe uma condição de espera circular entre as duas transações. É gerada uma condição de espera circular quando mais de uma transação tenta promover um bloqueio de um modo mais fraco para um mais forte para a mesma entrada do mapa. Neste cenário, o resultado é uma exceção LockDeadlockException ao invés de uma exceção LockTimeoutException.

O aplicativo pode evitar a exceção LockDeadlockException para o exemplo anterior utilizando a estratégia de bloqueio optimistic ao invés da estratégia de bloqueio pessimistic. Utilizar a estratégia de bloqueio optimistic é a solução preferida quando o mapa é em maior parte lido e as atualizações no mapa são infrequentes. Se a estratégia de bloqueio pessimistic deve ser utilizada, o método getForUpdate pode ser utilizado ao invés do método get no exemplo acima ou pode ser utilizado um nível de isolamento de transação de TRANSACTION_READ_COMMITTED.

Consulte o “Estratégias de Bloqueio” na página 473 para obter mais detalhes.

Utilizar o nível de isolamento da transação TRANSACTION_READ_COMMITTED evita o bloqueio S adquirido pelo método get seja mantido até a transação ser concluída. Como a chave nunca é invalidada no cache transacional, as leituras repetitíveis ainda são garantidas. Consulte “Gerenciador de Bloqueio” na página 472 para obter informações adicionais.

Uma alternativa para alterar o nível de isolamento de transação é utilizar o método getForUpdate. A primeira transação para chamar o método getForUpdate adquire um modo de bloqueio U ao invés de um bloqueio S. Este modo de bloqueio faz com que a segunda transação seja bloqueada quando ela chama o método getForUpdate, porque apenas uma transação recebe um modo de bloqueio U. Como a segunda transação é bloqueada, ela não possui nenhum modo de bloqueio na entrada do mapa de Lynn. A primeira transação não é bloqueada quando tenta atualizar o modo de bloqueio U para um modo de bloqueio X como um resultado da chamada de método put a partir da primeira transação. Este recurso demonstra porque o modo de bloqueio U é chamado no modo de bloqueio *atualizável*. Quando a primeira transação é concluída, a segunda transação é desbloqueada e recebe o modo de bloqueio U. Um aplicativo pode evitar o cenário de conflito de promoção de bloqueio utilizando o método getForUpdate ao invés do método get quando a estratégia de bloqueio pessimistic está sendo utilizada.

Importante: Esta solução não evita que transações somente leitura sejam capazes de ler uma entrada de mapa. As transações de leitura chamam o método get, mas nunca chamam os métodos put, insert, update ou remove. A simultaneidade é alta apenas quando o método get regular é utilizado. A única redução na simultaneidade ocorre quando o método getForUpdate é chamado por mais de uma transação para a mesma entrada do mapa.

Você deve estar ciente de que uma transação chama o método getForUpdate em mais de uma entrada de mapa para garantir que os bloqueios U sejam adquiridos na mesma ordem para cada transação. Por exemplo, suponha que a primeira transação chame o método getForUpdate para a chave 1 e o método getForUpdate

para a chave 2. Outra transação simultânea chama o método getForUpdate para as mesmas chaves, mas em ordem inversa. Esta sequência causa o conflito clássico, porque vários bloqueios são obtidos em diferentes ordens por diferentes transações. O aplicativo ainda precisará assegurar que cada transação acesse várias entradas do mapa na sequência de chaves para assegurar que não ocorrerá o conflito. Como o bloqueio U é obtido no momento em que o método getForUpdate é chamado ao invés de no momento do commit, o eXtreme Scale não pode ordenar os pedidos de bloqueio como ele faz durante o ciclo do commit. O aplicativo deve controlar a ordem de bloqueios neste caso.

A utilização do método flush na interface ObjectMap antes de uma confirmação pode introduzir considerações adicionais sobre ordem de bloqueios. O método flush geralmente é utilizado para forçar alterações no mapa fora do backend por meio do plug-in do Loader. Nesta situação, o backend utiliza seu próprio gerenciador de bloqueios para controlar a simultaneidade, assim, a condição de espera do bloqueio e o conflito podem ocorrer no backend ao invés de no gerenciador de bloqueios do eXtreme Scale. Considere a seguinte transação:

```
Session sess = ...;
ObjectMap person = sess.getMap("PERSON");
boolean activeTran = false;
try
{
    sess.begin();
    activeTran = true;
    Person p = (IPerson)person.get("Lynn");
    p.setAge( p.getAge() + 1 );
    person.put( "Lynn", p );
    person.flush();
    ...
    p = (IPerson)person.get("Tom");
    p.setAge( p.getAge() + 1 );
    sess.commit();
    activeTran = false;
}
finally
{
    if ( activeTran ) sess.rollback();
}
```

Suponha que outra transação também tenha atualizado a pessoa Tom person, chamado o método flush e, em seguida, atualizado a pessoa Lynn. Se esta situação tiver ocorrido, a seguinte intercalação das duas transações resultará em uma condição de conflito do banco de dados:

```
X lock is granted to transaction 1 for "Lynn" when flush is executed.
X lock is granted to transaction 2 for "Tom" when flush is executed..
X lock requested by transaction 1 for "Tom" during commit processing.
(Transaction 1 blocks waiting for lock owned by transaction 2.)
X lock requested by transaction 2 for "Lynn" during commit processing.
(Transaction 2 blocks waiting for lock owned by transaction 1.)
```

Este exemplo demonstra que o uso do método flush pode causar um conflito no banco de dados ao invés de no eXtreme Scale. Este exemplo de conflito pode ocorrer, independentemente da estratégia de bloqueio utilizada. O aplicativo deve ter atenção para evitar que ocorra este tipo de conflito ao utilizar o método flush e quando um Utilitário de Carga for conectado ao BackingMap. O exemplo anterior também ilustra outro motivo pelo qual o eXtreme Scale tem um mecanismo de tempo limite de espera de bloqueio. Uma transação que está aguardando um bloqueio de banco de dados poderia estar aguardando enquanto possuía um bloqueio de entrada de mapa do eXtreme Scale. Consequentemente, problemas no nível do banco de dados podem causar tempos de espera excessivos para um

modo de bloqueio do eXtreme Scale e resultam em uma exceção LockTimeoutException.

Tarefas relacionadas:

"Resolvendo Problemas de Conflitos" na página 885
As seções a seguir descrevem alguns dos cenários de conflitos mais comuns e sugestões sobre como evitá-los.

Implementando Manipulação de Exceção em Cenários de Bloqueio: Java

Para evitar que bloqueios sejam mantidos por quantidades excessivas de tempo quando ocorre uma exceção LockTimeoutException ou LockDeadlockException, um aplicativo deve garantir que obtenha exceções inesperadas e chama o método rollback quando ocorre algo inesperado.

Procedimento

1. Capture a exceção e exiba a mensagem resultante.

   ```
   try {
   ...
   } catch (ObjectGridException oe) {
   System.out.println(oe);
   }
   ```

   A seguinte exceção é exibida como resultado:

   ```
   com.ibm.websphere.objectgrid.plugins.LockDeadlockException: Message
   ```

   Essa mensagem representa a cadeia que é transmitida como um parâmetro quando a exceção é criada e emitida.

2. Retroceda a transação após uma exceção:

   ```
   Session sess = ...;
   ObjectMap person = sess.getMap("PERSON");
   boolean activeTran = false;
   try
   {
       sess.begin();
       activeTran = true;
       Person p = (IPerson)person.get("Lynn");
       // Lynn had a birthday, so we make her 1 year older.
       p.setAge( p.getAge() + 1 );
       person.put( "Lynn", p );
       sess.commit();
       activeTran = false;
   }
   finally
   {
       if ( activeTran ) sess.rollback();
   }
   ```

   O bloco de `finally` no fragmento de código assegura que uma transação é retrocedida quando ocorrer uma exceção inesperada. Ele não apenas manipula uma exceção LockDeadlockException, mas qualquer outra exceção inesperada que possa ocorrer. O bloco finally manipula o caso em que ocorre uma exceção durante uma chamada de método commit. Este exemplo não é a única maneira de lidar com exceções inesperadas e pode haver casos em que um aplicativo deseja capturar algumas das exceções inesperadas que podem ocorrer e exibir uma de suas exceções do aplicativo. É possível incluir blocos de captura conforme apropriado, mas o aplicativo deve assegurar que o trecho de código não seja encerrado sem concluir a transação.

Configurando uma Estratégia de Bloqueio: Java

É possível definir uma estratégia otimista, pessimista ou de nenhum bloqueio em cada BackingMap na configuração do WebSphere eXtreme Scale.

Sobre Esta Tarefa

Cada instância do BackingMap pode ser configurada para usar uma das seguintes estratégias de bloqueio:

1. Modo de Bloqueio Otimista
2. Modo de Bloqueio Pessimista
3. Nenhum

A estratégia de bloqueio padrão é OPTIMISTIC. Utilize o bloqueio optimistic quando os dados são alterados de maneira infrequente. Os bloqueios são mantidos apenas por uma curta duração enquanto os dados estão sendo lidos do cache e copiados para a transação. Quando o cache da transação é sincronizado com o cache principal, quaisquer objetos de cache que foram atualizados são verificados junto à versão original. Se a verificação falhar, então, ocorre o rollback da transação e o resultado é uma exceção
OptimisticCollisionException.

A estratégia de bloqueio PESSIMISTIC adquire bloqueios para entradas de cache e deve ser utilizada quando os dados são alterados frequentemente. Sempre que uma entrada de cache é lida, um bloqueio é adquirido e mantido condicionalmente até que a transação seja concluída. A duração de alguns bloqueios pode ser ajustada utilizando níveis de isolamento de transação para a sessão.

Se o bloqueio não for necessário porque os dados nunca são atualizados ou são atualizados apenas durante períodos tranquilos, você pode desativar o bloqueio utilizando a estratégia de bloqueio NONE. Esta estratégia é muito rápida porque um gerenciador de bloqueio não é necessário. A estratégia de bloqueio NONE é ideal para tabelas de consulta ou mapas somente leitura.

Para obter mais informações sobre as estratégicas de bloqueio, consulte "Estratégias de Bloqueio" na página 473.

Procedimento

- **Configure uma estratégia de bloqueio otimista**
  - Usando o método setLockStrategy programaticamente:

```
import com.ibm.websphere.objectgrid.BackingMap;
import com.ibm.websphere.objectgrid.LockStrategy;
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
...
ObjectGrid og =
 ObjectGridManagerFactory.getObjectGridManager().createObjectGrid("test");
BackingMap bm = og.defineMap("optimisticMap");
bm.setLockStrategy( LockStrategy.OPTIMISTIC );
```

  - Usando o atributo lockStrategy no Arquivo XML descritor do ObjectGrid:

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
    xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="test">
```

```
            <backingMap name="optimisticMap"
                lockStrategy="OPTIMISTIC"/>
        </objectGrid>
    </objectGrids>
</objectGridConfig>
```

- **Configure uma estratégia de bloqueio pessimista**
  - Usando o método setLockStrategy programaticamente:

```
especificar programaticamente
estratégia pessimista
import com.ibm.websphere.objectgrid.BackingMap;
import com.ibm.websphere.objectgrid.LockStrategy;
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
...
ObjectGrid og =
 ObjectGridManagerFactory.getObjectGridManager().createObjectGrid("test");
BackingMap bm = og.defineMap("pessimisticMap");
bm.setLockStrategy( LockStrategy.PESSIMISTIC );
```

  - Usando o atributo lockStrategy no Arquivo XML descritor do ObjectGrid:

```
Especificar estratégia pessimista usando XML
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
    xmlns="http://ibm.com/ws/objectgrid/config">

    <objectGrids>
        <objectGrid name="test">
            <backingMap name="pessimisticMap"
                lockStrategy="PESSIMISTIC"/>
        </objectGrid>
    </objectGrids>
</objectGridConfig>
```

- **Configure uma estratégia de ausência de bloqueio**
  - Usando o método setLockStrategy programaticamente:

```
import com.ibm.websphere.objectgrid.BackingMap;
import com.ibm.websphere.objectgrid.LockStrategy;
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
...
ObjectGrid og =
 ObjectGridManagerFactory.getObjectGridManager().createObjectGrid("test");
BackingMap bm = og.defineMap("noLockingMap");
bm.setLockStrategy( LockStrategy.NONE );
```

  - Usando o atributo lockStrategy no Arquivo XML descritor do ObjectGrid:

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
    xmlns="http://ibm.com/ws/objectgrid/config">

    <objectGrids>
        <objectGrid name="test">
            <backingMap name="noLockingMap"
                lockStrategy="NONE"/>
        </objectGrid>
    </objectGrids>
</objectGridConfig>
```

O que Fazer Depois

Para evitar uma exceção java.lang.IllegalStateException, é necessário chamar o método setLockStrategy antes de chamar os métodos initialize ou getSession na instância ObjectGrid.

Configurando o Valor de Tempo Limite de Bloqueio: Java

O valor de tempo limite de bloqueio é usado em uma instância BackingMap para garantir que um aplicativo não aguarde infinitamente por um modo de bloqueio a ser concedido devido a uma condição de conflito que ocorre por causa de um erro de aplicativo.

Antes de Iniciar

Para configurar o valor de tempo limite de bloqueio, a estratégia de bloqueio deve ser configurada para um OPTIMISTIC ou PESSIMISTIC. Consulte o "Configurando uma Estratégia de Bloqueio" na página 500 para obter informações adicionais.

Sobre Esta Tarefa

Quando ocorrer uma exceção LockTimeoutException, o aplicativo deve determinar se o tempo limite está ocorrendo porque o aplicativo está em execução mais lento do que o esperado ou se o tempo limite ocorreu devido a uma condição de conflito. Se tiver ocorrido uma condição de conflito real, aumentar o valor de tempo limite de espera de bloqueio não elimina a exceção. Aumentar o tempo limite implica na exceção demorar mais tempo para ocorrer. No entanto, se o aumento do valor de tempo limite de espera de bloqueio eliminar a exceção, isto indica que o problema ocorreu porque o aplicativo estava em execução de forma mais lenta que o esperado. Neste caso, o aplicativo deve determinar por que o desempenho é lento.

Para evitar a ocorrência de conflitos, o gerenciador de bloqueios possui um valor de tempo limite de 15 segundos. Se o tempo limite for excedido, ocorre uma exceção LockTimeoutException. Se o sistema estiver muito carregado, o valor de tempo limite padrão poderá fazer com que ocorram exceções LockTimeoutException quando não existir nenhum conflito. Nesta situação, é possível aumentar o valor de tempo limite de bloqueio programaticamente ou no arquivo descritor XML do ObjectGrid.

Procedimento

- Configure um valor de tempo limite de bloqueio programaticamente em uma instância do BackingMap com o método setLockTimeout.

  O exemplo a seguir ilustra como configurar o valor de tempo limite de espera de bloqueio para o mapa de apoio map1 em 60 segundos:

```
import com.ibm.websphere.objectgrid.BackingMap;
import com.ibm.websphere.objectgrid.LockStrategy;
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
...
ObjectGrid og =
 ObjectGridManagerFactory.getObjectGridManager().createObjectGrid("test");
BackingMap bm = og.defineMap( "map1" );
bm.setLockStrategy( LockStrategy.PESSIMISTIC );
bm.setLockTimeout( 60 );
```

Para evitar uma exceção java.lang.IllegalStateException, chame tanto o método setLockStrategy quanto o método setLockTimeout antes da chamada dos métodos initialize ou getSession na instância ObjectGrid. O parâmetro do método setLockTimeout é um número inteiro de primitiva Java que especifica o número de segundos que o eXtreme Scale aguarda para que um modo de bloqueio seja concedido. Se uma transação esperar mais do que o valor de tempo limite de espera de bloqueio configurado para o BackingMap, isto resultará em uma exceção com.ibm.websphere.objectgrid.LockTimeoutException.

- Configure o valor de tempo limite de bloqueio usando o atributo lockTimeout no Arquivo XML descritor do ObjectGrid.

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
    xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="test">
            <backingMap name="optimisticMap"
                lockStrategy="OPTIMISTIC"
             lockTimeout="60"/>
        </objectGrid>
    </objectGrids>
</objectGridConfig>
```

- Substitua o tempo limite de espera de bloqueio para uma única instância do ObjectMap. Use o método ObjectMap.setLockTimeout para substituir o valor de tempo limite de bloqueio por uma instância do ObjectMap específica. O valor de tempo limite do bloqueio afeta todas as transações iniciadas após o novo valor de tempo limite ser configurado. Este método pode ser útil quando colisões de bloqueio são possível ou esperadas nas transações select.

Bloqueios de Entrada de Mapa com Consultas e Índices: Java

Este tópico descreve como as APIs de consulta do eXtreme Scale e o plug-in de indexação MapRangeIndex interagem com bloqueios e algumas boas práticas para aumentar a concorrência e diminuir os conflitos ao usar a estratégia de bloqueio pessimista para mapas.

Visão Geral

A API de Consulta do ObjectGrid permite consultas SELECT sobre objetos e entidades de cache do ObjectMap. Quando uma consulta é executada, o mecanismo de consulta utiliza um MapRangeIndex quando possível para localizar chaves correspondentes na cláusula WHERE da consulta ou para vincular relacionamentos. Quando um índice não está disponível, o mecanismo de consulta varrerá cada entrada em um ou mais mapas para localizar as entradas apropriadas. O mecanismo de consulta e os plug-ins de índice adquirirão bloqueios para verificar dados consistentes, dependendo da estratégia de bloqueio, nível de isolamento de transação e estado da transação.

Bloqueio com o Plug-in HashIndex

O plug-in HashIndex do eXtreme Scale permite localizar chaves baseadas em um único atributo armazenado no valor de entrada do cache. O índice armazena o valor indexado em uma estrutura de dados separada do mapa de cache. O índice valida as chaves em relação a entradas de mapa antes de retornar para o usuário para tentar alcançar um conjunto de resultados exato. Quando a estratégia de bloqueio pessimista é utilizada e o índice é utilizado junto a uma instância local do ObjectMap (versus um ObjectMap do cliente/servidor), o índice adquirirá

bloqueios para cada entrada correspondente. Ao utilizar o bloqueio optimistic ou um ObjectMap remoto, os bloqueios são sempre liberados imediatamente.

O tipo de bloqueio que é adquirido depende do argumento forUpdate passado para o método ObjectMap.getIndex. O argumento forUpdate especifica o tipo de bloqueio que o índice deve adquirir. Se false, um bloqueio compartilhável (S) é adquirido e se true, um bloqueio atualizável (U) é adquirido.

Se o tipo de bloqueio for compartilhável, a configuração de isolamento de transação para a sessão é aplicada e afeta a duração do bloqueio. Consulte o tópico Isolamento de Transação para obter detalhes sobre como o nível de isolamento é utilizado para incluir simultaneidade nos aplicativos.

Bloqueios Compartilhados com Consultas

O mecanismo de consulta do eXtreme Scale adquire bloqueios S quando necessário para introspectar as entrada do cache para descobrir se elas satisfazem os critérios de filtro da consulta. Ao utilizar o isolamento de transação de leitura repetível com bloqueio pessimistic, os bloqueios S são retidos apenas para os elementos que estão incluídos no resultado da consulta e não são incluídos no resultado. Se utilizando um nível de isolamento de transação inferior ou o bloqueio optimistic, os bloqueios S não são retidos.

Bloqueios Compartilhados com o Cliente para Consulta do Servidor

Ao usar a consulta do eXtreme Scale a partir de um cliente, a consulta tipicamente é executada no servidor, a menos que todos os mapas ou entidades referenciadas na consulta sejam locais para o cliente (por exemplo: um mapa replicado pelo cliente ou uma entidade de resultado da consulta). Todas as consultas que são executadas em uma transação de leitura/gravação reterão bloqueios S, conforme descrito na seção anterior. Se a transação não for uma transação de leitura/gravação, então, uma sessão não será retida no servidor e os bloqueios S serão liberados.

Uma transação de leitura/gravação é roteada apenas para uma partição primária e uma sessão é mantida no servidor para a sessão do cliente. Uma transação pode ser promovida para leitura/gravação sob as seguintes condições:

1. Qualquer mapa configurado para utilizar o bloqueio pessimistic é acessado utilizando os métodos de API get e getAll do ObjectMap ou os métodos EntityManager.find.
2. Ocorreu o flush da transação, fazendo com que as atualizações sejam enviadas para o servidor.
3. Qualquer mapa configurado para utilizar o bloqueio optimistic é acessado utilizando o método ObjectMap.getForUpdate ou EntityManager.findForUpdate.

Bloqueios Atualizáveis com Consultas

Bloqueios compartilháveis são úteis quando a simultaneidade e a consistência são importantes. Isto garante que um valor de entrada não seja alterado durante a duração da transação. Nenhuma outra transação pode alterar o valor enquanto qualquer outro bloqueio S é mantido, e apenas uma outra transação possa estabelecer uma tentativa de atualizar a entrada. Consulte o tópico Modo de Bloqueio Pessimistic para obter mais detalhes sobre os modos S, U e X.

Bloqueios atualizáveis são utilizados para identificar a tentativa de atualizar uma entrada de cache ao utilizar a estratégia de bloqueio pessimistic. Isto permite a sincronização entre transações que desejam modificar uma entrada de cache. As transações ainda podem visualizar a entrada utilizando um bloqueio S, mas outras transações são impedidas de adquirir um bloqueio U ou um bloqueio X. Em muitos cenários, adquirir um bloqueio U sem primeiro adquirir um bloqueio S é necessário para evitar conflitos. Consulte o tópico Modo de Bloqueio Pessimistic para obter exemplos de conflitos comuns.

As interfaces de Consulta ObjectQuery e EntityManager fornecem o método setForUpdate para identificar o uso destinado para o resultado da consulta. Especificamente, o mecanismo de consulta adquire bloqueios U ao invés de bloqueios S para cada entrada de mapa envolvida no resultado da consulta:

```
ObjectMap orderMap = session.getMap("Order");
ObjectQuery q = session.createQuery("SELECT o FROM Order o WHERE o.orderDate=?1");
q.setParameter(1, "20080101");
q.setForUpdate(true);
session.begin();
// Run the query.  Each order has  U lock
Iterator result = q.getResultIterator();
// For each order, update the status.
while(result.hasNext()) {
    Order o = (Order) result.next();
    o.status = "shipped";
    orderMap.update(o.getId(), o);
}
// When committed, the
session.commit();
```

```
Query q = em.createQuery("SELECT o FROM Order o WHERE o.orderDate=?1");
q.setParameter(1, "20080101");
q.setForUpdate(true);
emTran.begin();
// Run the query.  Each order has  U lock
Iterator result = q.getResultIterator();
// For each order, update the status.
while(result.hasNext()) {
    Order o = (Order) result.next();
    o.status = "shipped";
}
tmTran.commit();
```

Quando o atributo **setForUpdate** está ativado, a transação é automaticamente convertida em uma transação de leitura/gravação e os bloqueios são mantidos no servidor, conforme esperado. Se a consulta não puder utilizar nenhum índice, então, o mapa deve ser varrido, o que resultará em bloqueios U temporários para entradas de mapas que não satisfazem o resultado da consulta, e bloqueios U para as entradas que estão incluídas no resultado.

Isolamento de transação: Java

Para transações, é possível configurar cada configuração de mapa de apoio com uma das três estratégias de bloqueio: pessimistic, optimistic ou none. Quando você usa os bloqueios pessimistic e optimistic, o eXtreme Scale usa bloqueios compartilhado(S), atualizável (U) e exclusivo (X) para manter a consistência. Este comportamento de bloqueio é mais perceptível quando o bloqueio pessimistic é usado, pois os bloqueios optimistic não são mantidos. É possível usar um dos três níveis de isolamento de transação para ajustar as semânticas de bloqueio que o eXtreme Scale usa para manter a consistência em cada mapa de cache: repeatable read, read committed e read uncommitted.

Visão Geral de Isolamento da Transação

O isolamento de transação define como as alterações que são feitas por uma operação se tornam visíveis a outras operações concorrentes.

O WebSphere eXtreme Scale suporta três níveis de isolamento de transação com os quais é possível ajustar adicionalmente as semânticas de bloqueio que o eXtreme Scale usa para manter a consistência em cada mapa do cache: repeatable read, read committed e read uncommitted. O nível de isolamento de transação é configurado na interface Sessão usando o método setTransactionIsolation. O isolamento de transação pode ser alterado a qualquer momento durante a duração da sessão, se uma transação não estiver atualmente em andamento.

O produto força várias semânticas de isolamento de transação ajustando a forma na qual os bloqueios compartilhados (S) são solicitados e mantidos. O isolamento de transação não tem efeito nos mapas configurado para utilizar as estratégias de bloqueio optimistic ou none ou quando bloqueios atualizáveis (U) são necessários.

Leitura Repetível com Bloqueio Pessimistic

O nível de isolamento de transação repeatable read é o padrão. Este nível de isolamento evita leituras sujas e leituras não repetitivas, mas não evita leituras fantasmas. Uma leitura suja é uma operação de leitura que ocorre nos dados que foram modificados por uma transação mas não foi consolidada. Uma leitura não repetitiva pode ocorrer quando os bloqueios de leitura não são adquiridos na execução de uma operação de leitura. Uma leitura fantasma pode ocorrer quando duas operações de leitura idênticas são executadas, mas dois conjuntos diferentes de resultados são retornados porque uma atualização ocorreu nos dados entre as operações de leitura. O produto atinge uma leitura repetitiva se mantendo em qualquer bloqueio S até que a transação que possui o bloqueio seja concluída. Como um bloqueio X não é concedido até que todos os bloqueios S sejam liberados, todas as transações contendo o bloqueio S são garantidas para visualizar o mesmo valor quando lidas novamente.

```
map = session.getMap("Order");
session.setTransactionIsolation(Session.TRANSACTION_REPEATABLE_READ);
session.begin();

// An S lock is requested and held and the value is copied into
// the transactional cache.
Order order = (Order) map.get("100");
// The entry is evicted from the transactional cache.
map.invalidate("100", false);

// The same value is requested again.  It already holds the
// lock, so the same value is retrieved and copied into the
// transactional cache.
Order order2 (Order) = map.get("100");

// All locks are released after the transaction is synchronized
// with cache map.
session.commit();
```

As leituras fantasmas são possíveis quando você usa consultas ou índices pois os bloqueios não são adquiridos para intervalos de dados, somente para as entradas de cache que correspondem ao índice ou critérios de busca. Por exemplo:

```
session1.setTransactionIsolation(Session.TRANSACTION_REPEATABLE_READ);
session1.begin();

// A query is run which selects a range of values.
```

```
ObjectQuery query = session1.createObjectQuery
    ("SELECT o FROM Order o WHERE o.itemName='Widget'");

// In this case, only one order matches the query filter.
// The order has a key of "100".
// The query engine automatically acquires an S lock for Order "100".
Iterator result = query.getResultIterator();

// A second transaction inserts an order that also matches the query.
Map orderMap = session2.getMap("Order");
orderMap.insert("101", new Order("101", "Widget"));

// When the query runs again in the current transaction, the
// new order is visible and will return both Orders "100" and "101".
result = query.getResultIterator();

// All locks are released after the transaction is synchronized
// with cache map.
session.commit();
```

Leitura com Commit com Bloqueio Pessimistic

O nível de isolamento de transação consolidado da leitura pode ser usado com o eXtreme Scale, o que evita leituras sujas, mas não evita leituras não repetitivas ou leituras fantasmas, assim o eXtreme Scale continua a usar bloqueios S para ler dados a partir do mapa de cache, mas libera imediatamente os bloqueios.

```
map1 = session1.getMap("Order");
session1.setTransactionIsolation(Session.TRANSACTION_READ_COMMITTED);
session1.begin();

// An S lock is requested but immediately released and
//the value is copied into the transactional cache.

Order order = (Order) map1.get("100");

// The entry is evicted from the transactional cache.
map1.invalidate("100", false);

// A second transaction updates the same order.
// It acquires a U lock, updates the value, and commits.
// The ObjectGrid successfully acquires the X lock during
// commit since the first transaction is using read
// committed isolation.

Map orderMap2 = session2.getMap("Order");
session2.begin();
order2 = (Order) orderMap2.getForUpdate("100");
order2.quantity=2;
orderMap2.update("100", order2);
session2.commit();

// The same value is requested again.  This time, they
// want to update the value, but it now reflects
// the new value
Order order1Copy (Order) = map1.getForUpdate("100");
```

Leitura não Consolidada com Bloqueio Pessimistic

O nível de isolamento de transação não consolidado de leitura pode ser usado com o eXtreme Scale, o que é um nível que permite leituras sujas, leituras não repetitivas e leituras fantasmas.

Exceção de Colisão Otimista: Java

É possível receber uma OptimisticCollisionException diretamente ou recebê-la com uma ObjectGridException.

O código a seguir é um exemplo de como capturar a exceção e, em seguida, exibir sua mensagem:

```
try {
...
} catch (ObjectGridException oe) {
    System.out.println(oe);
}
```

Causa da Exceção

Uma exceção OptimisticCollisionException é criada em uma situação na qual dois clientes diferentes tentam atualizar a mesma entrada do mapa relativamente ao mesmo tempo. Por exemplo, se um cliente tentar executar uma sessão e atualizar a entrada do mapa após outro cliente ler os dados antes da execução, estes dados estarão incorretos. A exceção é criada quando o outro cliente tenta cometer os dados incorretos.

Recuperando a Chave que Acionou a Exceção

Pode ser útil, durante a resolução de problemas como uma exceção, recuperar a chave correspondente à entrada que acionou a exceção. O benefício da OptimisticCollisionException é que ela contém o método getKey, que retorna o objeto que representa essa chave. A seguir está um exemplo de como recuperar e imprimir a chave ao capturar a OptimisticCollisionException:

```
try {
...
} catch (
OptimisticCollisionException oce) {
    System.out.println(oce.getKey());
}
```

ObjectGridException Causa uma OptimisticCollisionException

Uma OptimisticCollisionException pode ser a causa de exibição da ObjectGridException. Se este for o caso, será possível utilizar o seguinte código para determinar o tipo de exceção e imprimir a chave. O seguinte código utiliza o método do utilitário findRootCause, conforme descrito na seção abaixo.

```
try {
...
}
catch (ObjectGridException oe) {
    Throwable Root = findRootCause( oe );
    if (Root instanceof
OptimisticCollisionException) {

OptimisticCollisionException oce = (
OptimisticCollisionException)Root;
        System.out.println(oce.getKey());
    }
}
```

Técnica Geral de Manipulação de Exceção

Saber a causa-raiz de um objeto Throwable é útil no isolamento da origem de um problema. O exemplo a seguir demonstra como um manipulador de exceções usa um método utilitário para localizar a causa-raiz do objeto Throwable.

Exemplo:

```
static public Throwable findRootCause( Throwable t )
{
     // Inicie com o Throwable que ocorreu como a raiz.
     Throwable root = t;

     // Siga a cadeia de causas até localizar o último Throwable na cadeia.
     Throwable cause = root.getCause();
     while ( cause != null )
     {
        root = cause;
        cause = root.getCause();
     }

     // Retorne o último Throwable na cadeia como a causa raiz.
     return root;
}
```

Executando a Lógica de Negócios em Paralelo na Grade de Dados (API DataGrid): Java

A API do DataGrid fornece uma interface de programação simples para executar lógica de negócios sobre toda a, ou um subconjunto da, grade de dados em paralelo onde os dados estão localizados.

Informações relacionadas:

Java API de DataGrid

APIs do DataGrid e Particionamento: Java

Com as APIs do DataGrid, um cliente pode enviar solicitações a uma partição, a um subconjunto de partições ou a todas as partições em uma grade de dados. O cliente pode especificar uma lista de chaves, e o WebSphere eXtreme Scale determina o conjunto de partições que estão hospedando as chaves. O pedido é então enviado a todas as partições no conjunto em paralelo e o cliente aguarda pelos resultados. O cliente também pode enviar pedidos sem especificar chaves, portanto, os pedidos são enviados para todas as partições.

Os agentes que são implementados na grade de dados não funcionam no modo cliente. Esses agentes funcionam diretamente contra o shard primário. Funcionando diretamente contra o shard principal resulta em desempenho máximo, permitindo dezenas de milhares de transações ou mais por segundo porque o agente funciona com os dados em velocidades de memória completas. Trabalhar diretamente com o shard primário também significa que um agente possa ver somente dados que estejam dentro deste shard. Isso proporciona oportunidades interessantes que não podem ser feitas em um cliente.

Um cliente típico do eXtreme Scale deve poder determinar a partição da transação, pois o cliente precisa rotear a solicitação. Se um agente estiver ligado diretamente a um shard, então, nenhum roteamento é necessário. Todos os pedidos seguem contra esse shard. Como o agente está diretamente ligado a um shard, os dados em

outros mapas no shard podem ser acessados sem a preocupação com chaves de particionamento comum, e assim por diante, porque não ocorre nenhum roteamento.

Informações relacionadas:

Java API de DataGrid

Agentes do DataGrid e Mapas Baseados em Entidade: Java

Um mapa contém objetos-chave e objetos de valor. O objeto-chave é uma tupla gerada conforme o valor. Um agente normalmente é fornecido com o aplicativo especificado pelos objetos-chave.

O objeto-chave é uma tupla gerada conforme o valor. Um agente normalmente é fornecido com o aplicativo especificado pelos objetos-chave. Esse agente será os objetos-chave utilizados pelo aplicativo ou Tuplas se for um Mapa de entidade. Um aplicativo que usa Entidades não desejará lidar com Tuplas diretamente e preferirá trabalhar com os objetos Java mapeados para a Entidade.

Portanto, uma classe de Agente pode implementar a interface EntityAgentMixin. Isso força a classe a implementar mais um método, o getClassForEntity(). Isso retorna a classe de entidade para utilizar com o agente no lado do servidor. As chaves são convertidas nessa Entidade antes de chamar os métodos de processo e de redução.

Essa é uma diferença semântica de um agente não EntityAgentMixin em que esses métodos são fornecidas apenas com as chaves. Um agente implementando EntityAgentMixin recebe o objeto de Entidade que inclui as chaves e os valores em um objeto.

Nota: Se a entidade não existir no servidor, as chaves estão no formato de Tupla bruto da chave ao invés da entidade gerenciada.

Informações relacionadas:

Java API de DataGrid

Exemplo da API do DataGrid: Java

As APIs do DataGrid suportam dois padrões de programação de grade comuns: mapa de paralelo e redução de paralelo.

Mapa de Paralelos

O mapa de paralelos permite que as entradas de um conjunto de chaves sejam processadas e retorna um resultado para cada entrada processada. O aplicativo faz uma lista de chaves e recebe um Mapa de pares chave/resultado depois de chamar uma operação do Mapa. O resultado provém da aplicação de uma função à entrada de cada chave. A função é fornecida pelo aplicativo.

Fluxo de chamada do MapGridAgent

Quando o método AgentManager.callMapAgent é chamado com uma coleção de chaves, a instância MapGridAgent é serializada e enviada para cada partição primária que as chaves resolvem. Isto significa que quaisquer dados de instância armazenados no agente podem ser enviados para o servidor. Portanto, cada partição primária possui uma instância do agente. O método process é chamado

para cada instância uma vez para cada chave que resolve a partição. O resultado de cada método process é, então, serializado de volta para o cliente e retornado para o responsável pela chamada em uma instância de Mapa, onde o resultado é representado como o valor no mapa.

Quando o método AgentManager.callMapAgent é chamado sem uma coleção de chaves, a instância MapGridAgent é serializada e enviada para todas as partições primárias. Isto significa que quaisquer dados de instância armazenados no agente podem ser enviados para o servidor. Cada partição principal, portanto, tem uma instância (partição) do agente. O método processAllEntries é chamado para cada partição. O resultado de cada método processAllEntries é então serializado de volta para o cliente e retornado ao responsável pela chamada em uma instância de Mapa. O exemplo a seguir parte da premissa de que há uma entidade de Pessoa com o seguinte formato:

```
import com.ibm.websphere.projector.annotations.Entity;
import com.ibm.websphere.projector.annotations.Id;
@Entity
public class Person {
  @Id String ssn;
  String firstName;
  String surname;
  int age;
}
```

A função fornecida pelo aplicativo é redigida como uma classe que implementa a interface MapAgentGrid. Este é um agente de exemplo que mostra uma função para retornar a idade de uma Pessoa multiplicada por dois.

```
public class DoublePersonAgeAgent implements MapGridAgent, EntityAgentMixin
{
  private static final long serialVersionUID = -2006093916067992974L;

  int lowAge;
  int highAge;

  public Object process(Session s, ObjectMap map, Object key)
  {
    Person p = (Person)key;
    return new Integer(p.age * 2);
  }

  public Map processAllEntries(Session s, ObjectMap map)
  {
    EntityManager em = s.getEntityManager();
    Query q = em.createQuery("select p from Person p where p.age > ?1 and p.age < ?2");
    q.setParameter(1, lowAge);
    q.setParameter(2, highAge);
    Iterator iter = q.getResultIterator();
    Map<Person, Interger> rc = new HashMap<Person, Integer>();
   while(iter.hasNext())
    {
   Person p = (Person)iter.next();
   rc.put(p, (Integer)process(s, map, p));
  }
  return rc;
 }
 public Class getClassForEntity()
 {
  return Person.class;
 }
}
```

O exemplo anterior mostra o agente de Mapa para duplicar uma entidade de Pessoa. O primeiro método de processo é fornecido com a Pessoa com a qual trabalhar e retorna o dobro da idade dessa entrada. O segundo método do processo é chamado para cada partição e localiza todos os objetos Person com idades entre lowAge e highAge e retorna os dobros das idades.

```
Session s = grid.getSession();
ObjectMap map = s.getMap("Person");
AgentManager amgr = map.getAgentManager();
```

```
DoublePersonAgeAgent agent = new DoublePersonAgeAgent();

// make a list of keys
ArrayList<Person> keyList = new ArrayList<Person>();
Person p = new Person();
p.ssn = "1";
keyList.add(p);
p = new Person ();
p.ssn = "2";
keyList.add(p);

// get the results for those entries
Map<Tuple, Object> = amgr.callMapAgent(agent, keyList);
// Close the session (optional in Version 7.1.1 and later) for improved performance
s.close();
```

O exemplo anterior mostra um cliente que obtém uma Sessão e uma referência ao Mapa de Pessoa. A operação do agente é executada em um Mapa específico. A interface AgentManager é recuperada a partir de tal Mapa. Uma instância do agente a ser chamado é criada e qualquer estado necessário incluído no objeto pelos atributos da configuração; nesse caso, não há nenhum. Uma lista de chaves é construída. Um Mapa com os valores para pessoa 1 dobrados, e os mesmos valores para pessoa 2 são retornados.

Em seguida, o agente é chamado para esse conjunto de chaves. O método de processamento dos agentes é chamado em cada partição com algumas chaves especificadas na grade em paralelo. Um Mapa é retornado, fornecendo os resultados combinados para a chave especificada. Nesse caso, um Mapa com os valores que mantêm a idade da pessoa 1 dobrada e a mesma da pessoa 2 é retornado.

Mesmo que a chave não exista, o agente será chamado. Essa chamada oferece ao agente a oportunidade de criar a entrada do mapa. Se você estiver usando um EntityAgentMixin, a chave a ser processada não será a entidade, mas o valor real da chave Tupla da entidade. Se as chaves forem desconhecidas, será possível consultar todas as partições para localizar os objetos Pessoais de uma determinada forma e retornar suas idades duplicadas. Este é um exemplo:

```
Session s = grid.getSession();
  ObjectMap map = s.getMap("Person");
  AgentManager amgr = map.getAgentManager();

  DoublePersonAgeAgent agent = new DoublePersonAgeAgent();
  agent.lowAge = 20;
  agent.highAge = 9999;

  Map m = amgr.callMapAgent(agent);
```

O exemplo anterior mostra o AgentManager sendo obtido para o Mapa da Pessoa, e o agente construído e inicializado com as idades mínima e máxima para Pessoa de interesse. O agente é então chamado com o uso do método callMapAgent. Observe que nenhuma chave é fornecida. Como resultado, o ObjectGrid chama o agente em cada partição na grade em paralelo e retorna os resultados mesclados ao cliente. Este conjunto de devoluções contêm todos os objetos Pessoais na grade com uma idade entre menor e maior e calcula a idade desses objetos Pessoais duplicada. Esse exemplo mostra como as APIs na grade podem ser usadas para executar uma consulta para localizar as entidades que correspondem a uma determinada consulta. O agente é serializado e transportado pelo ObjectGrid para as partições com as entradas necessárias. Os resultados são similarmente serializados para o transporte de volta ao cliente. É necessário ter cuidado com as APIs do Mapa. Se o ObjectGrid estivesse hospedando terabytes de objetos e sendo

executado em muitos servidores, esse processamento potencialmente sobrecarregaria as máquinas do cliente. Use as APIs de Mapa para processar um subconjunto pequeno. Se for necessário processar um grande subconjunto, use um agente de redução para executar o processamento fora da grade de dados em vez de fazê-lo em um cliente.

Redução de Paralelo ou agentes de agregação

Este estilo de programação processa um subconjunto das entradas e calcula um único resultado para o grupo de entradas. Os exemplos de resultados podem ser:

- Valor mínimo
- Valor máximo
- Alguma outra função específica do negócio

Um agente de redução é codificado e chamado de modo similar aos agentes de Mapa.

Fluxo de chamada ReduceGridAgent

Quando o método AgentManager.callReduceAgent é chamado com uma coleção de chaves, a instância ReduceGridAgent é serializada e enviada para cada partição primária que as chaves resolvem. Isto significa que quaisquer dados de instância armazenados no agente podem ser enviados para o servidor. Portanto, cada partição primária possui uma instância do agente. O método reduce(Session s, ObjectMap map, Collection keys) é chamado uma vez por instância (partição) com o subconjunto de chaves que resolve a partição. O resultado de cada método de redução é, então, serializado de volta para o cliente. O método reduceResults é chamado na instância ReduceGridAgent do cliente com a coleção de cada resultado de cada chamada de redução remota. O resultado do método reduceResults é retornado para o responsável pela chamada do método callReduceAgent.

Quando o método AgentManager.callReduceAgent é chamado sem uma coleção de chaves, o ReduceGridAgentinstance é serializado e enviado para cada partição primária. Isto significa que quaisquer dados de instância armazenados no agente podem ser enviados para o servidor. Portanto, cada partição primária possui uma instância do agente. O método reduce(Session s, ObjectMap map) é chamado uma vez por instância (partição). O resultado de cada método de redução é, então, serializado de volta para o cliente. O método reduceResults é chamado na instância ReduceGridAgent do cliente com a coleção de cada resultado de cada chamada de redução remota. O resultado do método reduceResults é retornado para o responsável pela chamada do método callReduceAgent. Este é um exemplo de um agente de redução que simplesmente inclui as idades das entradas compatíveis.

```
package com.ibm.ws.objectgrid.test.agent.jdk5;

import java.util.Collection;
import java.util.Iterator;

import com.ibm.websphere.objectgrid.ObjectMap;
import com.ibm.websphere.objectgrid.Session;
import com.ibm.websphere.objectgrid.datagrid.EntryErrorValue;
import com.ibm.websphere.objectgrid.datagrid.ReduceGridAgent;
import com.ibm.websphere.objectgrid.query.ObjectQuery;
import com.ibm.websphere.samples.objectgrid.entityxmlgen.PersonFeature1Entity.PersonKey;

public class SumAgeReduceAgent implements ReduceGridAgent {
 private static final long serialVersionUID = 2521080771723284899L;

 /**
  * Invoked on the server if a collection of keys is passed to
  * AgentManager.callReduceAgent(). This is invoked on each primary shard
  * where the key applies.
  */
 public Object reduce(Session s, ObjectMap map, Collection keyList) {
  try {
```

```
  int sum = 0;
  Iterator<PersonKey> iter = keyList.iterator();
  while (iter.hasNext()) {
   Object nextKey = iter.next();
   PersonKey pk = (PersonKey) nextKey;
   Person p = (Person) map.get(pk);
   sum += p.age;
  }

  return sum;
 } catch (Exception e) {
  throw new RuntimeException(e.getMessage(), e);
 }
}

/**
 * Invoked on the server if a collection of keys is NOT passed to
 * AgentManager.callReduceAgent(). This is invoked on every primary shard.
 */
public Object reduce(Session s, ObjectMap map) {
 ObjectQuery q = s
   .createObjectQuery("select p from Person p where p.age > -1");
 Iterator<Person> iter = q.getResultIterator();
 int sum = 0;
 while (iter.hasNext()) {
  Object nextKey = iter.next();
  Person p = (Person) nextKey;
  sum += p.age;
 }
 return sum;
}

/**
 * Invoked on the client to reduce the results from all partitions.
 */
public Object reduceResults(Collection results) {
 // If we encounter an EntryErrorValue, then throw a RuntimeException
 // to indicate that there was at least one failure and include each
 // EntryErrorValue
 // as part of the thrown exception.
 Iterator<Integer> iter = results.iterator();
 int sum = 0;
 while (iter.hasNext()) {
  Object nextResult = iter.next();
  if (nextResult instanceof EntryErrorValue) {
   EntryErrorValue eev = (EntryErrorValue) nextResult;
   throw new RuntimeException(
     "Erro encontrado em uma das partições: "
       + nextResult, eev.getException());
  }

  sum += ((Integer) nextResult).intValue();
 }
 return new Integer(sum);
}
}
```

O exemplo anterior mostra o agente. O agente tem três partes importantes. A primeira permite que um conjunto específico de entradas seja processado sem uma consulta. Ela itera o conjunto de entradas, incluindo as idades. A soma é retornada do método. A segunda utiliza uma consulta para selecionar as entradas a serem agregadas. Em seguida, ela soma todas as idades Person correspondentes. O terceiro método é utilizado para agregar os resultados de cada partição a um único resultado. O ObjectGrid executa a agregação de entradas em paralelo por meio do grade. Cada partição produz um resultado intermediário que deve ser agregado aos resultados intermediários de outra partição. Esse terceiro método executa essa tarefa. No exemplo a seguir, o agente é chamado e as idades de todas as Pessoas exclusivamente com idades entre 10 e 20 são agregadas:

```
Session s = grid.getSession();
ObjectMap map = s.getMap("Person");
AgentManager amgr = map.getAgentManager();

SumAgeReduceAgent agent = new SumAgeReduceAgent();

Person p = new Person();
p.ssn = "1";
ArrayList<Person> list = new ArrayList<Person>();
list.add(p);
p = new Person ();
```

```
p.ssn = "2";
list.add(p);
Integer v = (Integer)amgr.callReduceAgent(agent, list);
// Close the session (optional in Version 7.1.1 and later) for improved performance
s.close();
```

Funções do agente

O agente é livre para fazer operações de ObjectMap ou EntityManager dentro do shard local onde está executando. O agente recebe uma Sessão e pode incluir, atualizar, consultar, ler ou remover dados da partição que a Sessão representa. Alguns aplicativos consultam somente dados da grade, mas também é possível gravar um agente para incrementar todas as idades da Pessoa em 1 que correspondam a uma determinada consulta. Existe uma transação na Sessão quando o agente é chamado, e é consolidado quando o agente retorna, a menos que uma exceção seja lançada

Manipulação de erros

Se um agente de mapa for chamado com uma chave desconhecida, o valor retornado será um objeto de erro que implementa a interface EntryErrorValue.

Transações

Um agente de mapas é executado numa transação separada do cliente. As chamadas do agente podem ser agrupadas numa única transação. Se um agente falhar e lançar uma exceção, a transação será retrocedida. Quaisquer agentes executados com êxito em uma transação retrocederão com o agente com falha. O AgentManager executará novamente os agentes retrocedidos que foram executados com êxito em uma nova transação.

Informações relacionadas:

Java API de DataGrid

Configurando Clientes Programaticamente

Java

É possível substituir as configurações do lado do cliente programaticamente. Crie um objeto ObjectGridConfiguration que seja semelhante em estrutura à instância de ObjectGrid do lado do servidor.

Sobre Esta Tarefa

O exemplo de código a seguir cria as mesmas substituições que são descritas no Configurando Clientes com a Configuração XML.

Para obter uma lista dos plug-ins e atributos que podem ser substituídos no cliente, consulte “Substituições do Cliente” na página 516.

Procedimento

O código a seguir cria uma instância do ObjectGrid do lado do cliente.

```
ObjectGridConfiguration companyGridConfig = ObjectGridConfigFactory
    .createObjectGridConfiguration("CompanyGrid");
Plugin txCallbackPlugin = ObjectGridConfigFactory.createPlugin(
    PluginType.TRANSACTION_CALLBACK, "com.company.MyClientTxCallback");
companyGridConfig.addPlugin(txCallbackPlugin);
```

```
Plugin ogEventListenerPlugin = ObjectGridConfigFactory.createPlugin(
    PluginType.OBJECTGRID_EVENT_LISTENER, "");
companyGridConfig.addPlugin(ogEventListenerPlugin);

BackingMapConfiguration customerMapConfig = ObjectGridConfigFactory
    .createBackingMapConfiguration("Customer");
customerMapConfig.setNumberOfBuckets(1429);
Plugin evictorPlugin = ObjectGridConfigFactory.createPlugin(PluginType.EVICTOR,
    "com.ibm.websphere.objectgrid.plugins.builtins.LRUEvictor");
customerMapConfig.addPlugin(evictorPlugin);

companyGridConfig.addBackingMapConfiguration(customerMapConfig);

BackingMapConfiguration orderLineMapConfig = ObjectGridConfigFactory
    .createBackingMapConfiguration("OrderLine");
orderLineMapConfig.setNumberOfBuckets(701);
orderLineMapConfig.setTimeToLive(800);
orderLineMapConfig.setTtlEvictorType(TTLType.LAST_ACCESS_TIME);

companyGridConfig.addBackingMapConfiguration(orderLineMapConfig);

List ogConfigs = new ArrayList();
ogConfigs.add(companyGridConfig);

Map overrideMap = new HashMap();
overrideMap.put(CatalogServerProperties.DEFAULT_DOMAIN, ogConfigs);

ogManager.setOverrideObjectGridConfigurations(overrideMap);
ClientClusterContext client =
ogManager.connect(catalogServerEndpoints, null, null);
ObjectGrid companyGrid = ogManager.getObjectGrid(client, objectGridName);
```

A instância ogManager da interface ObjectGridManager verifica se há substituições apenas nos objetos ObjectGridConfiguration e BackingMapConfiguration que você inclui no Mapa overrideMap. Por exemplo, o código anterior substitui o número de depósitos no mapa OrderLine. Entretanto, o mapa Order permanece inalterado no lado do cliente porque nenhuma configuração para esse mapa é incluída.

Substituições do Cliente: Java

É possível configurar um cliente do WebSphere eXtreme Scale com base em seus requisitos, substituindo as configurações do servidor. É possível substituir vários plug-ins e atributos.

Para substituir as configurações em um cliente, você pode utilizar a configuração XML ou programática. Para obter mais informações sobre como substituir configurações do cliente, consulte Configurando Clientes com a Configuração XML e “Configurando Clientes Programaticamente” na página 515.

É possível substituir os seguintes plug-ins em um cliente:

- **Plug-ins do BackingMap**
  - Plug-in Evictor
  - Plug-in MapEventListener
  - Plug-in BackingMapLifecycleListener
  - Plug-in MapSerializerPlugin
- **Atributos de BackingMap**
  - Atributo numberOfBuckets

    Reprovado: Esta propriedade foi descontinuada. Use o atributo nearCacheEnabled para ativar o cache local.
  - Atributo timeToLive
  - Atributo ttlEvictorType

  - Atributo evictionTriggers
  - 8.6+ Atributo nearCacheEnabled
  - 8.6+ Atributo nearCacheInvalidationEnabled
  - 8.6+ Atributo nearCacheLastAccessTTLSyncEnabled
- **Plug-ins do ObjectGrid**
  - Plug-in TransactionCallback
  - Plug-in ObjectGridEventListener
  - Plug-in ObjectGridLifecycleListener
- **atributos ObjectGrid**
  - Atributo entityMetadataXMLFile
  - Atributo txTimeout
  - Atributo txIsolation

Ativando a Replicação de Mapas do Lado do Cliente: Java

Você também pode ativar a replicação de mapas no lado do cliente para disponibilizar os dados mais rápido.

Com o eXtreme Scale, é possível replicar um mapa de servidor em um ou mais clientes utilizando a replicação assíncrona. Um cliente pode pedir uma cópia local somente leitura de um mapa de lado do servidor utilizando o método ClientReplicableMap.enableClientReplication.

```
void enableClientReplication(Mode mode, int[] partitions,
ReplicationMapListener listener) throws ObjectGridException;
```

O primeiro parâmetro é o modo de replicação. Esse modo pode ser uma replicação contínua ou uma replicação de captura instantânea. O segundo parâmetro é uma matriz de IDs de partição que representa as partições a partir das quais replicar os dados. Se o valor for nulo ou uma matriz vazia, os dados são replicados a partir de todas as partições. O último parâmetro é um listener para receber eventos de replicação de cliente. Consulte ClientReplicableMap e ReplicationMapListener na documentação da API para obter detalhes.

Depois de ativada a replicação, então o servidor começa a replicar o mapa para o cliente. O cliente eventualmente está apenas algumas transações atrás do servidor em questão de tempo.

Acessando Dados com o Serviço de Dados REST

Java

Desenvolva aplicativos que executam operações usando protocolos do serviço de dados REST.

Conceitos relacionados:

Java "Operações com o Serviço de Dados REST"
Após iniciar o serviço de dados REST do eXtreme Scale, é possível usar qualquer cliente HTTP para interagir com ele. Um navegador da Web, um cliente PHP, um cliente Java ou um cliente WCF Data Services podem ser utilizados para emitir quaisquer operações de pedido suportadas.

Java "Visão Geral do Serviço de Dados REST" na página 327
O serviço de dados REST WebSphere eXtreme Scale é um serviço HTTP Java compatível com Microsoft WCF Data Services (formalmente, ADO.NET Data Services) e implementa o Open Data Protocol (OData). O Microsoft WCF Data Services é compatível com essa especificação quando utiliza Visual Studio 2008 SP1 e .NET Framework 3.5 SP1.

Referências relacionadas:

Java "Simultaneidade Otimista no Serviço de Dados REST" na página 522
O serviço de dados REST do eXtreme Scale usa um modelo de bloqueio otimista ao usar cabeçalhos HTTP nativos: If-Match, If-None-Match e ETag. Esses cabeçalhos são enviados em mensagens de pedido e de resposta para retransmitir informações da versão da entidade do servidor para o cliente e do cliente para o servidor.

Java "Protocolos de Pedido para o Serviço de Dados REST" na página 523
No geral, os protocolos para interação com o serviço REST são os mesmos que os descritos no protocolo AtomPub de Serviços de Dados WCF. No entanto, o eXtreme Scale fornece detalhes adicionais, da perspectiva Modelo de Entidade do eXtreme Scale. Os usuários devem estar familiarizados com os protocolos WCF Data Services antes de lerem esta seção. Alternativamente, os usuários podem ler esta seção com a seção do protocolo WCF Data Services.

Java "Recuperar Pedidos com Serviço de Dados REST" na página 524
Um Pedido RetrieveEntity é usado por um cliente para recuperar uma entidade do eXtreme Scale. A carga útil da resposta contém os dados da entidade no formato AtomPub ou JSON. Além disso, o operador do sistema $expand pode ser utilizado para expandir as relações. As relações são representadas em sequência dentro da resposta do serviço de dados como um Atom Feed Document, que é uma relação para-muitos, ou um Atom Entry Document que é uma relação para-um.

Java "Recuperando Não Entidades com Serviços de Dados REST" na página 531
O serviço de dados REST permite recuperar mais que apenas entidades, como coletas e propriedades das entidades.

Java "Pedidos de Inserção com Serviço de Dados REST" na página 537
Um Pedido InsertEntity pode ser usado para inserir uma nova instância de entidade do eXtreme Scale, potencialmente com novas entidades relacionadas, no serviço de dados REST do eXtreme Scale.

Java "Pedidos de Atualização com Serviço de Dados REST" na página 541
O serviço de dados REST do WebSphere eXtreme Scale suporta pedidos de atualização para entidades, propriedades de primitivas de entidades e assim por diante.

Java "Pedidos de Exclusão com Serviços de Dados REST" na página 546
O serviço de dados REST do WebSphere eXtreme Scale pode excluir entidades, valores da propriedade e links.

Operações com o Serviço de Dados REST

Java

Após iniciar o serviço de dados REST do eXtreme Scale, é possível usar qualquer cliente HTTP para interagir com ele. Um navegador da Web, um cliente PHP, um cliente Java ou um cliente WCF Data Services podem ser utilizados para emitir quaisquer operações de pedido suportadas.

O serviço REST implementa um subconjunto da especificação Microsoft Atom Publishing Protocol: Data Services URI and Payload Extensions, Versão 1.0, que faz parte do protocolo OData. Este tópico descreve quais dos recursos da especificação são suportados e como eles são mapeados para o eXtreme Scale.

URI da Raiz do Serviço

O Microsoft WCF Data Services normalmente define um serviço por origem de dados ou modelo de entidade. O serviço de dados REST do eXtreme Scale define um serviço por ObjectGrid definido. Cada ObjectGrid que é definido no arquivo XML de substituição de cliente do ObjectGrid do eXtreme Scale é automaticamente exposto como uma raiz de serviço REST separada.

O URI para a raiz do serviço é:

`http://host:port/contextroot/restservice/gridname`

Em que:

- *contextroot* é definido quando você implementa o aplicativo de serviço de dados REST e depende do servidor de aplicativos
- *gridname* é o nome do ObjectGrid

Tipos de Pedidos

A lista a seguir descreve os tipos de pedidos do Microsoft WCF Data Services suportados pelo serviço de dados REST do eXtreme Scale. Para obter detalhes sobre cada tipo de pedido suportado pelo WCF Data Services, consulte: MSDN: Tipos de Pedidos.

Tipos de pedido de inserção

Clientes podem inserir recursos utilizando o verbo POST HTTP com as seguintes limitações:

- Pedido InsertEntity: Suportado.
- Pedido InsertLink: Suportado.
- Pedido InsertMediaResource: Não suportado devido à restrição de suporte do recurso de mídia.

Para obter informações adicionais, consulte MSDN: Inserir Tipos de Pedidos.

Tipos de pedido de atualização

Clientes podem atualizar recursos utilizando os verbos PUT e MERGE HTTP com as seguintes limitações:

Nota: 8.6+ Os métodos upsert e upsertAll substituem os métodos put e putAll do ObjectMap. Use o método upsert para informar ao BackingMap e carregador que uma entrada na grade de dados precisa colocar a chave e o valor na grade. O BackingMap e carregador executam uma inserção ou uma atualização para colocar o valor na grade e no carregador. Se você executar a API upsert dentro de seus aplicativos, o

carregador obterá um tipo UPSERT de LogElement, que permite que carregadores façam a mesclagem do banco de dados ou chamadas upsert em vez de usar insert ou update.

- Pedido UpdateEntity: Suportado.
- Pedido UpdateComplexType: Não suportado devido à restrição de tipo complexo.
- Pedido UpdatePrimitiveProperty: Suportado.
- Pedido UpdateValue: Suportado.
- Pedido UpdateLink: Suportado.
- Pedido UpdateMediaResource: Não suportado devido à restrição de suporte do recurso de mídia.

Para obter informações adicionais, consulte: MSDN: Inserir Tipos de Pedidos.

Tipos de pedido de exclusão

Clientes podem excluir recursos utilizando o verbo DELETE HTTP com as seguintes limitações:

- Pedido DeleteEntity: Suportado.
- Pedido DeleteLink: Suportado.
- Pedido DeleteValue: Suportado.

Para obter informações adicionais, consulte: MSDN: Excluir Tipos de Pedidos.

Tipos de pedido de recuperação

Clientes podem recuperar recursos utilizando o verbo GET HTTP com as seguintes limitações:

- Pedido RetrieveEntitySet: Suportado.
- Pedido RetrieveEntity: Suportado.
- Pedido RetrieveComplexType: Não suportado devido à restrição de tipo complexo.
- Pedido RetrievePrimitiveProperty: Suportado.
- Pedido RetrieveValue: Suportado.
- Pedido RetrieveServiceMetadata: Suportado.
- Pedido RetrieveServiceDocument: Suportado.
- Pedido RetrieveLink: Suportado.
- Pedido Retrieve Contendo um Mapeamento de Feed Customizável: Não Suportado.
- RetrieveMediaResource: Não suportado devido à restrição de recurso de mídia.

Para obter informações adicionais, consulte: MSDN: Recuperar Tipos de Pedidos.

Opções de consulta do sistema

São suportadas consultas que permitem que clientes identifiquem uma coleta de entidades ou uma única entidade. As opções de consulta do sistema são especificadas em um URI de serviço de dados e são suportadas com as seguintes limitações:

- $expand: Suportada.
- $filter: Suportada.

- $orderby: Suportada.
- $format: Não suportada. O formato aceitável é identificado no cabeçalho do pedido HTTP Accept.
- $skip: Suportada.
- $top: Suportada.

Para obter informações adicionais, consulte: MSDN: Opções de Consulta do Sistema.

Roteamento de partição

O roteamento de partição é baseado na entidade raiz. Um URI de pedido infere uma entidade raiz se o caminho do recurso começar com uma entidade raiz ou com uma entidade que tenha uma associação direta ou indireta com a entidade. Em um ambiente particionado, qualquer pedido que não possa inferir uma entidade raiz será rejeitado. Qualquer pedido que infira uma entidade raiz será roteado para a partição correta.

Para obter informações adicionais sobre como definir um esquema com associações e entidades-raiz, consulte o Modelo de Dados Escalável no eXtreme Scale e o Particionamento.

Pedido de Chamada

Pedidos de chamada não são suportados. Para obter informações adicionais, consulte MSDN: Pedido de Chamada.

Pedido em Lote

Clientes podem criar lotes de vários Conjuntos de Mudanças ou Operações de Consulta dentro de um único pedido. Isso pode reduzir o número de roundtrips para o servidor e permite que vários pedidos participem de uma única transação. Para obter informações adicionais, consulte MSDN: Pedido em Lote.

Pedidos em Túnel

Pedidos em túnel não são suportados. Para obter informações adicionais, consulte MSDN: Pedidos em Túnel.

Tarefas relacionadas:

Java "Acessando Dados com o Serviço de Dados REST" na página 517
Desenvolva aplicativos que executam operações usando protocolos do serviço de dados REST.

Referências relacionadas:

Java "Simultaneidade Otimista no Serviço de Dados REST"
O serviço de dados REST do eXtreme Scale usa um modelo de bloqueio otimista ao usar cabeçalhos HTTP nativos: If-Match, If-None-Match e ETag. Esses cabeçalhos são enviados em mensagens de pedido e de resposta para retransmitir informações da versão da entidade do servidor para o cliente e do cliente para o servidor.

Java "Protocolos de Pedido para o Serviço de Dados REST" na página 523
No geral, os protocolos para interação com o serviço REST são os mesmos que os descritos no protocolo AtomPub de Serviços de Dados WCF. No entanto, o eXtreme Scale fornece detalhes adicionais, da perspectiva Modelo de Entidade do eXtreme Scale. Os usuários devem estar familiarizados com os protocolos WCF Data Services antes de lerem esta seção. Alternativamente, os usuários podem ler esta seção com a seção do protocolo WCF Data Services.

Java "Recuperar Pedidos com Serviço de Dados REST" na página 524
Um Pedido RetrieveEntity é usado por um cliente para recuperar uma entidade do eXtreme Scale. A carga útil da resposta contém os dados da entidade no formato AtomPub ou JSON. Além disso, o operador do sistema $expand pode ser utilizado para expandir as relações. As relações são representadas em sequência dentro da resposta do serviço de dados como um Atom Feed Document, que é uma relação para-muitos, ou um Atom Entry Document que é uma relação para-um.

Java "Recuperando Não Entidades com Serviços de Dados REST" na página 531
O serviço de dados REST permite recuperar mais que apenas entidades, como coletas e propriedades das entidades.

Java "Pedidos de Inserção com Serviço de Dados REST" na página 537
Um Pedido InsertEntity pode ser usado para inserir uma nova instância de entidade do eXtreme Scale, potencialmente com novas entidades relacionadas, no serviço de dados REST do eXtreme Scale.

Java "Pedidos de Atualização com Serviço de Dados REST" na página 541
O serviço de dados REST do WebSphere eXtreme Scale suporta pedidos de atualização para entidades, propriedades de primitivas de entidades e assim por diante.

Java "Pedidos de Exclusão com Serviços de Dados REST" na página 546
O serviço de dados REST do WebSphere eXtreme Scale pode excluir entidades, valores da propriedade e links.

Simultaneidade Otimista no Serviço de Dados REST

Java

O serviço de dados REST do eXtreme Scale usa um modelo de bloqueio otimista ao usar cabeçalhos HTTP nativos: If-Match, If-None-Match e ETag. Esses cabeçalhos são enviados em mensagens de pedido e de resposta para retransmitir informações da versão da entidade do servidor para o cliente e do cliente para o servidor.

Para obter mais detalhes sobre a simultaneidade otimista, consulte Biblioteca MSDN: Simultaneidade Otimista (ADO.NET).

O serviço de dados REST do eXtreme Scale ativará a simultaneidade otimista para uma entidade se um atributo de versão for definido no esquema de entidade para essa entidade. Uma propriedade de versão pode ser definida no esquema da entidade por uma anotação @Version para classes Java ou um atributo <version/> para entidades definidas com o uso de um arquivo XML do descritor de entidade. O serviço de dados REST do eXtreme Scale propaga automaticamente o valor da propriedade da versão para o cliente no cabeçalho ETag para respostas únicas da entidade usando um atributo m:etag na carga útil para várias respostas XML da entidade e um atributo etag na carga útil para várias respostas JSON da entidade.

Para obter mais detalhes sobre como definir um esquema de entidade do eXtreme Scale, consulte “Definindo um Esquema de Entidade” na página 391.

Conceitos relacionados:

Java “Operações com o Serviço de Dados REST” na página 518
Após iniciar o serviço de dados REST do eXtreme Scale, é possível usar qualquer cliente HTTP para interagir com ele. Um navegador da Web, um cliente PHP, um cliente Java ou um cliente WCF Data Services podem ser utilizados para emitir quaisquer operações de pedido suportadas.

Java “Visão Geral do Serviço de Dados REST” na página 327
O serviço de dados REST WebSphere eXtreme Scale é um serviço HTTP Java compatível com Microsoft WCF Data Services (formalmente, ADO.NET Data Services) e implementa o Open Data Protocol (OData). O Microsoft WCF Data Services é compatível com essa especificação quando utiliza Visual Studio 2008 SP1 e .NET Framework 3.5 SP1.

Tarefas relacionadas:

Java “Acessando Dados com o Serviço de Dados REST” na página 517
Desenvolva aplicativos que executam operações usando protocolos do serviço de dados REST.

Protocolos de Pedido para o Serviço de Dados REST

Java

No geral, os protocolos para interação com o serviço REST são os mesmos que os descritos no protocolo AtomPub de Serviços de Dados WCF. No entanto, o eXtreme Scale fornece detalhes adicionais, da perspectiva Modelo de Entidade do eXtreme Scale. Os usuários devem estar familiarizados com os protocolos WCF Data Services antes de lerem esta seção. Alternativamente, os usuários podem ler esta seção com a seção do protocolo WCF Data Services.

São fornecidos exemplos para ilustrar o pedido e a resposta. Esses exemplos aplicam-se ao serviço de dados REST e aos Serviços de Dados WCF do eXtreme Scale. Como os navegadores da Web podem apenas recuperar dados, as operações CUD (create, update and delete) devem ser executadas por outro cliente, como Java, JavaScript, RUBY ou PHP.

Conceitos relacionados:

Java "Operações com o Serviço de Dados REST" na página 518
Após iniciar o serviço de dados REST do eXtreme Scale, é possível usar qualquer cliente HTTP para interagir com ele. Um navegador da Web, um cliente PHP, um cliente Java ou um cliente WCF Data Services podem ser utilizados para emitir quaisquer operações de pedido suportadas.

Java "Visão Geral do Serviço de Dados REST" na página 327
O serviço de dados REST WebSphere eXtreme Scale é um serviço HTTP Java compatível com Microsoft WCF Data Services (formalmente, ADO.NET Data Services) e implementa o Open Data Protocol (OData). O Microsoft WCF Data Services é compatível com essa especificação quando utiliza Visual Studio 2008 SP1 e .NET Framework 3.5 SP1.

Tarefas relacionadas:

Java "Acessando Dados com o Serviço de Dados REST" na página 517
Desenvolva aplicativos que executam operações usando protocolos do serviço de dados REST.

Recuperar Pedidos com Serviço de Dados REST: Java

Um Pedido RetrieveEntity é usado por um cliente para recuperar uma entidade do eXtreme Scale. A carga útil da resposta contém os dados da entidade no formato AtomPub ou JSON. Além disso, o operador do sistema $expand pode ser utilizado para expandir as relações. As relações são representadas em sequência dentro da resposta do serviço de dados como um Atom Feed Document, que é uma relação para-muitos, ou um Atom Entry Document que é uma relação para-um.

Dica: Para obter mais detalhes sobre o protocolo RetrieveEntity definido no WCF Data Services, consulte MSDN: Solicitação RetrieveEntity.

Recuperando uma Entidade

O exemplo de RetrieveEntity a seguir recupera uma entidade Customer com uma chave.

AtomPub

- Método

  GET
- URI do Pedido:

  http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('ACME')
- Cabeçalho do Pedido:

  Aceitar: application/atom+xml
- Carga Útil de Pedido:

  Nenhum
- Cabeçalho da Resposta:

  Tipo de Conteúdo: application/atom+xml
- Carga Útil de Resposta:

```
<?xml version="1.0"
encoding="ISO-8859-1"?>
<entry xml:base = "http://localhost:8080/wxsrestservice/
restservice" xmlns:d= "http://schemas.microsoft.com/ado/2007/
08/dataservices" xmlns:m = "http://schemas.microsoft.com/ado/2007/
```

```
08/dataservices/metadata" xmlns = "http://www.w3.org/2005/Atom">

<category term = "NorthwindGridModel.Customer" scheme = "http://
schemas.microsoft.com/ado/2007/08/dataservices/scheme"/>
<id>http://localhost:8080/wxsrestservice/restservice/
   NorthwindGrid/Customer('ACME')</id>
    <title type = "text"/>
    <updated>2009-12-16T19:52:10.593Z</updated>
    <author>
        <name/>
    </author>
    <link rel = "edit" title = "Customer" href =
"Customer('ACME')"/>
    <link rel = "http://schemas.microsoft.com/ado/2007/08/
     dataservices/related/
orders" type =
"application/atom+xml;type=feed" title =
  "orders" href ="Customer('ACME')/orders"/>
    <content type="application/xml">
        <m:properties>
            <d:customerId>ACME</d:customerId>
            <d:city m:null = "true"/>
            <d:companyName>RoaderRunner</d:companyName>
            <d:contactName>ACME</d:contactName>
            <d:country m:null = "true"/>
            <d:version m:type = "Edm.Int32">3</d:version>
        </m:properties>
    </content>
</entry>
```

- Código de Resposta:

  200 OK

JSON

- Método

  GET

- URI do Pedido:

  http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('ACME')

- Cabeçalho do Pedido:

  Aceitar: application/json

- Carga Útil de Pedido:

  Nenhum

- Cabeçalho da Resposta:

  Tipo de Conteúdo: application/json

- Carga Útil de Resposta:

```
{"d":{"__metadata":{"uri":"http://localhost:8080/wxsrestservice/
   restservice/NorthwindGrid/Customer('ACME')",
   "type":"NorthwindGridModel.Customer"},
   "customerId":"ACME",
   "city":null,
   "companyName":"RoaderRunner",
   "contactName":"ACME",
   "country":null,
   "version":3,
   "orders":{"__deferred":{"uri":"http://localhost:8080/
      wxsrestservice/restservice/
   NorthwindGrid/Customer('ACME')/orders"}}}}
```

- Código de Resposta:

  200 OK

Consultas

Uma consulta também pode ser utilizada com um pedido RetrieveEntitySet ou RetrieveEntity. Uma consulta é especificada pelo operador $filter do sistema.

Para obter detalhes sobre o operador $filter, consulte: MSDN: Opção de Consulta do Sistema de Filtros ($filter)

O protocolo OData suporta várias expressões comuns. O serviço de dados REST do eXtreme Scale suporta um subconjunto de expressões definidas na especificação:

- Expressões Booleanas:
  - eq, ne, lt, le, gt, ge
  - negate
  - not
  - parenthesis
  - and, or
- Expressões Aritméticas:
  - add
  - sub
  - mul
  - div
- Literais de Primitivas
  - Sequência
  - date-time
  - decimal
  - único
  - double
  - int16
  - int32
  - int64
  - binário
  - null
  - byte

As expressões a seguir *não* estão disponíveis:

- Expressões Booleanas:
  - isof
  - cast
- Expressões de Chamada de Método
- Expressões Aritméticas:
  - mod
- Literais de primitivas:
  - Guid
- Expressões de Membro

Para obter uma lista e uma descrição completas das expressões que estão disponíveis no Microsoft WCF Data Services, consulte a seção 2.2.3.6.1.1: Sintaxe de Expressão Comum.

O exemplo a seguir demonstra um pedido RetrieveEntity com uma consulta. Neste exemplo, todos os clientes cujo nome do contato é “RoadRunner” são recuperados. O único cliente que corresponde a esse filtro é Customer('ACME'), conforme mostrado na carga útil da resposta.

Restrição: Essa consulta só funcionará para entidades não particionadas. Se Customer for particionada, a chave pertencente ao cliente será necessária.

AtomPub

- Método: GET
- URI de Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer?$filter=contactName eq 'RoadRunner'
- Cabeçalho do Pedido: Aceitar: application/atom+xml
- Carga Útil de Entrada: Nenhuma
- Cabeçalho de Resposta: Conteúdo-Tipo: application/atom+xml
- Carga Útil de Resposta:

```
<?xml version="1.0"
encoding="iso-8859-1"?>
<feed
 xml:base="http://localhost:8080/wxsrestservice/restservice"
 xmlns:d="http://schemas.microsoft.com/ado/2007/08/
   dataservices"
 xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata"
 xmlns="http://www.w3.org/2005/Atom">
 <title type="text">Customer</title>
 <id>http://localhost:8080/wxsrestservice/restservice/
   NorthwindGrid/Customer </id>
 <updated>2009-09-16T04:59:28.656Z</updated>
 <link rel="self" title="Customer" href="Customer" />
 <entry>
  <category term="NorthwindGridModel.Customer"
   scheme="http://schemas.microsoft.com/ado/2007/08/
   dataservices/scheme"/>
  <id>
http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/
  Customer('ACME')</id>
  <title type = "text"/>
  <updated>2009-09-16T04:59:28.656Z</updated>
  <author>
   <name />
  </author>
  <link rel="edit" title="Customer" href="Customer('ACME')" />
  <link
   rel="http://schemas.microsoft.com/ado/2007/08/dataservices/
      related/orders"
   type=
"application/atom+xml;type=feed" title="orders"
   href="Customer('ACME')/orders" />
  <content type="application/xml">
     <m:properties>
            <d:customerId>ACME</d:customerId>
            <d:city m:null = "true"/>
            <d:companyName>RoaderRunner</d:companyName>
            <d:contactName>ACME</d:contactName>
            <d:country m:null = "true"/>
            <d:version m:type = "Edm.Int32">3</d:version>
       </m:properties>
  </content>
 </entry>
</feed>
```

- Código de Resposta: 200 OK

JSON

- Método: GET
- URI do Pedido:

  http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer?$filter=contactName eq 'RoadRunner'
- Cabeçalho do Pedido: Aceitar: application/json
- Carga Útil de Pedido: Nenhuma
- Cabeçalho de Resposta: Conteúdo-Tipo: application/json
- Carga Útil de Resposta:

```
{"d":[{"__metadata":{"uri":"http://localhost:8080/wxsrestservice/
   restservice/NorthwindGrid/Customer('ACME')",
   "type":"NorthwindGridModel.Customer"},
   "customerId":"ACME",
   "city":null,
   "companyName":"RoaderRunner",
   "contactName":"ACME",
   "country":null,
   "version":3,
   "orders":{"__deferred":{"uri":"http://localhost:8080/
     wxsrestservice/restservice/NorthwindGrid/
     Customer('ACME')/orders"}}}]}
```

- Código de Resposta: 200 OK

Operador do Sistema $expand

O operador do sistema $expand pode ser utilizado para expandir associações. As associações são representadas em linha na resposta do serviço de dados. As associações com diversos valores (para-muitos) são representadas como um Atom Feed Document ou matriz JSON. As associações com valor único (para-um) são representadas como um Atom Entry Document ou objeto JSON.

Para obter mais detalhes sobre o operador do sistema $expand, consulte Expandir Opção de Consulta do Sistema ($expand).

Veja aqui um exemplo de uso do operador do sistema $expand. Neste exemplo, recuperamos a entidade Customer('IBM') com Orders 5000, 5001 e outras associadas a ela. A cláusula $expand está configurada como “orders”, portanto, a coleta de pedidos será expandida como sequencial na carga útil da resposta. Apenas os pedidos 5000 e 5001 são exibidos aqui.

AtomPub

- Método: GET
- URI do Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')?$expand=orders
- Cabeçalho do Pedido: Aceitar: application/atom+xml
- Carga Útil de Pedido: Nenhuma
- Cabeçalho de Resposta: Conteúdo-Tipo: application/atom+xml
- Carga Útil de Resposta:

```
<?xml version="1.0" encoding="utf-8"?>
<entry xml:base = "http://localhost:8080/wxsrestservice/restservice"
   xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices"
   xmlns:m = "http://schemas.microsoft.com/ado/2007/08/dataservices/
   metadata" xmlns = "http://www.w3.org/2005/Atom">
<category term = "NorthwindGridModel.Customer" scheme = "http://schemas.
```

```
microsoft.com/ado/2007/08/dataservices/scheme"/>
    <id>http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/
    Customer('IBM')</id>
    <title type = "text"/>
    <updated>2009-12-16T22:50:18.156Z</updated>
    <author>
        <name/>
    </author><link rel = "edit" title = "Customer" href =
"Customer('IBM')"/>
    <link rel = "http://schemas.microsoft.com/ado/2007/08/dataservices/
    related/orders" type =
"application/atom+xml;type=feed" title =
    "orders" href = "Customer('IBM')/orders">
        <m:inline>
            <feed>
                <title type = "text">orders</title>
                <id>http://localhost:8080/wxsrestservice/restservice/
         NorthwindGrid/Customer('IBM')/orders</id>
                <updated>2009-12-16T22:50:18.156Z</updated>
                <link rel = "self" title = "orders" href = "Customer
          ('IBM')/orders"/>
                <entry>
                    <category term = "NorthwindGridModel.Order" scheme =
           "http://schemas.microsoft.com/ado/2007/08/
           dataservices/scheme"/>
                    <id>http://localhost:8080/wxsrestservice/restservice/
          NorthwindGrid/Order(orderId=5000,customer_customerId=
            'IBM')</id>
                    <title type = "text"/>
                    <updated>2009-12-16T22:50:18.156Z</updated>
                    <author>
                        <name/>
                    </author>
                    <link rel = "edit" title = "Order" href =
          "Order(orderId=5000,customer_customerId='IBM')"/>
                    <link rel = "http://schemas.microsoft.com/ado/2007/08/
          dataservices/related/customer" type = "application/
          atom+xml;type=entry" title ="customer" href =
          "Order(orderId=5000,customer_customerId='IBM')/customer"/>
                    <link rel = "http://schemas.microsoft.com/ado/2007/08/
          dataservices/related/orderDetails" type = "application/
           atom+xml;type=feed" title ="orderDetails" href =
           "Order(orderId=5000,customer_customerId='IBM')/orderDetails"/>
                    <content type="application/xml">
                        <m:properties>
                            <d:orderId m:type =
"Edm.Int32">5000</d:orderId>
                            <d:customer_customerId>IBM</d:customer_customerId>
                            <d:orderDate m:type =
"Edm.DateTime">
                2009-12-16T19:46:29.562</d:orderDate>
                            <d:shipCity>Rochester</d:shipCity>
                            <d:shipCountry m:null = "true"/>
                            <d:version m:type =
"Edm.Int32">0</d:version>
                        </m:properties>
                    </content>
                </entry>
                <entry>
                    <category term = "NorthwindGridModel.Order" scheme =
           "http://schemas.microsoft.com/ado/2007/08/
           dataservices/scheme"/>
                    <id>http://localhost:8080/wxsrestservice/restservice/
          NorthwindGrid/Order(orderId=5001,customer_customerId=
          'IBM')</id>
                    <title type = "text"/>
                    <updated>2009-12-16T22:50:18.156Z</updated>
```

```
                    <author>
                        <name/></author>
                    <link rel = "edit" title = "Order" href =
"Order(
orderId=5001,customer_customerId='IBM')"/>
                    <link rel = "http://schemas.microsoft.com/ado/2007/
           08/dataservices/related/customer" type =

"application/atom+xml;type=entry" title =
           "customer" href = "Order(orderId=5001,customer_customerId=
           'IBM')/customer"/>
                    <link rel = "http://schemas.microsoft.com/ado/2007/08/
            dataservices/related/orderDetails" type =
"application/atom+xml;type=feed" title =
            "orderDetails" href = "Order(orderId=5001,
            customer_customerId='IBM')/orderDetails"/>
                    <content type="application/xml">
                        <m:properties>
                            <d:orderId m:type = "Edm.Int32">5001</d:orderId>
                            <d:customer_customerId>IBM</d:customer_customerId>
                            <d:orderDate m:type = "Edm.DateTime">2009-12-16T19:
               50:11.125</d:orderDate>
                            <d:shipCity>Rochester</d:shipCity>
                            <d:shipCountry m:null = "true"/>
                            <d:version m:type =
"Edm.Int32">0</d:version>
                        </m:properties>
                    </content>
                </entry>
            </feed>
        </m:inline>
    </link>
    <content type="application/xml">
        <m:properties>
            <d:customerId>IBM</d:customerId>
            <d:city m:null = "true"/>
            <d:companyName>IBM Corporation</d:companyName>
            <d:contactName>John Doe</d:contactName>
            <d:country m:null = "true"/>
            <d:version m:type = "Edm.Int32">4</d:version>
        </m:properties>
    </content>
</entry>
```

- Código de Resposta: 200 OK

JSON

- Método: GET
- URI do Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')?$expand=orders
- Cabeçalho do Pedido: Aceitar: application/json
- Carga Útil de Pedido: Nenhuma
- Cabeçalho de Resposta: Conteúdo-Tipo: application/json
- Carga Útil de Resposta:

```
{"d":{"__metadata":{"uri":"http://localhost:8080/wxsrestservice/
   restservice/NorthwindGrid/Customer('IBM')",
 "type":"NorthwindGridModel.Customer"},
"customerId":"IBM",
"city":null,
"companyName":"IBM Corporation",
"contactName":"John Doe",
"country":null,
"version":4,
"orders":[{"__metadata":{"uri":"http://localhost:8080/
```

```
    wxsrestservice/restservice/NorthwindGrid/Order(
    orderId=5000,customer_customerId='IBM')",
"type":"NorthwindGridModel.Order"},
"orderId":5000,
"customer_customerId":"IBM",
"orderDate":"\/Date(1260992789562)\/",
"shipCity":"Rochester",
"shipCountry":null,
"version":0,
"customer":{"__deferred":{"uri":"http://localhost:8080/
   wxsrestservice/restservice/NorthwindGrid/Order(
   orderId=5000,customer_customerId='IBM')/customer"}},
"orderDetails":{"__deferred":{"uri":"http://localhost:
     8080/wxsrestservice/restservice/NorthwindGrid/
     Order(orderId=5000,customer_customerId='IBM')/
     orderDetails"}}},
{"__metadata":{"uri":"http://localhost:8080/wxsrestservice/
     restservice/NorthwindGrid/Order(orderId=5001,
     customer_customerId='IBM')","type":
     "NorthwindGridModel.Order"},
"orderId":5001,
"customer_customerId":"IBM",
"orderDate":"\/Date(1260993011125)\/",
"shipCity":"Rochester",
"shipCountry":null,
"version":0,
"customer":{"__deferred":{"uri":"http://localhost:8080/wxsrestservice/restservice/
NorthwindGrid/Order(orderId=5001,customer_customerId='IBM')/customer"}},
"orderDetails":{"__deferred":{"uri":"http://localhost:8080/
   wxsrestservice/restservice/NorthwindGrid/Order(
   orderId=5001, customer_customerId='IBM')/
   orderDetails"}}}]}}
```

- Código de Resposta: 200 OK

Conceitos relacionados:

Java "Operações com o Serviço de Dados REST" na página 518
Após iniciar o serviço de dados REST do eXtreme Scale, é possível usar qualquer cliente HTTP para interagir com ele. Um navegador da Web, um cliente PHP, um cliente Java ou um cliente WCF Data Services podem ser utilizados para emitir quaisquer operações de pedido suportadas.

Java "Visão Geral do Serviço de Dados REST" na página 327
O serviço de dados REST WebSphere eXtreme Scale é um serviço HTTP Java compatível com Microsoft WCF Data Services (formalmente, ADO.NET Data Services) e implementa o Open Data Protocol (OData). O Microsoft WCF Data Services é compatível com essa especificação quando utiliza Visual Studio 2008 SP1 e .NET Framework 3.5 SP1.

Tarefas relacionadas:

Java "Acessando Dados com o Serviço de Dados REST" na página 517
Desenvolva aplicativos que executam operações usando protocolos do serviço de dados REST.

Recuperando Não Entidades com Serviços de Dados REST: Java

O serviço de dados REST permite recuperar mais que apenas entidades, como coletas e propriedades das entidades.

Recuperar uma Coleta de Entidades

Um Pedido RetrieveEntitySet pode ser usado por um cliente para recuperar um conjunto de entidades do eXtreme Scale. As entidades são representadas como um

Atom Feed Document ou uma matriz JSON na carga útil da resposta. Para obter mais detalhes sobre o protocolo RetrieveEntitySet definido em Serviços de Dados WCF, consulte MSDN: Pedido RetrieveEntitySet.

O exemplo de pedido RetrieveEntitySet a seguir recupera todas as entidades Order associadas à entidade Customer('IBM'). Apenas os pedidos 5000 e 5001 são exibidos aqui.

AtomPub

- Método: GET
- URI de Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')/orders
- Cabeçalho do Pedido: Aceitar: application/atom+xml
- Carga Útil de Pedido: Nenhuma
- Cabeçalho de Resposta: Conteúdo-Tipo: application/atom+xml
- Carga Útil de Resposta:

```
<?xml version="1.0" encoding="utf-8"?>
<feed xml:base = "http://localhost:8080/wxsrestservice/restservice"
   xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices"
   xmlns:m = "http://schemas.microsoft.com/ado/2007/08/dataservices/
   metadata" xmlns = "http://www.w3.org/2005/Atom">
    <title type = "text">Order</title>
    <id>http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/
     Order</id>
    <updated>2009-12-16T22:53:09.062Z</updated>
    <link rel = "self" title = "Order" href = "Order"/>
    <entry>
        <category term = "NorthwindGridModel.Order"
scheme = "http://
      schemas.microsoft.com/
      ado/2007/08/dataservices/scheme"/>
        <id>http://localhost:8080/wxsrestservice/restservice/
      NorthwindGrid/Order(orderId=5000,customer_customerId=
      'IBM')</id>
        <title type = "text"/>
        <updated>2009-12-16T22:53:09.062Z</updated>
        <author>
            <name/>
        </author>
        <link rel = "edit" title = "Order" href =
"Order(orderId=5000,
      customer_customerId='IBM')"/>
        <link rel = "http://schemas.microsoft.com/ado/2007/08/
      dataservices/related/customer"
      type =
"application/atom+xml;type=entry"
      title = "customer" href = "Order(orderId=5000,
      customer_customerId='IBM')/customer"/>
        <link rel = "http://schemas.microsoft.com/ado/2007/08/
      dataservices/related/orderDetails"
      type =
"application/atom+xml;type=feed"
      title = "orderDetails" href = "Order(orderId=5000,customer_customerId='IBM')/
        orderDetails"/>
        <content type="application/xml">
            <m:properties>
                <d:orderId m:type = "Edm.Int32">5000</d:orderId>
                <d:customer_customerId>IBM</d:customer_customerId>
                <d:orderDate m:type = "Edm.DateTime">2009-12-16T19:
          46:29.562</d:orderDate>
                <d:shipCity>Rochester</d:shipCity>
                <d:shipCountry m:null = "true"/>
```

```
                <d:version m:type = "Edm.Int32">0</d:version>
            </m:properties>
        </content>
    </entry>
    <entry>
        <category term = "NorthwindGridModel.Order"
scheme = "http://
      schemas.microsoft.com/ado/2007/08/dataservices/scheme"/>
        <id>http://localhost:8080/wxsrestservice/restservice/
      NorthwindGrid/Order(orderId=5001, customer_customerId='IBM')
    </id>
        <title type = "text"/>
        <updated>2009-12-16T22:53:09.062Z</updated>
        <author>
            <name/>
        </author>
        <link rel = "edit" title = "Order" href = "Order(orderId=5001,
       customer_customerId='IBM')"/>
        <link rel = "http://schemas.microsoft.com/ado/2007/08/
       dataservices/related/customer"
       type =
"application/atom+xml;type=entry"
       title = "customer" href = "Order(orderId=5001,
         customer_customerId='IBM')/customer"/>
        <link rel = "http://schemas.microsoft.com/ado/2007/08/
         dataservices/related/orderDetails"
       type =
"application/atom+xml;type=feed"
       title = "orderDetails" href = "Order(orderId=5001,
         customer_customerId='IBM')/orderDetails"/>
        <content type="application/xml">
            <m:properties>
                <d:orderId m:type = "Edm.Int32">5001</d:orderId>
                <d:customer_customerId>IBM</d:customer_customerId>
                <d:orderDate m:type = "Edm.DateTime">2009-12-16T19:50:
          11.125</d:orderDate>
                <d:shipCity>Rochester</d:shipCity>
                <d:shipCountry m:null = "true"/>
                <d:version m:type = "Edm.Int32">0</d:version>
            </m:properties>
        </content>
    </entry>
</feed>
```

- Código de Resposta: 200 OK

JSON

- Método: GET
- URI de Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')/orders
- Cabeçalho do Pedido: Aceitar: application/json
- Carga Útil de Pedido: Nenhuma
- Cabeçalho de Resposta: Conteúdo-Tipo: application/json
- Carga Útil de Resposta:

```
{"d":[{"__metadata":{"uri":"http://localhost:8080/wxsrestservice/
   restservice/NorthwindGrid/Order(orderId=5000,
   customer_customerId='IBM')",
"type":"NorthwindGridModel.Order"},
"orderId":5000,
"customer_customerId":"IBM",
"orderDate":"\/Date(1260992789562)\/",
"shipCity":"Rochester",
"shipCountry":null,
"version":0,
```

```
"customer":{"__deferred":{"uri":"http://localhost:8080/
   wxsrestservice/restservice/NorthwindGrid/Order(orderId=
   5000,customer_customerId='IBM')/customer"}},
"orderDetails":{"__deferred":{"uri":"http://localhost:8080/
   wxsrestservice/restservice/NorthwindGrid/Order(orderId=
   5000,customer_customerId='IBM')/orderDetails"}}},
{"__metadata":{"uri":"http://localhost:8080/wxsrestservice/
     restservice/NorthwindGrid/
   Order(orderId=5001,
   customer_customerId='IBM')",
"type":"NorthwindGridModel.Order"},
"orderId":5001,
"customer_customerId":"IBM",
"orderDate":"\/Date(1260993011125)\/",
"shipCity":"Rochester",
"shipCountry":null,
"version":0,
"customer":{"__deferred":{"uri":"http://localhost:8080/
   wxsrestservice/restservice/NorthwindGrid/Order(orderId=
   5001,customer_customerId='IBM')/customer"}},
"orderDetails":{"__deferred":{"uri":"http://localhost:8080/
   wxsrestservice/restservice/NorthwindGrid/Order(orderId=
   5001,customer_customerId='IBM')/orderDetails"}}}]}
```

- Código de Resposta: 200 OK

Recuperar uma Propriedade

Um pedido RetrievePrimitiveProperty pode ser usado para obter o valor de uma propriedade de uma instância de entidade do eXtreme Scale. O valor da propriedade é representado como formato XML para pedidos AtomPub e objeto JSON para pedidos JSON na carga útil de resposta. Para obter mais detalhes sobre o pedido RetrievePrimitiveProperty, consulte MSDN: Pedido RetrievePrimitiveProperty.

O exemplo de pedido RetrievePrimitiveProperty a seguir recupera a propriedade contactName da entidade Customer('IBM').

AtomPub

- Método: GET
- URI do pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')/contactName
- Cabeçalho do Pedido: Aceitar: application/xml
- Carga Útil de Pedido: Nenhuma
- Cabeçalho de Resposta: Conteúdo-Tipo: application/atom+xml
- Carga Útil de Resposta:

```
<contactName
xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices">
    John Doe
</contactName>
```

- Código de Resposta: 200 OK

JSON

- Método: GET
- URI do pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')/contactName
- Cabeçalho do Pedido: Aceitar: application/json
- Carga Útil de Pedido: Nenhuma

- Cabeçalho de Resposta: Conteúdo-Tipo: application/json
- Carga Útil de Resposta: `{"d":{"contactName":"John Doe"}}`
- Código de Resposta: 200 OK

Recuperar um Valor da Propriedade

Um pedido RetrieveValue pode ser usado para obter o valor bruto de uma propriedade em uma instância de entidade do eXtreme Scale. O valor da propriedade é representado como um valor bruto na carga útil da resposta. Se o tipo de entidade for um dos seguintes, o tipo de mídia da resposta será “text/plain." Caso contrário, o tipo de mídia da resposta será “application/octet-stream." Esses tipos são:

- Tipos primitivos Java e seus respectivos wrappers
- java.lang.String
- byte[]
- Byte[]
- char[]
- Character[]
- enums
- java.math.BigInteger
- java.math.BigDecimal
- java.util.Date
- java.util.Calendar
- java.sql.Date
- java.sql.Time
- java.sql.Timestamp

Para obter mais detalhes sobre o pedido RetrieveValue, consulte MSDN: Pedido RetrieveValue.

O seguinte exemplo de pedido RetrieveValue recupera o valor bruto da propriedade contactName da entidade Customer('IBM').

- Método de Pedido: GET
- URI do Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')/contactName/$value
- Cabeçalho do Pedido: Aceitar: text/plain
- Carga Útil de Pedido: Nenhuma
- Cabeçalho da Resposta: Tipo de Conteúdo: text/plain
- Carga Útil da Resposta: John Doe
- Código de Resposta: 200 OK

Recuperar um Link

Um pedido RetrieveLink pode ser utilizado para obter o(s) link(s) representando uma associação para-um ou uma associação para-muitos. Para a associação to-one, o link é de uma instância de Entidade do eXtreme Scale para outra e o link é representado na carga útil da resposta. Para a associação to-many, os links são de uma instância de Entidade do eXtreme Scale para todas as outras em uma coleta de entidades do eXtreme Scale especificadas e a resposta é representada como um

conjunto de links na carga útil da resposta. Para obter mais detalhes sobre o pedido RetrieveLink, consulte MSDN: Pedido RetrieveLink.

Veja aqui um exemplo de pedido RetrieveLink. Neste exemplo, recuperamos a associação entre a entidade Order(orderId=5000,customer_customerId='IBM') e seu cliente. A resposta mostra o URI da entidade Customer.

AtomPub

- Método: GET
- URI do Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Order(orderId=5000,customer_customerId='IBM')/$links/customer
- Cabeçalho do Pedido: Aceitar: application/xml
- Carga Útil de Pedido: Nenhuma
- Cabeçalho da Resposta: Tipo de Conteúdo: application/xml
- Carga Útil de Resposta:

```
<?xml version="1.0" encoding="utf-8"?>
<uri>http://localhost:8080/wxsrestservice/restservice/
   NorthwindGrid/Customer('IBM')</uri>
```

- Código de Resposta: 200 OK

JSON

- Método: GET
- URI do Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Order(orderId=5000,customer_customerId='IBM')/$links/customer
- Cabeçalho do Pedido: Aceitar: application/json
- Carga Útil de Pedido: Nenhuma
- Cabeçalho de Resposta: Conteúdo-Tipo: application/json
- Carga Útil da Resposta: {"d":{"uri":"http:\/\/localhost:8080\/wxsrestservice\/restservice\/NorthwindGrid\/Customer('IBM')"}}

Recuperar Metadados do Serviço

Um Pedido RetrieveServiceMetadata pode ser usado para obter o documento Conceptual Schema Definition Language (CSDL), que descreve o modelo de dados associado ao serviço de dados REST do eXtreme Scale. Para obter mais detalhes sobre o pedido RetrieveServiceMetadata, consulte MSDN: Pedido RetrieveServiceMetadata.

Recuperar Documento de Serviço

Um Pedido RetrieveServiceDocument pode ser usado para recuperar o Documento de Serviço que descreve a coleta de recursos expostos pelo serviço de dados REST do eXtreme Scale. Para obter mais detalhes sobre o pedido RetrieveServiceDocument, consulte MSDN: Pedido RetrieveServiceDocument.

Conceitos relacionados:

Java "Operações com o Serviço de Dados REST" na página 518
Após iniciar o serviço de dados REST do eXtreme Scale, é possível usar qualquer cliente HTTP para interagir com ele. Um navegador da Web, um cliente PHP, um cliente Java ou um cliente WCF Data Services podem ser utilizados para emitir quaisquer operações de pedido suportadas.

Java "Visão Geral do Serviço de Dados REST" na página 327
O serviço de dados REST WebSphere eXtreme Scale é um serviço HTTP Java compatível com Microsoft WCF Data Services (formalmente, ADO.NET Data Services) e implementa o Open Data Protocol (OData). O Microsoft WCF Data Services é compatível com essa especificação quando utiliza Visual Studio 2008 SP1 e .NET Framework 3.5 SP1.

Tarefas relacionadas:

Java "Acessando Dados com o Serviço de Dados REST" na página 517
Desenvolva aplicativos que executam operações usando protocolos do serviço de dados REST.

Pedidos de Inserção com Serviço de Dados REST: Java

Um Pedido InsertEntity pode ser usado para inserir uma nova instância de entidade do eXtreme Scale, potencialmente com novas entidades relacionadas, no serviço de dados REST do eXtreme Scale.

Pedido Inserir Entidade

Um Pedido InsertEntity pode ser usado para inserir uma nova instância de entidade do eXtreme Scale, potencialmente com novas entidades relacionadas, no serviço de dados REST do eXtreme Scale. Ao inserir uma entidade, o cliente pode especificar se o recurso ou a entidade devem ser vinculados automaticamente a outras entidades existentes no serviço de dados.

O cliente deve incluir as informações sobre ligação necessárias na representação da relação associada na carga útil do pedido.

Além do suporte à inserção de uma nova instância EntityType (E1), o pedido InsertEntity também permite a inserção de novas entidades relacionadas à E1 (descritas por qualquer relação de entidade) em um único Pedido. Por exemplo, ao inserir um Customer('IBM'), podemos inserir todos os pedidos com Customer('IBM'). Esta forma de um Pedido InsertEntity também é conhecida como *inserção profunda*. Com uma inserção profunda, as entidades relacionadas devem ser representadas usando a representação sequencial da relação associada com E1 que identifica o link para as entidades relacionadas a serem inseridas.

As propriedades da entidade a ser inserida são especificadas na carga útil do pedido. As propriedades são analisadas pelo serviço de dados REST e configuradas para a propriedade correspondente na instância da entidade. Para o formato AtomPub, a propriedade é especificada como um elemento XML <d:PROPERTY_NAME>. Para JSON, a propriedade é especificada como uma propriedade de um objeto JSON.

Se uma propriedade estiver ausente na carga útil do pedido, o serviço de dados REST irá configurar o valor da propriedade da entidade para o valor padrão java. Entretanto, o banco de dados backend deve rejeitar um valor padrão, por exemplo,

se a coluna não for anulável no banco de dados. Um código de resposta 500 será retornado para indicar um erro do Servidor Interno.

Se houver propriedades duplicadas especificadas na carga útil, a última propriedade será utilizada. Todos os valores anteriores para o mesmo nome da propriedade serão ignorados pelo serviço de dados REST.

Se a carga útil contiver uma propriedade não existente, o serviço de dados REST retornará um código de resposta 400 (Pedido Inválido) para indicar que o pedido enviado pelo cliente estava sintaticamente incorreto.

Se as propriedades-chave estiverem ausentes, o serviço de dados REST retornará um código de resposta 400 (Pedido Inválido) para indicar uma propriedade-chave ausente.

Se a carga útil contiver um link para uma entidade relacionada com uma chave não existente, o serviço de dados REST retornará um código de resposta 404 (Não Localizado) para indicar que a entidade vinculada não pode ser localizada.

Se a carga útil contiver um link para uma entidade relacionada com um nome de associação incorreto, o serviço de dados REST retornará um código de resposta 400 (Pedido Inválido) para indicar que o link não pode ser localizado.

Se a carga útil contiver mais de um link para uma relação para-um, o último link será utilizado. Todos os links anteriores para a mesma associação serão ignorados.

Para obter mais detalhes sobre o pedido InsertEntity, consulte Biblioteca MSDN: Pedido InsertEntity.

Um pedido InsertEntity insere uma entidade Customer com a chave 'IBM'.

AtomPub

- Método: POST
- URI do pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')
- Cabeçalho do pedido: Aceitar: application/atom+xml Content-Type: application/atom+xml
- Carga Útil de Pedido:

```
<?xml version="1.0"
encoding="ISO-8859-1"?>
<entry
xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices"
 xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata"
 xmlns="http://www.w3.org/2005/Atom">
 <category term="NorthwindGridModel.Customer"
  scheme="http://schemas.microsoft.com/ado/2007/08/dataservices/scheme"
/>
<content type="application/xml">
  <m:properties>
   <d:customerId>Rational</d:customerId>
   <d:city>Rochester</d:city>
   <d:companyName>Rational</d:companyName>
   <d:contactName>John Doe</d:contactName>
   <d:country>USA</d:country>
  </m:properties>
 </content>
</entry>
```

- Cabeçalho de Resposta: Conteúdo-Tipo: application/atom+xml

- Carga Útil de Resposta:

```
<?xml version="1.0"
encoding="ISO-8859-1"?>
<entry
xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices"
 xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata"
 xmlns="http://www.w3.org/2005/Atom">
 <category term="NorthwindGridModel.Customer"
  scheme="http://schemas.microsoft.com/ado/2007/08/dataservices/scheme"
/>
<content type="application/xml">
  <m:properties>
   <d:customerId>Rational</d:customerId>
   <d:city>Rochester</d:city>
   <d:companyName>Rational</d:companyName>
   <d:contactName>John Doe</d:contactName>
   <d:country>USA</d:country>
  </m:properties>
 </content>
</entry>
Cabeçalho da Resposta:
Tipo de Conteúdo: application/atom+xml
Carga
Útil de Resposta:
<?xml version="1.0" encoding="utf-8"?>
<entry xml:base =
"http://localhost:8080/wxsrestservice/restservice" xmlns:d =
   "http://schemas.microsoft.com/ado/2007/08/dataservices" xmlns:m =
     "http://schemas.microsoft.com/
   ado/2007/08/dataservices/metadata" xmlns =
"http://www.w3.org/2005/Atom">
    <category term = "NorthwindGridModel.Customer" scheme =
"http://schemas.
     microsoft.com/ado/2007/08/dataservices/scheme"/>
    <id>http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/
     Customer('Rational')</id>
    <title type = "text"/>
    <updated>2009-12-16T23:25:50.875Z</updated>
    <author>
        <name/>
    </author>
    <link rel = "edit" title = "Customer" href =
"Customer('Rational')"/>
    <link rel =
"http://schemas.microsoft.com/ado/2007/08/dataservices/related/
    orders" type =
"application/atom+xml;type=feed"
    title = "orders" href = "Customer('Rational')/orders"/>
    <content type="application/xml">
        <m:properties>
            <d:customerId>Rational</d:customerId>
            <d:city>Rochester</d:city>
            <d:companyName>Rational</d:companyName>
            <d:contactName>John Doe</d:contactName>
            <d:country>USA</d:country>
            <d:version m:type = "Edm.Int32">0</d:version>
        </m:properties>
    </content>
</entry>
```

- Código de Resposta: 201 Criado

JSON

- Método: POST
- URI do Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer

- Cabeçalho do Pedido: Aceitar: application/json Content-Type: application/json
- Carga Útil de Pedido:

```
{"customerId":"Rational",
"city":null,
"companyName":"Rational",
"contactName":"John Doe",
"country": "USA",}
```

- Cabeçalho de Resposta: Conteúdo-Tipo: application/json
- Carga Útil de Resposta:

```
{"d":{"__metadata":{"uri":"http://localhost:8080/wxsrestservice/restservice/
   NorthwindGrid/Customer('Rational')",
"type":"NorthwindGridModel.Customer"},
"customerId":"Rational",
"city":null,
"companyName":"Rational",
"contactName":"John Doe",
"country":"USA",
"version":0,
"orders":{"__deferred":{"uri":"http://localhost:8080/wxsrestservice/restservice/
   NorthwindGrid/Customer('Rational')/orders"}}}}
```

- Código de Resposta: 201 Criado

Pedido Inserir Link

Um Pedido InsertLink pode ser usado para criar um novo Link entre duas instâncias de entidade do eXtreme Scale. A URI do pedido deve resolver para uma associação to-many do eXtreme Scale. A carga útil do pedido contém um único link que aponta para a entidade de destino da associação para-muitos.

Se o URI do pedido InsertLink representar uma associação para-um, o serviço de dados REST retornará uma resposta 400 (Pedido Inválido).

Se o URI do pedido InsertLink apontar para uma associação que não existe, o serviço de dados REST retornará uma resposta 404 (Não Localizado) para indicar que o link não foi localizado.

Se a carga útil contiver um link com uma chave que não existe, o serviço de dados REST retornará uma resposta 404 (Não Localizado) para indicar que a entidade vinculada não pode ser localizada.

Se a carga útil contiver mais de um link, o Serviço de Dados REST do eXtreme Scale analisará o primeiro link. Os links restantes serão ignorados.

Para obter mais detalhes sobre o pedido InsertLink, consulte: Biblioteca MSDN: Pedido InsertLink.

O seguinte exemplo de pedido InsertLink cria um link de Customer('IBM') para Order(orderId=5000,customer_customerId='IBM').

AtomPub

- Método: POST
- URI do Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')/$link/orders
- Cabeçalho do Pedido: Tipo de Conteúdo: application/xml
- Carga Útil de Pedido:

```
<?xml version="1.0"
encoding="ISO-8859-1"?>
<uri>http://host:1000/wxsrestservice/restservice/NorthwindGrid/Order(orderId=
   5000,customer_customerId='IBM')</uri>
```

- Carga Útil de Resposta: Nenhuma
- Código de Resposta: 204 Nenhum Conteúdo

JSON

- Método: POST
- URI do Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')/$links/orders
- Cabeçalho do Pedido: Tipo de Conteúdo: application/json
- Carga Útil de Pedido:

```
{"uri":
"http://host:1000/wxsrestservice/restservice/NorthwindGrid/Order(orderId
    =5000,customer_customerId='IBM')"}
```

- Carga Útil de Resposta: Nenhuma
- Código de Resposta: 204 Nenhum Conteúdo

Conceitos relacionados:

Java "Operações com o Serviço de Dados REST" na página 518
Após iniciar o serviço de dados REST do eXtreme Scale, é possível usar qualquer cliente HTTP para interagir com ele. Um navegador da Web, um cliente PHP, um cliente Java ou um cliente WCF Data Services podem ser utilizados para emitir quaisquer operações de pedido suportadas.

Java "Visão Geral do Serviço de Dados REST" na página 327
O serviço de dados REST WebSphere eXtreme Scale é um serviço HTTP Java compatível com Microsoft WCF Data Services (formalmente, ADO.NET Data Services) e implementa o Open Data Protocol (OData). O Microsoft WCF Data Services é compatível com essa especificação quando utiliza Visual Studio 2008 SP1 e .NET Framework 3.5 SP1.

Tarefas relacionadas:

Java "Acessando Dados com o Serviço de Dados REST" na página 517
Desenvolva aplicativos que executam operações usando protocolos do serviço de dados REST.

Pedidos de Atualização com Serviço de Dados REST: Java

O serviço de dados REST do WebSphere eXtreme Scale suporta pedidos de atualização para entidades, propriedades de primitivas de entidades e assim por diante.

Atualizar uma Entidade

Um Pedido UpdateEntity pode ser usado para atualizar uma entidade existente do eXtreme Scale. O cliente pode usar um método HTTP PUT para substituir ume entidade existente do eXtreme Scale ou usar um método HTTP MERGE para mesclar as mudanças em uma entidade existente do eXtreme Scale.

Nota: 8.6+ Os métodos upsert e upsertAll substituem os métodos put e putAll do ObjectMap. Use o método upsert para informar ao BackingMap e carregador que uma entrada na grade de dados precisa colocar a chave e o valor na grade. O BackingMap e carregador executam uma inserção ou uma atualização

para colocar o valor na grade e no carregador. Se você executar a API upsert dentro de seus aplicativos, o carregador obterá um tipo UPSERT de LogElement, que permite que carregadores façam a mesclagem do banco de dados ou chamadas upsert em vez de usar insert ou update.

Ao atualizar a entidade, o cliente pode especificar se a entidade, além de ser atualizada, deve ser vinculada automaticamente a outras entidades existentes no serviço de dados que estão relacionadas por meio de associações com valor único.

A propriedade da entidade a ser atualizada está na carga útil do pedido. A propriedade é analisada pelo serviço de dados REST e configurada para a propriedade correspondente na entidade. Para o formato AtomPub, a propriedade é especificada como um elemento XML <d:PROPERTY_NAME>. Para JSON, a propriedade é especificada como uma propriedade de um objeto JSON.

Se uma propriedade estiver ausente na carga útil de solicitação, o serviço de dados REST configurará o valor de propriedade da entidade com o valor padrão Java para o método HTTP PUT. Entretanto, o banco de dados backend deve rejeitar um valor padrão, por exemplo, se a coluna não for anulável no banco de dados. Então, um código de resposta 500 (Erro do Servidor Interno) é retornado para indicar um Erro do Servidor Interno. Se uma propriedade estiver ausente na carga útil de solicitação HTTP MERGE, o serviço de dados REST não alterará o valor da propriedade existente.

Se houver propriedades duplicadas especificadas na carga útil, a última propriedade será usada. Todos os valores anteriores com o mesmo nome da propriedade serão ignorados pelo serviço de dados REST.

Se a carga útil contiver uma propriedade não existente, o serviço de dados REST irá retornar um código de resposta 400 (Pedido Inválido) para indicar que o pedido enviado pelo cliente estava sintaticamente incorreto.

Como parte da serialização de um recurso, se a carga útil de um pedido de Atualização contiver alguma das propriedades-chave para a entidade, o serviço de dados REST irá ignorar esses valores de chave já que as chaves de entidades são imutáveis.

Para obter detalhes sobre o pedido UpdateEntity, consulte: Biblioteca MSDN: Pedido UpdateEntity.

Um pedido UpdateEntity atualiza o nome da cidade de Customer('IBM') para 'Raleigh'.

AtomPub

- Método: PUT
- URI do pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')
- Cabeçalho do Pedido: Tipo de Conteúdo: application/atom+xml
- Carga Útil de Pedido:

```
<?xml version="1.0"
encoding="ISO-8859-1"?>
<entry
xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices"
 xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata"
 xmlns="http://www.w3.org/2005/Atom">
 <category term="NorthwindGridModel.Customer"
```

```
  scheme="http://schemas.microsoft.com/ado/2007/08/dataservices/scheme"
/>
 <title/>
 <updated>2009-07-28T21:17:50.609Z</updated>
 <author>
  <name />
 </author>
 <id />
 <content type="application/xml">
  <m:properties>
   <d:customerId>IBM</d:customerId>
   <d:city>Raleigh</d:city>
   <d:companyName>IBM Corporation</d:companyName>
   <d:contactName>Big Blue</d:contactName>
   <d:country>USA</d:country>
  </m:properties>
 </content>
</entry>
```

- Carga Útil de Resposta: Nenhuma
- Código de Resposta: 204 Nenhum Conteúdo

JSON

- Método: PUT
- URI do pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')
- Cabeçalho do Pedido: Tipo de Conteúdo: application/json
- Carga Útil de Pedido:

```
{"customerId":"IBM",
"city":"Raleigh",
"companyName":"IBM Corporation",
"contactName":"Big Blue",
"country": "USA",}
```

- Carga Útil de Resposta: Nenhuma
- Código de Resposta: 204 Nenhum Conteúdo

Atualizar uma Propriedade Primitiva da Entidade

O Pedido UpdatePrimitiveProperty pode atualizar um valor da propriedade de uma entidade do eXtreme Scale. A propriedade e o valor a serem atualizados estão na carga útil do pedido. A propriedade não pode ser uma propriedade-chave uma vez que o eXtreme Scale não permite que os clientes alterem as chaves de entidades.

Para obter mais detalhes sobre o pedido UpdatePrimitiveProperty, consulte: Biblioteca MSDN: Pedido UpdatePrimitiveProperty.

Veja aqui um exemplo de pedido UpdatePrimitiveProperty. Neste exemplo, atualizamos o nome da cidade de Customer('IBM') para 'Raleigh'.

AtomPub

- Método: PUT
- URI do Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')/city
- Cabeçalho do Pedido: Tipo de Conteúdo: application/xml
- Carga Útil de Pedido:

```
<?xml version="1.0"
encoding="ISO-8859-1"?>
<city
xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices">
 Raleigh
</city>
```

- Carga Útil de Resposta: Nenhuma
- Código de Resposta: 204 Nenhum Conteúdo

JSON

- Método: PUT
- URI do Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')/city
- Cabeçalho do Pedido: Tipo de Conteúdo: application/json
- Carga Útil do Pedido: {"city":"Raleigh"}
- Carga Útil de Resposta: Nenhuma
- Código de Resposta: 204 Nenhum Conteúdo

Atualizar um Valor de Propriedade Primitiva da Entidade

O Pedido UpdateValue pode atualizar um valor bruto da propriedade de uma entidade do eXtreme Scale. O valor a ser atualizado é representado como um valor bruto na carga útil do pedido. A propriedade não pode ser uma propriedade-chave uma vez que o eXtreme Scale não permite que os clientes alterem as chaves de entidades.

O tipo de conteúdo do pedido pode ser “text/plain” ou “application/octet-stream”, dependendo do tipo de propriedade. Para obter informações adicionais, consulte “Recuperando Não Entidades com Serviços de Dados REST” na página 531.

Para obter mais detalhes sobre o pedido UpdateValue, consulte: Biblioteca MSDN: Pedido UpdateValue

Veja aqui um exemplo do pedido UpdateValue. Neste exemplo, atualize o nome da cidade de Customer('IBM') para 'Raleigh'.

- Método: PUT
- URI do Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')/city/$value
- Cabeçalho do Pedido: Tipo de Conteúdo: text/plain
- Carga Útil de Pedido: Raleigh
- Carga Útil de Resposta: Nenhuma
- Código de Resposta: 204 Nenhum Conteúdo

Atualizar um Link

O pedido UpdateLink pode ser usado para estabelecer uma associação entre duas instâncias de entidade do eXtreme Scale. A associação pode ser uma relação com valor único (para um) ou uma relação com diversos valores (para muitos).

A atualização de um link entre duas instâncias de entidade do eXtreme Scale pode estabelecer associações ou remover associações. Por exemplo, se o cliente estabelecer uma associação "para um" entre uma entidade

`Order(orderId=5000,customer_customerId='IBM')` e a instância `Customer('ALFKI')`, ele precisará dessociar a entidade `Order(orderId=5000,customer_customerId='IBM')` e a entidade de sua instância Customer associada atualmente.

Se as instâncias de entidade especificadas no pedido UpdateLink não puderem ser localizadas, o serviço de dados REST retornará uma resposta 404 (Não Localizado).

Se o URI do pedido UpdateLink especificar uma associação não existente, o serviço de dados REST retornará uma resposta 404 (Não Localizado) para indicar que o link não pode ser localizado.

Se a URI especificada na carga útil do pedido UpdateLink não resolver para a mesma entidade ou a mesma chave conforme especificado na URI, se existir, o Serviço de Dados REST do eXtreme Scale retornará uma resposta 400 (Pedido Inválido).

Se a carga útil de solicitação de UpdateLink contiver diversos links, o serviço de dados REST analisará somente o primeiro link. O restante dos links será ignorado.

Para obter mais detalhes sobre o pedido UpdateLink, consulte: Biblioteca MSDN: Pedido UpdateLink.

Veja aqui um exemplo de pedido UpdateLink. Neste exemplo, atualizamos a relação do cliente da entidade `Order(orderId=5000,customer_customerId='IBM')` e de Customer('IBM') para Customer('IBM').

Lembre-se: O exemplo anterior é apenas ilustrativo. Como todas as associações normalmente são associações chave para uma grade particionada, o link não poderá ser alterado.

AtomPub

- Método: PUT
- URI de Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Order(101)/$links/customer
- Cabeçalho do Pedido: Tipo de Conteúdo: application/xml
- Carga Útil de Pedido:

```
<?xml version="1.0"
encoding="ISO-8859-1"?>
<uri>
 http://host:1000/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')
</uri>
```

- Carga Útil de Resposta: Nenhuma
- Código de Resposta: 204 Nenhum Conteúdo

JSON

- Método: PUT
- URI da Solicitação: `http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Order(orderId=5000,customer_customerId='IBM')/$links/customer`
- Cabeçalho do Pedido: Tipo de Conteúdo: application/xml
- Carga Útil da Solicitação: `{"uri": "http://host:1000/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')"}`
- Carga Útil de Resposta: Nenhuma

- Código de Resposta: 204 Nenhum Conteúdo

Conceitos relacionados:

Java "Operações com o Serviço de Dados REST" na página 518
Após iniciar o serviço de dados REST do eXtreme Scale, é possível usar qualquer cliente HTTP para interagir com ele. Um navegador da Web, um cliente PHP, um cliente Java ou um cliente WCF Data Services podem ser utilizados para emitir quaisquer operações de pedido suportadas.

Java "Visão Geral do Serviço de Dados REST" na página 327
O serviço de dados REST WebSphere eXtreme Scale é um serviço HTTP Java compatível com Microsoft WCF Data Services (formalmente, ADO.NET Data Services) e implementa o Open Data Protocol (OData). O Microsoft WCF Data Services é compatível com essa especificação quando utiliza Visual Studio 2008 SP1 e .NET Framework 3.5 SP1.

Tarefas relacionadas:

Java "Acessando Dados com o Serviço de Dados REST" na página 517
Desenvolva aplicativos que executam operações usando protocolos do serviço de dados REST.

Pedidos de Exclusão com Serviços de Dados REST: Java

O serviço de dados REST do WebSphere eXtreme Scale pode excluir entidades, valores da propriedade e links.

Excluir uma Entidade

O Pedido DeleteEntity pode excluir uma entidade do eXtreme Scale do serviço de dados REST.

Se alguma relação com a entidade a ser excluída tiver a exclusão em cascata configurada, o serviço de dados REST do eXtreme Scale excluirá a entidade ou entidades relacionadas. Para obter mais detalhes sobre o pedido DeleteEntity, consulte Biblioteca MSDN: Pedido DeleteEntity.

O pedido DeleteEntity a seguir exclui o cliente com a chave 'IBM'.

- Método: DELETE
- URI do pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')
- Carga Útil de Pedido: Nenhuma
- Carga Útil de Resposta: Nenhuma
- Código de Resposta: 204 Nenhum Conteúdo

Excluir um Valor da Propriedade

O Pedido DeleteValue configura uma propriedade de entidade do eXtreme Scale para nula.

Qualquer propriedade de uma entidade do eXtreme Scale pode ser configurada para nula com um pedido DeleteValue. Para configurar uma propriedade como nula, certifique-se do seguinte:

- Para qualquer tipo de número de primitiva e seu wrapper, BigInteger ou BigDecimal, o valor da propriedade será configurado como 0.

- Para o tipo Boolean ou boolean, o valor da propriedade será configurado como false.
- Para o tipo char ou Character, o valor da propriedade será configurado como character #X1 (NIL).
- Para o tipo enum, o valor da propriedade será configurado para o valor numérico com ordinal 0.
- Para todos os outros tipos, o valor da propriedade será configurado como nulo.

Entretanto, um pedido de exclusão pode ser rejeitado pelo banco de dados backend se, por exemplo, a propriedade não for anulável no banco de dados. Nesse caso, o serviço de dados REST retorna uma resposta 500 (Erro do Servidor Interno). Para obter mais detalhes sobre o pedido DeleteValue, consulte: Biblioteca MSDN: Pedido DeleteValue.

Aqui está um exemplo de pedido DeleteValue. Neste exemplo, configuramos o nome do contato de Customer('IBM') como nulo.

- Método: DELETE
- URI do pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Customer('IBM')/contactName
- Carga Útil de Pedido: Nenhuma
- Carga Útil de Resposta: Nenhuma
- Código de Resposta: 204 Nenhum Conteúdo

Excluir um Link

O pedido DeleteLink pode remover uma associação entre duas instâncias de entidade do eXtreme Scale. A associação pode ser uma relação para-um ou uma relação para-muitos. Entretanto, um pedido de exclusão pode ser rejeitado pelo banco de dados backend se, por exemplo, a restrição de chave estrangeira estiver configurada. Nesse caso, o serviço de dados REST retorna uma resposta 500 (Erro do Servidor Interno). Para obter mais detalhes sobre o pedido DeleteLink, consulte: Biblioteca MSDN: Pedido DeleteLink.

O pedido DeleteLink a seguir remove a associação entre Order(101) e seu Customer associado.

- Método: DELETE
- URI de Pedido: http://localhost:8080/wxsrestservice/restservice/NorthwindGrid/Order(101)/$links/customer
- Carga Útil de Pedido: Nenhuma
- Carga Útil de Resposta: Nenhuma
- Código de Resposta: 204 Nenhum Conteúdo

Conceitos relacionados:

Java "Operações com o Serviço de Dados REST" na página 518
Após iniciar o serviço de dados REST do eXtreme Scale, é possível usar qualquer cliente HTTP para interagir com ele. Um navegador da Web, um cliente PHP, um cliente Java ou um cliente WCF Data Services podem ser utilizados para emitir quaisquer operações de pedido suportadas.

Java "Visão Geral do Serviço de Dados REST" na página 327
O serviço de dados REST WebSphere eXtreme Scale é um serviço HTTP Java compatível com Microsoft WCF Data Services (formalmente, ADO.NET Data Services) e implementa o Open Data Protocol (OData). O Microsoft WCF Data Services é compatível com essa especificação quando utiliza Visual Studio 2008 SP1 e .NET Framework 3.5 SP1.

Tarefas relacionadas:

Java "Acessando Dados com o Serviço de Dados REST" na página 517
Desenvolva aplicativos que executam operações usando protocolos do serviço de dados REST.

APIs e Plug-ins do Sistema

Java

Um plug-in é um componente que fornece uma função aos componentes conectáveis que incluem ObjectGrid e BackingMap. Para usar de maneira mais eficiente o eXtreme Scale como um espaço de processamento de grade de dados ou de banco de dados de memória, é necessário determinar cuidadosamente a melhor maneira de maximizar o desempenho com os plug-ins disponíveis.

Gerenciando Ciclos de Vida de Plug-in

Java

É possível gerenciar ciclos de vida de plug-in com métodos especializados de cada plug-in, que estão disponíveis para serem chamados em pontos funcionais designados. Ambos os métodos initialize e destroy definem o ciclo de vida de plug-ins, que são controlados pelos seus objetos *proprietário*. Um objeto proprietário é o objeto que realmente usa o plug-in fornecido. Um proprietário pode ser um cliente de grade, um servidor ou um mapa de apoio.

Sobre Esta Tarefa

Da mesma forma, todos os plug-ins podem implementar interfaces combinadas opcionais adequadas para seu objeto proprietário. Qualquer plug-in ObjectGrid pode implementar o ObjectGridPlugin de interface combinada opcional. Qualquer plug-in BackingMap pode implementar o BackingMapPlugin de interface combinada opcional. As interfaces combinadas opcionais requerem a implementação de vários métodos adicionais além dos métodos initialize() e destroy() para os plug-ins básicos. Para obter mais informações sobre essas interfaces, consulte a documentação da API.

Quando os objetos proprietários estão inicializando, esses objetos configuram atributos no plug-in e, em seguida, chamam o método initialize dos plug-ins proprietários. Durante o ciclo de destruição dos objetos proprietários, o método destroy dos plug-ins também será chamado consequentemente. Para obter detalhes sobre os métodos initialize e destroy específicos, junto com outros métodos aptos para cada plug-in, consulte os tópicos relevantes para cada plug-in.

Como exemplo, considere um ambiente distribuído. Ambos os ObjectGrids do lado do cliente e do lado do servidor podem ter seus próprios plug-ins. O ciclo de vida de um ObjectGrid do lado do cliente e, portanto, suas instâncias de plug-in são independentes de todas as instâncias ObjectGrids e de plug-in do lado do servidor.

Nessa topologia distribuída, suponha que você tenha um ObjectGrid denominado `myGrid` definida no arquivo `objectGrid.xml` e configurado com um ObjectGridEventListener customizado chamado myObjectGridEventListener. O arquivo `objectGridDeployment.xml` define a política de implementação para o ObjectGrid `myGrid`. Ambos os arquivos `objectGrid.xml` e `objectGridDeployment.xml` são usados para iniciar servidores de contêiner. Durante a inicialização do servidor de contêiner, a instância do ObjectGrid `myGrid` do lado do servidor é inicializada. Enquanto isso, o método initialize da instância myObjectGridEventListener de propriedade da instância myObjectGrid é chamada. Depois que o servidor de contêiner for iniciado, o aplicativo poderá se conectar à instância ObjectGrid `myGrid` do lado do servidor e obter uma instância do lado do cliente.

Ao obter a instância myGrid do ObjectGrid do lado do cliente, a instância `myGrid` do lado do cliente passa pelo seu próprio ciclo de inicialização e chama o método initialize da sua própria instância myObjectGridEventListener do lado do cliente. Essa instância myObjectGridEventListener do lado do cliente é independente da instância myObjectGridEventListener do lado do servidor. O ciclo de vida é controlado pelo proprietário, que é a instância `myGrid` do ObjectGrid do lado do cliente.

Se o aplicativo desconectar ou destruir a instância `myGrid` do ObjectGrip do lado do cliente, o método destroy que pertence à instância myObjectGridEventListener do lado do cliente será chamado automaticamente. No entanto, esse processo não afeta a instância myObjectGridEventListener no lado do servidor. O método destroy da instância myObjectGridEventListener do lado do servidor pode ser chamado apenas durante o ciclo de vida de destruição da instância `myGrid` do ObjectGrid do lado do servidor ao parar um servidor de contêiner. Especificamente, ao parar um servidor de contêiner, as instâncias ObjectGrid contidas são destruídas e o método destroy de todos os plug-ins proprietários é chamado.

Embora o exemplo anterior seja aplicado especificamente para o caso de uma instância do cliente e do servidor de um ObjectGrid, o proprietário de um plug-in também pode ser uma interface BackingMap. Além disso, tenha cuidado ao determinar suas configurações para os plug-ins que você pode gravar, com base nessas considerações do ciclo de vida. Use os tópicos a seguir para gravar os plug-ins que fornecem eventos de gerenciamento de ciclo de vida estendido que podem ser usados para configurar ou remover recursos em seu ambiente:

Conceitos relacionados:

"Visão Geral da Estrutura do OSGi" na página 162
O OSGi define um sistema módulo dinâmico para Java. A plataforma de serviço OSGi possui uma arquitetura em camadas e é projetada para ser executada em vários perfis padrão Java. É possível iniciar servidores e clientes do WebSphere eXtreme Scale em um contêiner OSGi.

Informações relacionadas:

Documentação da API

Gravando um Plug-in do ObjectGridPlugin: Java

Um ObjectGridPlugin é uma interface combinada opcional que pode ser usada para fornecer eventos de gerenciamento de ciclo de vida estendidos para todos os outros plug-ins do ObjectGrid.

Sobre Esta Tarefa

Qualquer plug-in do ObjectGrid que implementa o ObjectGridPlugin recebe o conjunto de eventos de ciclo de vida estendido que, além de fornecer mais controle, pode ser usado para configurar ou remover os recursos. Em um contêiner para uma grade de dados particionados, haverá uma instância de ObjectGrid (o proprietário de plugin) para cada partição gerenciada pelo contêiner.Quando partições individuais são removidas, os recursos usados por essa instância de ObjectGrid também devem ser removidos. Portanto, pode ser necessário fechar ou finalizar um recurso, como um arquivo de configuração aberto ou um encadeamento em execução gerenciado por um plug-in, quando a partição proprietária para esse recurso for removida.

A interface ObjectGridPlugin fornece métodos para configurar ou modificar o estado do plug-in, além de métodos para examinar o estado atual do plug-in. Todos os métodos devem ser implementados corretamente e o ambiente de tempo de execução do WebSphere eXtreme Scale verifica o comportamento do método sob determinadas circunstâncias. Por exemplo, depois de chamar o método initialize(), o ambiente de tempo de execução do eXtreme Scale chama o método isInitialized() para assegurar que o método concluiu com êxito a inicialização apropriada.

Procedimento

1. Implemente a interface ObjectGridPlugin para que o plug-in ObjectGridPlugin receba notificações sobre eventos significativos do eXtreme Scale. Há três categorias principais de métodos a seguir:

Métodos de propriedades	Propósito
setObjectGrid()	Chamado para configurar a instância do ObjectGrid usada pelo plug-in.
getObjectGrid()	Chamado para confirmar a instância do ObjectGrid usada pelo plug-in.

Métodos de inicialização	Propósito
initialize()	Chamado para inicializar o ObjectGridPlugin.
isInitialized()	Chamado para obter ou confirmar o status de inicialização do plug-in.

Métodos de destruição	Propósito
destroy()	Chamado para destruir o ObjectGridPlugin.
isDestroyed()	Chamado para obter ou confirme o status destruído do plug-in.

   Consulte a Documentação da API para obter mais informações sobre essas interfaces.
2. Configure um Plug-in ObjectGridPlugin com o XML. Use a classe com.company.org.MyObjectGridPluginTxCallback, que implementa a interface TransactionCallback e a interface ObjectGridPlugin.

   No exemplo de código a seguir, o retorno de chamada de transação customizada, que receberá definitivamente os eventos de ciclo de vida estendidos, é gerado e incluído em um ObjectGrid.

   Importante: A interface TransactionCallback já possui um método initialize, e um novo método de initialize é incluído bem como o método destroy e outros

métodos do ObjectGridPlugin. Cada método é utilizado e os métodos initialize executam apenas uma inicialização por vez. O XML a seguir cria uma configuração que usa a interface TransactionCallback aprimorada.

O texto a seguir deve estar no arquivo `myGrid.xml`:

```
?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="myGrid">
            <bean id="TransactionCallback"
                  className="com.company.org.MyObjectGridPluginTxCallback" />
            <backingMap name="Book"/>
        </objectGrid>
    </objectGrids>
</objectGridConfig>
```

Observe que as declarações de bean aparecem antes das declarações de `backingMap`.

3. Forneça o arquivo `myGrid.xml` para o plug-in ObjectGridManager a fim de facilitar a criação desta configuração.

Tarefas relacionadas:

"Gravando um Plug-in BackingMapPlugin"
Um plug-in BackingMap implementa a interface combinada do BackingMapPlugin,que pode ser usada para receber os recursos estendidos para gerenciar seu ciclo de vida.

Informações relacionadas:

../com.ibm.websphere.extremescale.javadoc.doc/topics/com/ibm/websphere/objectgrid/management/package-summary.html

Gravando um Plug-in BackingMapPlugin: Java

Um plug-in BackingMap implementa a interface combinada do BackingMapPlugin,que pode ser usada para receber os recursos estendidos para gerenciar seu ciclo de vida.

Sobre Esta Tarefa

Qualquer plug-in BackingMap existente que também implementar a interface BackingMapPlugin receberá automaticamente o conjunto estendido de eventos de ciclo de vida durante a construção e uso.

A interface BackingMapPlugin fornece métodos para configurar ou modificar o estado do plug-in, bem como métodos para examinar o estado atual do plug-in.

Todos os métodos devem ser implementados corretamente e o ambiente de tempo de execução do WebSphere eXtreme Scale verifica o comportamento do método sob determinadas circunstâncias. Por exemplo, depois de chamar o método initialize(), o ambiente de tempo de execução do eXtreme Scale chama o método isInitialized() para assegurar que o método concluiu com êxito a inicialização apropriada.

Procedimento

1. Implemente a interface BackingMapPlugin para que o plug-in BackingMapPlugin receba notificações sobre eventos significativos do eXtreme Scale. Há três categorias principais de métodos a seguir:

Métodos de propriedades	Propósito
setBackingMap()	Chamado para configurar a instância do BackingMap usada pelo plug-in.
getBackingMap()	Chamado para obter ou confirmar a instância do BackingMap usada pelo plug-in.

Métodos de inicialização	Propósito
initialize()	Chamado para inicializar o plug-in BackingMapPlugin.
isInitialized()	Chamado para obter ou confirmar o status de inicialização do plug-in.

Métodos de destruição	Propósito
destroy()	Chamado para destruir o plug-in BackingMapPlugin.
isDestroyed()	Chamado para obter ou confirme o status destruído do plug-in.

Consulte a Documentação da API para obter mais informações sobre essas interfaces.

2. Configurar um Plug-in BackingMapPlugin com XML Suponha que o nome da classe de um plug-in Loader do eXtreme Scale seja a classe com.company.org.MyBackingMapPluginLoader, que implementa a interface Loader e a interface BackingMapPlugin.

   No exemplo de código a seguir, o retorno de chamada de transação customizada, que definitivamente receberá eventos do ciclo de vida estendido, é gerado e incluído em um BackingMap.

   Também é possível configurar um plug-in BackingMapPlugin usando XML. O texto a seguir deve estar no arquivo `myGrid.xml`:

```
<?xml version="1.0" encoding="UTF-8" ?>
<objectGridconfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
        xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="myGrid">
            <backingMap name="Book" pluginCollectionRef="myPlugins" />
        </objectGrid>
    </objectGrids>
    <backingMapPluginCollections>
        <backingMapPluginCollection id="myPlugins">
            <bean id="Loader"
                  className="com.company.org.MyBackingMapPluginLoader" />
        </backingMapPluginCollection>
    </backingMapPluginCollections>
</objectGridConfig>
```

3. Forneça o arquivo `myGrid.xml` para o plug-in ObjectGridManager para facilitar a criação desta configuração.

Resultados

A instância BackingMap criada tem um Loader que recebe eventos de ciclo de vida do BackingMapPlugin.

Tarefas relacionadas:

"Gravando um Plug-in do ObjectGridPlugin" na página 549
Um ObjectGridPlugin é uma interface combinada opcional que pode ser usada para fornecer eventos de gerenciamento de ciclo de vida estendidos para todos os outros plug-ins do ObjectGrid.

Informações relacionadas:

../com.ibm.websphere.extremescale.javadoc.doc/topics/com/ibm/websphere/objectgrid/management/package-summary.html

Plug-ins para Replicação Multimestre

Java

Considere a possibilidade de transformar objetos armazenados em cache para aumentar o desempenho do seu cache. É possível usar o plug-in ObjectTransformer quando seu uso do processador estiver alto. Até 60-70 por cento do tempo total do processador é gasto serializando e copiando entradas. Ao implementar o plug-in ObjectTransformer, é possível serializar e desserializar objetos com sua própria implementação. É possível usar um plug-in CollisionArbiter para definir como as colisões de mudanças são tratadas em seus domínios.

Desenvolvendo Árbitros Customizados para a Replicação Multimestre: Java

Poderão ocorrer colisões de mudanças se os mesmos registros puderem ser alterados simultaneamente em dois locais. Em uma topologia de replicação multimestre, os domínios do serviço de catálogo detectam colisões automaticamente. Quando um domínio de serviço de catálogo detecta uma colisão, ele chama um árbitro. Geralmente, as colisões são resolvidas com o árbitro de colisão padrão. No entanto, um aplicativo pode fornecer um árbitro de colisão customizado.

Antes de Iniciar

- Consulte "Planejando Diversas Topologias do Datacenter" na página 283 para obter mais informações sobre como planejar e projetar a topologia de replicação multimestre.
- Consulte Configurando Diversas Topologias do Datacenter para obter mais informações sobre como configurar links entre os domínios de serviço de catálogo.

Sobre Esta Tarefa

Se um domínio de serviço de catálogos receber uma entrada replicada que colide com um registro de colisão, o árbitro padrão usará as mudanças do domínio de serviço de catálogo nomeado mais baixo de maneira lexical. Por exemplo, se os domínios A e B gerarem um conflito para um registro, a mudança do domínio B será ignorada. O domínio A mantém sua versão e o registro no domínio B é alterado para que corresponda ao registro do domínio A. Os nomes de domínio são convertidos em maiúsculas para comparação.

Uma alternativa é a topologia de replicação multimestre chamar um plug-in de colisão customizado para decidir o resultado. Essas instruções esboçam como desenvolver um árbitro de colisão customizado e configurar uma topologia de replicação multimestre para usá-lo.

Procedimento

1. Desenvolva um árbitro de colisão customizado e integre-o em seu aplicativo.

   A classe deve implementar a interface:

   `com.ibm.websphere.objectgrid.revision.CollisionArbiter`

   Um plug-in de colisão tem três opções para decidir o resultado de uma colisão. Ele pode escolher a cópia local ou a cópia remota ou pode fornecer uma versão revisada da entrada. Um domínio de serviço de catálogo fornece as seguintes informações para um árbitro de colisão customizado:

   - A versão existente do registro
   - A versão da colisão do registro
   - Um Objeto de sessão que deve ser usado para criar a versão revisada da entrada colidida

   O método de plug-in retorna um objeto que indica sua decisão. O método chamado pelo domínio para chamar o plug-in deve retornar verdadeiro ou falso, em que falso significa ignorar a colisão. Quando a colisão é ignorada, a versão local permanece inalterada e o árbitro esquece que já ter visto a versão existente. O método retornará um valor real se tiver usado a sessão fornecida para criar uma versão nova, mesclada do registro, reconciliando a mudança.

2. No arquivo `objectgrid.xml`, especifique o plug-in do árbitro customizado.

   O ID deve ser `CollisionArbiter`.

```
<dgc:objectGrid name="revisionGrid" txTimeout="10">
     <dgc:bean className="com.you.your_application.
      CustomArbiter" id="CollisionArbiter">
      <dgc:property name="property" type="java.lang.String"
      value="propertyValue"/>
     </dgc:bean>
</dgc:objectGrid>
```

Conceitos relacionados:

"Planejando Diversas Topologias do Datacenter" na página 283
Ao usar a replicação assíncrona multimestre, duas ou mais grades de dados podem se tornar cópias exatas de uns dos outros. Cada grade de dados é hospedada em um domínio do serviço de catálogo independente, com seu próprio serviço de catálogo, servidores de contêiner e um nome exclusivo. Com a replicação assíncrona multimestre, é possível usar links para conectar uma coleção de domínios do serviço de catálogo. Os domínios do serviço de catálogo são então sincronizados usando a replicação sobre os links. É possível construir quase qualquer topologia por meio da definição de links entre os domínios de serviço de catálogo.

"Topologias para Replicação Multimaster" na página 283
Você tem várias opções diferentes ao escolher a topologia para sua implementação que incorpora replicação multimaster.

"Considerações de Configuração para Topologias Multimestre" na página 288
Considere os seguintes problemas ao decidir se e como usar as topologias de replicação multimestre.

"Considerações de Design para Replicação Multimestre" na página 292
Ao implementar da replicação multimestre, você deve considerar aspectos de design, como arbitragem, vinculação e desempenho.

"Considerações Sobre o Carregador em uma Topologia Multimestre" na página 289
Quando estiver usando os carregadores em uma topologia multimestre, você deve considerar a possibilidade de colisão e desafios de manutenção das informações de revisão. A grade de dados mantém as informações de revisão sobre os itens nela para que colisões possam ser detectadas quando outros shards primários na configuração gravarem entradas na grade de dados. Quando as entradas são incluídas a partir de um carregador, essas informações de revisão não são incluídas e a entrada assume uma nova revisão. Como a revisão da entrada parece ser uma nova inserção, uma colisão false poderá ocorrer se outro shard primário também alterar esse estado ou obtiver as mesmas informações a partir de um carregador.

Plug-ins para Versão e Comparação de Objetos de Cache

Java

Use o plug-in OptimisticCallback para customizar as operações de versão e de comparação de objetos do cache ao usar a estratégia de bloqueio otimista.

É possível fornecer um objeto de retorno de chamada otimista conectável que implementa a interface com.ibm.websphere.objectgrid.plugins.OptimisticCallback. Para mapas de entidade, um plug-in OptimisticCallback de alto desempenho é automaticamente configurado.

Propósito

Utilize a interface OptimisticCallback para fornecer operações de comparação otimistas para os valores de um mapa. Uma implementação OptimisticCallback é necessária ao utilizar a estratégia de bloqueio otimista. O produto fornece uma implementação de OptimisticCallback padrão. No entanto, geralmente o aplicativo deve conectar sua própria implementação da interface OptimisticCallback.

Implementação Padrão

A estrutura do eXtreme Scale fornece uma implementação padrão da interface OptimisticCallback que é usada se o aplicativo não for conectado a um objeto OptimisticCallback fornecido pelo aplicativo. A implementação padrão sempre

retorna o valor especial de NULL_OPTIMISTIC_VERSION como o objeto de versão para o valor e nunca atualiza o objeto de versão. Esta ação faz uma comparação otimista de uma função "no operation". Na maioria dos casos, você não deseja que a função "no operation" ocorra, quando estiver utilizando a estratégia de bloqueio otimista. Seus aplicativos devem implementar a interface OptimisticCallback e conectar suas próprias implementações de OptimisticCallback para que a implementação padrão não seja utilizada. No entanto, existe pelo menos um cenário no qual a implementação de OptimisticCallback fornecida padrão é útil. Considere a seguinte situação:

- Um utilitário de carga é conectado para o mapa de suporte.
- O utilitário de carga sabe como desempenhar a comparação otimista sem assistência de um plug-in OptimisticCallback.

Como o utilitário de carga pode executar a versão otimista sem assistência de um objeto OptimisticCallback? O utilitário de carga conhece o objeto de classe de valor e sabe qual campo de objeto de valor é utilizado como um valor de versão otimista. Por exemplo, suponha que a seguinte interface seja utilizada para o objeto de valor para o mapa employees:

```
public interface Employee
{
    // Sequential sequence number used for optimistic versioning.
    public long getSequenceNumber();
    public void setSequenceNumber(long newSequenceNumber);
    // Other get/set methods for other fields of Employee object.
}
```

Neste exemplo, o utilitário de carga sabe que pode utilizar o método getSequenceNumber para obter as informações de versão atuais para um objeto de valor Employee. O utilitário de carga incrementa o valor retornado para gerar um novo número de versão antes de atualizar o armazenamento persistente com o novo valor Employee. Para um utilitário de carga Java Database Connectivity (JDBC), o número de sequência atual na cláusula WHERE de uma instrução UPDATE SQL superqualificada é usado e ele usa o novo número de sequência gerado para configurar a coluna do número de sequência para o novo valor de número de sequência. Outra possibilidade é que o utilitário de carga faça uso de alguma função fornecida por backend que atualiza automaticamente uma coluna oculta que pode ser utilizada para versões otimistas.

Em alguns casos, um procedimento armazenado ou acionador possivelmente pode ser utilizado para ajudar a manter uma coluna que contém as informações de controle de versões. Se o utilitário de carga estiver utilizando uma destas técnicas para a manutenção de informações de versões otimistas, então, o aplicativo não precisa fornecer uma implementação do OptimisticCallback. A implementação OptimisticCallback padrão pode ser utilizada neste cenário porque o utilitário de carga consegue identificar versões otimistas sem nenhuma assistência de um objeto OptimisticCallback.

Implementação Padrão para Entidades

As entidades são armazenadas no ObjectGrid utilizando objetos de tupla. A implementação OptimisticCallback padrão se comporta da mesma maneira que se comporta com mapas de não-entidade. Entretanto, o campo de versão na entidade é identificado utilizando a anotação @Version ou o atributo version no arquivo XML descritor da entidade.

O atributo version pode ser de um dos seguintes tipos: int, Integer, short, Short, long, Long ou java.sql.Timestamp. Uma entidade deve ter apenas um atributo

version definido. O atributo version deve ser configurado apenas durante a construção. Depois de a entidade ser persistida, o valor do atributo de versão não deve ser modificado.

Se um atributo version não estiver configurado e a estratégia de bloqueio otimista for utilizada, então, a tupla inteira será implicitamente versionada utilizando o estado inteiro da tupla, o que é mais custoso

No exemplo a seguir, a entidade Employee possui um atributo de versão longa denominado SequenceNumber:

```
@Entity
public class Employee {
private long sequence;
    // Sequential sequence number used for optimistic versioning.
    @Version
    public long getSequenceNumber() {
        return sequence;
    }
    public void setSequenceNumber(long newSequenceNumber) {
        this.sequence = newSequenceNumber;
    }
    // Other get/set methods for other fields of Employee object.
}
```

Gravando um Plug-in OptimisticCallback

Um plug-in OptimisticCallback precisa implementar a interface OptimisticCallback e seguir as convenções comuns do plug-in ObjectGrid. Consulte a Interface OptimisticCallback para obter mais informações.

A lista a seguir fornece uma descrição ou consideração para cada um dos métodos na interface OptimisticCallback:

NULL_OPTIMISTIC_VERSION

Este valor especial será retornado pelo método getVersionedObjectForValue se a implementação OptimisticCallback não requerer uma verificação de versão. A implementação de plug-in integrada da classe com.ibm.websphere.objectgrid.plugins.builtins.NoVersioningOptimisticCallback usa esse valor porque a versão é desativada ao especificar essa implementação de plug-in.

Método getVersionedObjectForValue

O método getVersionedObjectForValue pode retornar uma cópia do valor ou um atributo do valor que pode ser utilizado para fins de versão. Este método é chamado sempre que um objeto é associado a uma transação. Quando nenhum Utilitário de Carga estiver conectado a um mapa de suporte, o mapa de suporte utilizará este valor no tempo de confirmação para desempenhar uma comparação de versão otimista. A comparação de versão otimista é utilizada pelo mapa de apoio para assegurar que a versão não tenha sido alterada depois que a primeira transação acessou pela primeira vez a entrada do mapa que foi modificada por esta transação. Se outra transação já tiver modificado a versão desta entrada do mapa, a comparação de versão falhará e o mapa de apoio exibirá uma exceção OptimisticCollisionException para forçar o retrocesso da transação. Se um Utilitário de Carga estiver conectado, o mapa de suporte não utilizará as informações de controle de versões otimista. Em vez disso, o Utilitário de Carga é responsável por desempenhar a comparação de controle de versões otimista e por atualizar as

informações de controle de versões quando necessário. O Utilitário de Carga geralmente obtém o objeto de versão inicial do LogElement transmitido para o método batchUpdate no utilitário de carga, que é chamado quando ocorre uma operação de limpeza ou quando uma transação é confirmada.

O código a seguir mostra a implementação utilizada pelo objeto EmployeeOptimisticCallbackImpl:

```
public Object getVersionedObjectForValue(Object value)
{
    if (value == null)
    {
        return null;
    }
    else
    {
        Employee emp = (Employee) value;
        return new Long( emp.getSequenceNumber() );
    }
}
```

Conforme demonstrado no exemplo anterior, o atributo sequenceNumber é retornado em um objeto java.lang.Long conforme esperado pelo Utilitário de Carga, que significa que a mesma pessoa que gravou o Utilitário de Carga gravou a implementação de EmployeeOptimisticCallbackImpl ou trabalhou junto com a pessoa que implementou o EmployeeOptimisticCallbackImpl - por exemplo, concordou com o valor retornado pelo método getVersionedObjectForValue. O plug-in OptimisticCallback padrão retorna o valor especial NULL_OPTIMISTIC_VERSION como o objeto de versão.

Método updateVersionedObjectForValue

Este método é chamado sempre que uma transação tiver atualizado um valor e um novo objeto de versão for requerido. Se o método getVersionedObjectForValue retornar um atributo do valor, este método geralmente atualizará o valor de atributo com um novo objeto de versão. Se o método getVersionedObjectForValue retornar uma cópia do valor, este método normalmente não executa nenhuma ação. O plug-in OptimisticCallback padrão não executa nenhuma ação com esse método pois a implementação padrão de getVersionedObjectForValue sempre retorna o valor especial NULL_OPTIMISTIC_VERSION como o objeto de versão. O seguinte exemplo mostra a implementação usada pelo objeto EmployeeOptimisticCallbackImpl que é usado na seção OptimisticCallback:

```
public void updateVersionedObjectForValue(Object value)
{
    if ( value != null )
    {
        Employee emp = (Employee) value;
        long next = emp.getSequenceNumber() + 1;
        emp.updateSequenceNumber( next );
    }
}
```

Conforme demonstrado no exemplo anterior, o atributo sequenceNumber é incrementado em um para que na próxima vez em que o método getVersionedObjectForValue for chamado, o valor java.lang.Long retornado tenha um valor longo que é o valor do número de sequência original mais um, por exemplo, é o próximo valor de versão para esta instância employee. Este exemplo significa que a pessoa que gravou o Utilitário de Carga gravou o EmployeeOptimisticCallbackImpl ou trabalhou junto com a pessoa que implementou o EmployeeOptimisticCallbackImpl.

Método serializeVersionedValue

Este método grava o valor com versão no fluxo especificado. Dependendo da implementação, o valor com versão pode ser utilizado para identificar colisões de atualização otimistas. Em algumas implementações, o valor com versão é uma cópia do valor original. Outras implementações podem ter um número de sequência ou algum outro objeto para indicar a versão do valor. Como a implementação real é desconhecida, este método é fornecido para executar a serialização apropriada. A implementação padrão faz uma chamada writeObject.

Método inflateVersionedValue

Este método utiliza a versão serializada do valor com versão e retorna o objeto de valor com versão real. Dependendo da implementação, o valor com versão pode ser utilizado para identificar colisões de atualização otimistas. Em algumas implementações, o valor com versão é uma cópia do valor original. Outras implementações podem ter um número de sequência ou algum outro objeto para indicar a versão do valor. Como a implementação real é desconhecida, este método é fornecido para executar a desserialização apropriada. A implementação padrão chama o método readObject.

Utilizando o Objeto OptimisticCallback Fornecido pelo Aplicativo

Há duas abordagens para incluir um objeto OptimisticCallback fornecido pelo aplicativo na configuração de BackingMap: configuração programática e configuração XML.

Conectar Programaticamente um Objeto OptimisticCallback

O exemplo a seguir demonstra como um aplicativo pode conectar programaticamente um objeto OptimisticCallback para o mapa de apoio de funcionários na instância grid1 do ObjectGrid local:

```
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
import com.ibm.websphere.objectgrid.ObjectGridManager;
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.BackingMap;
ObjectGridManager ogManager = ObjectGridManagerFactory.getObjectGridManager();
ObjectGrid og = ogManager.createObjectGrid( "grid1" );
BackingMap bm = dg.defineMap("employees");
EmployeeOptimisticCallbackImpl cb = new EmployeeOptimisticCallbackImpl();
bm.setOptimisticCallback( cb );
```

Abordagem de configuração XML para conectar um objeto OptimisticCallback

O aplicativo pode utilizar um arquivo XML para conectar seu objeto OptimisticCallback, conforme mostrado no seguinte exemplo:

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">
<objectGrids>
    <objectGrid name="grid1">
        <backingMap name="employees" pluginCollectionRef="employees" lockStrategy="OPTIMISTIC" />
    </objectGrid>
</objectGrids>

<backingMapPluginCollections>
    <backingMapPluginCollection id="employees">
        <bean id="OptimisticCallback" className="com.xyz.EmployeeOptimisticCallbackImpl" />
    </backingMapPluginCollection>
</backingMapPluginCollections>
</objectGridConfig>
```

Plug-ins para Serializar Objetos em Cache

Java

O WebSphere eXtreme Scale usa diversos processos Java serializar os dados, ao converter as instâncias de objeto Java em bytes e em objetos novamente, conforme necessário, para mover os dados entre processos do cliente e do servidor.

Para serializar dados no eXtreme Scale, é possível usar a serialização Java, o plug-in ObjectTransformer ou os plug-ins DataSerializer.

 A interface ObjectTransformer foi substituída pelos plug-ins DataSerializer, que podem ser usados para armazenar dados arbitrários com eficiência no WebSphere eXtreme Scale para que as APIs do produto existentes possam interagir eficientemente com seus dados.

Conceitos relacionados:

Visão Geral da Serialização
Os dados são sempre expressos, porém não necessariamente armazenados, como objetos Java na grade de dados. O WebSphere eXtreme Scale usa diversos processos Java para serializar os dados, ao converter as instâncias de objetos Java em bytes e retornar para os objetos novamente, conforme necessário, para mover os dados entre os processos do cliente e do servidor.

Visão Geral da Programação do Serialziador: Java

É possível usar os plug-ins do DataSerializer para gravar serializadores otimizados para armazenar objetos Java e outros dados no formato binário na grade. O plug-in também fornece métodos que você pode usar para atributos de consulta dentro dos dados binários sem exigir que o objeto de dados inteiro seja expandido.

Os plug-ins DataSerializer incluem três plug-ins principais e várias interfaces combinadas opcionais. O plug-in MapSerializerPlugin inclui metadados sobre o relacionamento entre um mapa e outros mapas. Ele também inclui uma referência a um KeySerializerPlugin e um ValueSerializerPlugin. Os plug-ins do serializador de chave e valor incluem metadados e código de serialização responsável pela interação com os respectivos dados de chave e valor para um mapa. Um plug-in MapSerializerPlugin deve incluir um ou ambos os serializadores de chave e valor.

O plug-in KeySerializerPlugin fornece métodos e metadados para serializar, aumentar e examinar as chaves. O plug-in ValueSerializer fornece métodos e metadados para serializar, aumentar e examinar valores. Ambas as interfaces possuem requisitos diferentes. Para obter detalhes sobre quais métodos estão disponíveis nos plug-inss DataSerializer, consulte a documentação da API para o pacote com.ibm.websphere.objectgrid.plugins.io.

Plug-in MapSerializerPlugin

O MapSerializerPlugin é o ponto de plug-in principal para a interface BackingMap e inclui dois plug-ins aninhados: os plug-ins KeySerializerPlugin e ValueSerializerPlugin. Como o eXtreme Scale não suporta plug-ins aninhados ou conectados, o plug-in BasicMapSerializerPlugin acessa estes plug-ins aninhados artificialmente. Quando você usa esses plug-ins com a estrutura do OSGi, o único proxy é o plug-in MapSerializerPlugin. Todos os plug-ins aninhados não devem ser armazenados em cache em outros plug-ins dependentes, como os carregadores, a menos que esses plug-ins também atendam aos eventos do

ciclo de vida do BackingMap. Isto é importante ao executar em uma estrutura do OSGi, porque as referências com esses plug-ins podem continuar sendo atualizadas.

Plug-in KeySerializerPlugin
O plug-in KeySerializerPlugin estende a interface DataSerializer e inclui outras interfaces e metadados combinados que descrevem a chave. Use este plug-in para serializar e aumentar os objetos de dados e atributos de chave.

Plug-in ValueSerializerPlugin
O plug-in ValueSerializerPlugin estende a interface DataSerializer, porém não expõe nenhum método adicional. Use este plug-in para serializar e aumentar objetos de dados e atributos de valor.

Interfaces Opcionais e Combinadas

As interfaces opcionais e combinadas fornecem capacidades adicionais, como:

Versão otimista
A interface Provida de Versões permite que o plug-in ValueSerializerPlugin manipule a verificação de versão e as atualizações de versão ao usar bloqueio otimista. Se a Versão não estiver implementada e o bloqueio otimista estiver ativado, a versão será o formulário serializado inteiro do valor de objeto de dados.

Roteamento não baseado em hashCode
A interface Particionável permite que as implementações de KeySerializerPlugin roteiem solicitações para partições explícitas. Isso é equivalente à interface PartitionableKey, quando usado com a API do ObjectMap sem KeySerializerPlugin. Sem esse recurso, a chave é roteada para a partição com base no hashCode resultante.

Interface UserReadable (toString)
A interface UserReadable (toString) permite que todas as implementações de DataSerializer forneçam um método alternativa para exibir dados em arquivos de log e depuradores. Com esse recurso, é possível ocultar dados sensíveis, como senhas. Se implementações de DataSerializer não implementarem esta interface, o ambiente de tempo de execução poderá chamar toString() diretamente no objeto ou incluir representações alternativas, se apropriado.

Suporte à evolução
A interface Mesclável pode ser implementada em implementações de plug-in ValueSerializerPlugin para permitir a interoperabilidade entre diversas versões de objetos quando houver versões diferentes do DataSerializer atualizando dados na grade durante seu tempo de vida. Os métodos Mergeable permitem que o plug-in DataSerializer retenha quaisquer dados que ele não possa entender de outra forma.

Tarefas relacionadas:

Java "Evitando Aumento de Objeto ao Atualizar e Recuperar os Dados em Cache"
É possível usar os plug-ins DataSerializer para ignorar o aumento de objetos automático e recuperar manualmente os atributos dos dados que já foram serializados. É possível também usar o DataSerializer para inserir e atualizar dados em seu formulário serializado. Esse uso pode ser útil quando apenas parte dos dados precisa ser acessada ou quando os dados precisam ser transmitidos entre os sistemas.

Java "Programando para Usar a Estrutura do OSGi" na página 654
Os servidores e clientes do eXtreme Scale podem ser iniciados em um contêiner OSGi para poder incluir e atualizar dinamicamente plug-ins do eXtreme Scale no ambiente de tempo de execução.

Informações relacionadas:

Java Documentação da API do DataSerializer

Evitando Aumento de Objeto ao Atualizar e Recuperar os Dados em Cache:

Java

É possível usar os plug-ins DataSerializer para ignorar o aumento de objetos automático e recuperar manualmente os atributos dos dados que já foram serializados. É possível também usar o DataSerializer para inserir e atualizar dados em seu formulário serializado. Esse uso pode ser útil quando apenas parte dos dados precisa ser acessada ou quando os dados precisam ser transmitidos entre os sistemas.

Sobre Esta Tarefa

Esta tarefa usa o modo de cópia COPY_TO_BYTES_RAW com os plug-ins MapSerializerPlugin e ValueSerializerPlugin. O MapSerializer é o ponto de plug-in principal para a interface BackingMap. Dois plug-ins aninhados são incluídos, o KeyDataSerializer e o ValueDataSerializer. Como o produto não suporta plug-ins aninhados, o plug-in BaseMapSerializer suporta artificialmente estes plug-ins aninhados ou ligados. Portanto, quando usar essas APIs no contêiner OSGi, o MapSerializer será o único proxy. Todos os plug-ins aninhados não devem ser armazenados em cache dentro de outros plug-ins dependentes, como um carregador, a menos que ele também atenda aos eventos de ciclo de vida do BackingMap, de modo que suas referências de suporte possam ser atualizadas.

Quando COPY_TO_BYTES_RAW é configurado, todos os métodos ObjectMap retornam objetos SerializedValue, permitindo que o usuário recupere o formulário serializado ou o formulário do objeto Java do valor.

Ao usar um plug-in KeySerializerPlugin, todos os métodos que retornam chaves, como os plug-ins MapIndexPlugin ou Loader retornam objetos SerializedKey.

Quando os dados já estiverem no formulário serializado, os dados são inseridos com o uso dos mesmos objetos SerializedKey e SerializedValue. Quando os dados estiverem no formato byte[], os factories DataObjectKeyFactory e DataObjectValueFactory serão usados para criar a chave apropriada ou um wrapper de valor. Os factories estão disponíveis no DataObjectContext, que podem ser acessados a partir do SerializerAccessor para o BackingMap ou a partir da implementação do DataSerializer.

O exemplo neste tópico demonstra como concluir as ações a seguir:

Procedimento

1. Usar os plug-ins DataSerializer para serializar e aumentar os objetos de dados.
2. Recuperar valores serializados.
3. Recuperar atributos individuais a partir de um valor serializado.
4. Inserir chaves e valores pré-serializados.

Exemplo

Use este exemplo para atualizar e recuperar os dados em cache:

```
import java.io.IOException;
import com.ibm.websphere.objectgrid.CopyMode;
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.ObjectGridException;
import com.ibm.websphere.objectgrid.ObjectMap;
import com.ibm.websphere.objectgrid.Session;
import com.ibm.websphere.objectgrid.io.XsDataOutputStream;
import com.ibm.websphere.objectgrid.plugins.io.SerializerAccessor;
import com.ibm.websphere.objectgrid.plugins.io.ValueSerializerPlugin;
import com.ibm.websphere.objectgrid.plugins.io.dataobject.DataObjectContext;
import com.ibm.websphere.objectgrid.plugins.io.dataobject.SerializedKey;
import com.ibm.websphere.objectgrid.plugins.io.dataobject.SerializedValue;

    /**
     * Use the DataSerializer to serialize an Order key.
     */
    public byte[] serializeOrderKey(ObjectGrid grid, String key)
            throws IOException {
        SerializerAccessor sa = grid.getMap("Order").getSerializerAccessor();
        DataObjectContext dftObjCtx = sa.getDefaultContext();
        XsDataOutputStream out = dftObjCtx.getDataStreamManager()
                .createOutputStream();
        sa.getMapSerializerPlugin().getKeySerializerPlugin()
                .serializeDataObject(sa.getDefaultContext(), key, out);
        return out.toByteArray();
    }

    /**
     * Use the DataSerializer to serialize an Order value.
     */
    public byte[] serializeOrderValue(ObjectGrid grid, Order value)
            throws IOException {
        SerializerAccessor sa = grid.getMap("Order").getSerializerAccessor();
        DataObjectContext dftObjCtx = sa.getDefaultContext();
        XsDataOutputStream out = dftObjCtx.getDataStreamManager()
                .createOutputStream();
        sa.getMapSerializerPlugin().getValueSerializerPlugin()
                .serializeDataObject(sa.getDefaultContext(), value, out);
        return out.toByteArray();
    }

    /**
     * Retrieve a single Order in serialized form.
     */
    public byte[] fetchOrderRAWBytes(Session session, String key)
            throws ObjectGridException {
        ObjectMap map = session.getMap("Order");

        // Override the CopyMode to retrieve the serialized form of the value.
        // This process affects all API methods from this point on for the life
        // of the Session.
        map.setCopyMode(CopyMode.COPY_TO_BYTES_RAW, null);
        SerializedValue serValue = (SerializedValue) map.get(key);

        if (serValue == null)
            return null;

        // Retrieve the byte array and return it to the caller.
        return serValue.getInputStream().toByteArray();
    }

    /**
     * Retrieve one or more attributes from the Order without inflating the
     * Order object.
     */
    public Object[] fetchOrderAttribute(Session session, String key,
            String... attributes) throws ObjectGridException, IOException {
        ObjectMap map = session.getMap("Order");

        // Override the CopyMode to retrieve the serialized form of the value.
        // This process affects all API methods from this point on for the life
```

```
        // of the Session.
        map.setCopyMode(CopyMode.COPY_TO_BYTES_RAW, null);
        SerializedValue serValue = (SerializedValue) map.get(key);

        if (serValue == null)
            return null;

        // Retrieve a single attribute from the byte buffer.
        ValueSerializerPlugin valSer = session.getObjectGrid()
                .getMap(map.getName()).getSerializerAccessor()
                .getMapSerializerPlugin().getValueSerializerPlugin();
        Object attrCtx = valSer.getAttributeContexts(attributes);
        return valSer.inflateDataObjectAttributes(serValue.getContext(),
                serValue.getInputStream(), attrCtx);
    }

    /**
     * Inserts a pre-serialized key and value into the Order map.
     */
    public void insertRAWOrder(Session session, byte[] key, byte[] value)
            throws ObjectGridException {
        ObjectMap map = session.getMap("Order");

        // Get a referece to the default DataObjectContext for the map.
        DataObjectContext dftDtaObjCtx = session.getObjectGrid()
                .getMap(map.getName()).getSerializerAccessor()
                .getDefaultContext();

        // Wrap the key and value in a SerializedKey and SerializedValue
        // wrapper.
        SerializedKey serKey = dftDtaObjCtx.getKeyFactory().createKey(key);
        SerializedValue serValue = dftDtaObjCtx.getValueFactory().createValue(
                value);

        // Insert the serialized form of the key and value.
        map.insert(serKey, serValue);
    }
}
```

Conceitos relacionados:

Java "Visão Geral da Programação do Serialziador" na página 560
É possível usar os plug-ins do DataSerializer para gravar serializadores otimizados para armazenar objetos Java e outros dados no formato binário na grade. O plug-in também fornece métodos que você pode usar para atributos de consulta dentro dos dados binários sem exigir que o objeto de dados inteiro seja expandido.

Java Visão Geral da Serialização
Os dados são sempre expressos, porém não necessariamente armazenados, como objetos Java na grade de dados. O WebSphere eXtreme Scale usa diversos processos Java para serializar os dados, ao converter as instâncias de objetos Java em bytes e retornar para os objetos novamente, conforme necessário, para mover os dados entre os processos do cliente e do servidor.

Java Amostras

Informações relacionadas:

Java Documentação da API do DataSerializer

Plug-in ObjectTransformer: Java

Com o plug-in ObjectTransformer, é possível serializar, desserializar e copiar objetos no cache para aumentar o desempenho.

A interface ObjectTransformer foi substituída pelos plug-ins DataSerializer, que podem ser usados para armazenar dados arbitrários eficientemente no WebSphere eXtreme Scale para que as APIs do produto existentes possam ser interagir de modo eficiente com seus dados.

Se você tiver problemas de desempenho com o uso do processador, inclua um plug-in ObjectTransformer em cada mapa. Se um plug-in ObjectTransformer não for fornecido, o processador gastará de 60 a 70% de seu tempo total só serializando e copiando entradas.

Propósito

O plug-in ObjectTransformer permite que os aplicativos forneçam métodos customizados para as seguintes operações:

- Serializar ou desserializar a chave para uma entrada
- Serializar ou desserializar o valor para uma entrada
- Copiar uma chave ou valor para uma entrada

Se nenhum plug-in ObjectTransformer for fornecido, será necessário serializar as chaves e valores, porque o ObjectGrid utiliza a sequência serializar e desserializar para copiar os objetos. Este método é caro, portanto, utilize um plug-in ObjectTransformer quando o desempenho for importante. A cópia ocorre quando um aplicativo consulta um objeto em uma transação pela primeira vez. É possível evitar essa cópia configurando o modo de cópia como COPY_ON_READ ou reduzir a cópia configurando o modo de cópia como COPY_ON_READ. Otimize a operação de cópia quando requerido pelo aplicativo, fornecendo um método de cópia customizado neste plug-in. Esse plug-in pode reduzir a sobrecarga de cópia de 65 a 70% para 2 a 3% do tempo total do processador.

As implementações dos métodos padrão copyKey e copyValue primeiro tentam utilizar o método clone, se este for fornecido. Se nenhuma implementação do método clone for fornecida, a implementação será padronizada como serialização.

A serialização do objeto também é utilizada diretamente quando o eXtreme Scale estiver em execução no modo distribuído. LogSequence utiliza o plug-in ObjectTransformer para ajudá-lo a serializar chaves e valores antes de transmitir as alterações para os equivalentes no ObjectGrid. Cuidado ao fornecer um método de serialização customizado em vez de utilizar a serialização do Java developer kit integrada. O controle de versões do objeto é um assunto complexo e é possível encontrar problemas com a compatibilidade de versões se você não assegurar que seus métodos customizados foram projetados para controle de versões.

A lista a seguir descreve como o eXtreme Scale tenta serializar chaves e valores:

- Se um plug-in ObjectTransformer customizado for gravado e conectado, o eXtreme Scale chamará os métodos nos métodos na interface ObjectTransformer para serializar chaves e valores e obter cópias de chaves e valores do objeto.
- Se um plug-in ObjectTransformer customizado não for usado, o eXtreme Scale serializa e desserializa os valores de acordo com o padrão. Se o plug-in padrão for utilizado, cada objeto será implementado como externalizável ou implementado como serializável.
  - Se o objeto suportar a interface Externalizável, o método writeExternal será chamado. Os objetos que são implementados como externalizáveis geram melhor desempenho.
  - Se o objeto não suportar a interface Externalizável e implementar a interface Serializável, o objeto será salvo usando o método ObjectOutputStream.

Utilizando a Interface ObjectTransformer

Um objeto ObjectTransformer precisa implementar a interface ObjectTransformer e seguir as convenções comuns do plug-in ObjectGrid.

Duas abordagens, configuração programática e configuração XML, são utilizadas para incluir um objeto ObjectTransformer na configuração BackingMap da seguinte forma.

Conectando um Objeto ObjectTransformer Programaticamente

O fragmento de código a seguir cria o objeto ObjectTransformer customizado e o inclui em um BackingMap:

```
ObjectGridManager objectGridManager = ObjectGridManagerFactory.getObjectGridManager();
ObjectGrid myGrid = objectGridManager.createObjectGrid("myGrid", false);
BackingMap backingMap = myGrid.getMap("myMap");
MyObjectTransformer myObjectTransformer = new MyObjectTransformer();
backingMap.setObjectTransformer(myObjectTransformer);
```

Abordagem de Configuração XML para Conectar um ObjectTransformer

Suponha que o nome da classe da implementação ObjectTransformer seja a classe com.company.org.MyObjectTransformer. Essa classe implementa a interface ObjectTransformer. Uma implementação ObjectTransformer pode ser configurada usando o seguinte XML:

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
    xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="myGrid">
     <backingMap name="myMap" pluginCollectionRef="myMap" />
        </objectGrid>
    </objectGrids>

    <backingMapPluginCollections>
 <backingMapPluginCollection id="myMap">
      <bean id="ObjectTransformer" className="com.company.org.MyObjectTransformer" />
 </backingMapPluginCollection>
    </backingMapPluginCollections>
</objectGridConfig>
```

Cenários de Uso do ObjectTransformer

É possível utilizar o plug-in ObjectTransformer nas seguintes situações:

- Objeto não-serializável
- Objeto serializável mas aprimorando o desempenho da serialização
- Cópia de chave ou valor

No exemplo a seguir, o ObjectGrid é utilizado para armazenar a classe Stock:

```
/**
* Objeto Stock para demo do ObjectGrid
*
*
*/
public class Stock implements Cloneable {
    String ticket;
    double price;
    String company;
    String description;
    int serialNumber;
    long lastTransactionTime;
    /**
    * @return Retorna a descrição.
    */
    public String getDescription()  {
```

```
        return description;
    }
    /**
    * @param description A descrição a ser configurada.
    */
    public void setDescription(String description) {
        this.description = description;
    }
    /**
    * @return Retorna lastTransactionTime.
    */
    public long getLastTransactionTime() {
        return lastTransactionTime;
    }
    /**
    * @param lastTransactionTime O último lastTransactionTime a ser configurado.
    */
    public void setLastTransactionTime(long lastTransactionTime) {
        this.lastTransactionTime = lastTransactionTime;
    }
    /**
    * @return Retorna o preço.
    */
    public double getPrice() {
        return price;
    }
    /**
    * @param price O preço a ser configurado.
    */
    public void setPrice(double price) {
        this.price = price;
    }
    /**
    * @return Retorna um serialNumber.
    */
    public int getSerialNumber() {
        return serialNumber;
    }
    /**
    * @param serialNumber O serialNumber a ser configurado.
    */
    public void setSerialNumber(int serialNumber) {
        this.serialNumber = serialNumber;
    }
    /**
    * @return Retorna o registro.
    */
    public String getTicket() {
        return ticket;
    }
    /**
    * @param ticket O registro a ser configurado.
    */
    public void setTicket(String ticket) {
        this.ticket = ticket;
    }
    /**
    * @return Retorna a empresa.
    */
    public String getCompany() {
        return company;
    }
    /**
    * @param company A empresa a ser configurada.
    */
    public void setCompany(String company) {
        this.company = company;
    }
    //clone
    public Object clone() throws CloneNotSupportedException
    {
        return super.clone();
    }
}
```

É possível gravar uma classe do transformador do objeto customizado para a classe Stock:

```
/**
* Implementação customizada do ObjectTransformer do ObjectGrid para objeto stock
*
*/
public class MyStockObjectTransformer implements ObjectTransformer {
/* (non-Javadoc)
* @see
* com.ibm.websphere.objectgrid.plugins.ObjectTransformer#serializeKey
* (java.lang.Object,
* java.io.ObjectOutputStream)
*/
public void serializeKey(Object key, ObjectOutputStream stream) throws IOException {
    String ticket= (String) key;
    stream.writeUTF(ticket);
}

/* (non-Javadoc)
* @see com.ibm.websphere.objectgrid.plugins.
ObjectTransformer#serializeValue(java.lang.Object,
java.io.ObjectOutputStream)
*/
public void serializeValue(Object value, ObjectOutputStream stream) throws IOException {
    Stock stock= (Stock) value;
    stream.writeUTF(stock.getTicket());
    stream.writeUTF(stock.getCompany());
    stream.writeUTF(stock.getDescription());
    stream.writeDouble(stock.getPrice());
    stream.writeLong(stock.getLastTransactionTime());
    stream.writeInt(stock.getSerialNumber());
}

/* (non-Javadoc)
* @see com.ibm.websphere.objectgrid.plugins.
ObjectTransformer#inflateKey(java.io.ObjectInputStream)
*/
public Object inflateKey(ObjectInputStream stream) throws IOException, ClassNotFoundException {
    String ticket=stream.readUTF();
    return ticket;
}

/* (non-Javadoc)
* @see com.ibm.websphere.objectgrid.plugins.
ObjectTransformer#inflateValue(java.io.ObjectInputStream)
*/

public Object inflateValue(ObjectInputStream stream) throws IOException, ClassNotFoundException {
    Stock stock=new Stock();
    stock.setTicket(stream.readUTF());
    stock.setCompany(stream.readUTF());
    stock.setDescription(stream.readUTF());
    stock.setPrice(stream.readDouble());
    stock.setLastTransactionTime(stream.readLong());
    stock.setSerialNumber(stream.readInt());
    return stock;
}

/* (non-Javadoc)
* @see com.ibm.websphere.objectgrid.plugins.
ObjectTransformer#copyValue(java.lang.Object)
*/
public Object copyValue(Object value) {
    Stock stock = (Stock) value;
    try {
        return stock.clone();
    }
    catch (CloneNotSupportedException e)
    {
        // display exception message    }
}

/* (non-Javadoc)
* @see com.ibm.websphere.objectgrid.plugins.
ObjectTransformer#copyKey(java.lang.Object)
*/
public Object copyKey(Object key) {
    String ticket=(String) key;
    String ticketCopy= new String (ticket);
    return ticketCopy;
}
}
```

Em seguida, conecte esta classe MyStockObjectTransformer customizada ao BackingMap:

```
ObjectGridManager ogf=ObjectGridManagerFactory.getObjectGridManager();
ObjectGrid og = ogf.getObjectGrid("NYSE");
BackingMap bm = og.defineMap("NYSEStocks");
MyStockObjectTransformer ot = new MyStockObjectTransformer();
bm.setObjectTransformer(ot);
```

Plug-ins para Fornecer Listeners de Eventos

Java

Os plug-ins ObjectGridEventListener, MapEventListener, ObjectGridLifecycleListener e BackingMapLifecycleListener podem ser usados para configurar notificações para vários eventos no cache eXtreme Scale. Os plug-ins de listener são registrados com uma instância ObjectGrid ou BackingMap como outros plug-ins do eXtreme Scale e incluem pontos de integração e de customização para aplicativos e provedores de cache.

Plug-in do ObjectGridEventListener

Um plug-in ObjectGridEventListener fornece eventos de ciclo de vida do eXtreme Scale para a instância do ObjectGrid, shards e transações. Utilize um plug-in ObjectGridEventListener para receber notificações quando ocorrerem eventos significativos em um ObjectGrid. Esses eventos incluem inicialização do ObjectGrid, o início de uma transação, o encerramento de uma transação e destruição de um ObjectGrid. Para atender estes eventos, crie uma classe que implementa a interface ObjectGridEventListener e inclua-a no eXtreme Scale.

Para obter mais informações sobre a gravação de um plug-in do ObjectGridEventListener, consulte “Plug-in ObjectGridEventListener” na página 571. Também é possível consultar a Documentação da API para obter mais informações.

Incluindo e removendo instâncias do ObjectGridEventListener

Um ObjectGrid pode ter vários listeners ObjectGridEventListener. Inclua e remova os listeners usando os métodos addEventListener e removeEventListener na interface ObjectGrid. Também é possível registrar de modo declarativo os plug-ins ObjectGridEventListener com o arquivo descritor ObjectGrid. Para obter exemplos, consulte “Plug-in ObjectGridEventListener” na página 571.

Plug-in do MapEventListener

Um plug-in do MapEventListener fornece notificações de callback e alterações de estado de cache significativas que ocorrem para uma instância do BackingMap. Para obter detalhes sobre a gravação de um MapEventListener, consulte “Plug-in MapEventListener” na página 570. Também é possível consultar a Documentação da API para obter mais informações.

Incluindo e Removendo Instâncias do MapEventListener

Um eXtreme Scale pode ter vários listeners ObjectGridEventListener. Inclua e remova listeners com os métodos addMapEventListener e removeMapEventListener na interface BackingMap. Também é possível registrar de modo declarativo os plug-ins MapEventListener com o arquivo descritor ObjectGrid. Para obter exemplos, consulte “Plug-in MapEventListener” na página 570.

Plug-in BackingMapLifecycleListener

Um plug-in BackingMapLifecycleListener fornece notificações de retorno de chamada para as mudanças no estado do ciclo de vida que ocorrem para uma instância do BackingMap. A instância BackingMap continua por meio de um conjunto predefinido de estados durante seu tempo de vida.

Incluindo e removendo instâncias do BackingMapLifecycleListener

Um servidor eXtreme Scale pode ter vários listeners BackingMapLifecycleListener. Inclua e remova listeners com os métodosaddMapEventListener e removeMapEventListener na interface BackingMap. Quaisquer plug-ins do BackingMap que implementam a interface BackingMapLifecycleListener também são incluídos automaticamente como um BackingMapLifecycleListener na instância do ObjectGrid com a qual eles estão registrados. Também é possível registrar declaradamente os listeners BackingMapLifecycleListener com o arquivo descritor ObjectGrid. Para obter exemplos, consulte Plug-in BackingMapLifecycleListener.

Plug-in ObjectGridLifecycleListener

Um plug-in ObjectGridLifecycleListener fornece notificações de retorno de chamada para as mudanças no estado do ciclo de vida que ocorrem para uma instância do ObjectGrid. A instância do ObjectGrid continua por meio de um conjunto predefinido de estados durante seu tempo de vida.

Incluindo e removendo instâncias do ObjectGridLifecycleListener

Um eXtreme Scale pode ter vários listeners ObjectGridLifecycleListener. Inclua e remova os listeners usando os métodos addEventListener e removeEventListener na interface ObjectGrid. Todos os plug-ins do ObjectGrid que implementam a interface ObjectGridLifecycleListener são automaticamente incluídos como um ObjectGridLifecycleListener na instância do ObjectGrid com a qual eles estão registrados. Também é possível registrar declaradamente os listeners ObjectGridLifecycleListener com o arquivo descritor de implementação ObjectGrid. Para obter exemplos, consulte Plug-in ObjectGridLifecycleListener.

Plug-in MapEventListener: Java

Um plug-in MapEventListener fornece notificações de retorno de chamada e mudanças de estado de cache significativas que ocorrem para um objeto BackingMap: quando um mapa termina o pré-carregamento ou quando uma entrada é despejada do mapa. Um plug-in MapEventListener específico é uma classe customizada que você grava implementando a interface MapEventListener.

Convenções de Plug-in do MapEventListener

Ao desenvolver um plug-in do MapEventListener, é necessário seguir convenções comuns do plug-in. Para obter mais informações sobre convenções de plug-in, consulte “Visão Geral dos Plug-ins Java” na página 324. Para os outros tipos de plug-ins de listener, consulte “Plug-ins para Fornecer Listeners de Eventos” na página 569.

Depois de gravar uma implementação do MapEventListener, será possível conectá-la à configuração de BackingMap programaticamente ou com uma configuração XML.

Gravar uma Implementação do MapEventListener

Seu aplicativo pode incluir uma implementação do plug-in do MapEventListener. O plug-in deve implementar a interface MapEventListener para receber eventos significativos sobre um mapa. Os eventos são enviados para o plug-in do MapEventListener quando uma entrada é despejada do mapa e quando o pré-carregamento de um mapa é concluído.

Conexão Programática em uma Implementação do MapEventListener

O nome da classe para o MapEventListener customizado é a classe com.company.org.MyMapEventListener. Esta classe implementa a interface MapEventListener. O trecho de código a seguir cria o objeto MapEventListener customizado e o inclui em um objeto BackingMap:

```
ObjectGridManager objectGridManager =
 ObjectGridManagerFactory.getObjectGridManager();
ObjectGrid myGrid = objectGridManager.createObjectGrid("myGrid", false);
BackingMap myMap = myGrid.defineMap("myMap");
MyMapEventListener myListener = new MyMapEventListener();
myMap.addMapEventListener(myListener);
```

Conectar uma Implementação do MapEventListener Utilizando XML

Uma implementação do MapEventListner pode ser configurada utilizando XML. O XML a seguir deve estar no arquivo `myGrid.xml`:

```
<?xml version="1.0" encoding="UTF-8" ?>
<objectGridconfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="myGrid">
            <backingMap name="myMap" pluginCollectionRef="myPlugins" />
        </objectGrid>
    </objectGrids>
    <backingMapPluginCollections>
        <backingMapPluginCollection id="myPlugins">
            <bean id="MapEventListener" className=
       "com.company.org.MyMapEventListener" />
        </backingMapPluginCollection>
    </backingMapPluginCollections>
</objectGridConfig>
```

Fornecer este arquivo para a instância do ObjectGridManager facilita a criação desta configuração. O fragmento de código a seguir mostra como criar um ObjectGrid utilizando este arquivo XML. A instância ObjectGrid recém-criada tem um MapEventListener configurado no BackingMap myMap.

```
ObjectGridManager objectGridManager =
 ObjectGridManagerFactory.getObjectGridManager();
ObjectGrid myGrid =
 objectGridManager.createObjectGrid("myGrid", new URL("file:etc/test/myGrid.xml"),
  true, false);
```

Plug-in ObjectGridEventListener: Java

Um plug-in ObjectGridEventListener fornece eventos de ciclo de vida do WebSphere eXtreme Scale para o ObjectGrid, shards e transações. Um plug-in ObjectGridEventListener fornece notificações quando um ObjectGrid é inicializado ou destruído, e quando uma transação é iniciada ou encerrada. Plug-ins ObjectGridEventListener são classes customizadas que você grava implementando a interface ObjectGridEventListener. Opcionalmente, a implementação inclui subinterfaces do ObjectGridEventGroup e segue as convenções comuns do plug-in do eXtreme Scale.

Visão Geral

Um plug-in ObjectGridEventListener é útil quando um plug-in Loader estiver disponível e for necessário inicializar uma ou mais conexões do Java Database Connectivity (JDBC) para um backend quando as transações forem iniciadas e

encerradas. Normalmente, um plug-in ObjectGridEventListener e um plug-in Loader são gravados juntos.

Gravando um plug-in ObjectGridEventListener

Um plug-in ObjectGridEventListener deve implementar a interface ObjectGridEventListener para receber notificações sobre eventos significativos do eXtreme Scale. Para receber notificações de eventos adicionais, é possível implementar as interfaces a seguir. Estas subinterfaces são incluídas na interface ObjectGridEventGroup:

- Interface ShardEvents
- Interface ShardLifecycle
- Interface TransactionEvents

Para obter mais informações sobre essas interfaces, consulte a Documentação da API.

Eventos do Shard

Quando o serviço de catálogo colocar shards primários ou de réplica na partição em uma Java virtual machine (JVM), uma nova instância do ObjectGrid será criada nessa JVM para hospedar esse shard. Alguns aplicativos que precisam iniciar os encadeamentos no JVM, hospedam a notificação de necessidade primária desses eventos. A interface ObjectGridEventGroup.ShardEvents declara os métodos shardActivate e shardDeactivate. Esses métodos são chamados apenas quando uma parte é ativada como primária e quando a parte é desativada a partir da primária. Esses dois eventos permitem que o aplicativo inicie encadeamentos adicionais quando o shard for primário e pare os encadeamentos quando o shard voltar a ser uma réplica ou for retirado de serviço.

Um aplicativo pode determinar qual partição foi ativada ao procurar por um BackingMap específico na referência ObjectGrid fornecida para o método shardActivate usando o método ObjectGrid#getMap. O aplicativo pode visualizar, em seguida, o número de partição usando o método BackingMap#getPartitionId(). As partições são numeradas de 0 ao número de partições no descritor de implementação menos um.

Eventos de Ciclo de Vida do Shard

Os eventos dos métodos ObjectGridEventListener.initialize e ObjectGridEventListener.destroy são entregues utilizando a interface ObjectGridEventGroup.ShardLifecycle.

Eventos de Transação

Os métodos ObjectGridEventListener.transactionBegin e ObjectGridEventListener.transactionEnd são entregues através da interface ObjectGridEventGroup.TransactionEvents.

Se um plug-in ObjectGridEventListener implementa as interfaces ObjectGridEventListener e ShardLifecycle, então, os eventos de ciclo de vida do shard serão os únicos eventos a serem entregues para o listener. Após implementar qualquer uma das novas interfaces ObjectGridEventGroup internas, o eXtreme Scale entrega apenas esses eventos específicos através de novas interfaces. Com

essa implementação, o código pode ser compatível com as versões anteriores. Se você estiver utilizando as novas interfaces internas, poderá agora receber apenas os eventos específicos necessários.

Utilizando o Plug-in ObjectGridEventListener

Para utilizar um plug-in ObjectGridEventListener customizado, primeiro crie uma classe que implementa a interface ObjectGridEventListener e quaisquer subinterfaces do ObjectGridEventGroup opcionais. Inclua o listener customizado em um ObjectGrid para receber notificação de eventos importantes. Você tem duas abordagens para incluir um plug-in ObjectGridEventListener na configuração do eXtreme Scale: configuração programática e configuração XML.

Configurar um Plug-in do ObjectGridEventListener Programaticamente

Suponha que o nome de classe do listener de eventos do eXtreme Scale seja a classe com.company.org.MyObjectGridEventListener. Esta classe implementa a interface ObjectGridEventListener. O fragmento de código a seguir cria um ObjectGridEventListener customizado e o inclui em um ObjectGrid.

```
ObjectGridManager objectGridManager = ObjectGridManagerFactory.getObjectGridManager();
ObjectGrid myGrid = objectGridManager.createObjectGrid("myGrid", false);
MyObjectGridEventListener myListener = new MyObjectGridEventListener();
myGrid.addEventListener(myListener);
```

Configurar um Plug-in do ObjectGridEventListener com XML

Também é possível configurar um plug-in ObjectGridEventListener utilizando XML. O XML a seguir cria uma configuração que é equivalente ao listener de eventos do ObjectGrid programaticamente criado e descrito. O texto a seguir deve estar no arquivo `myGrid.xml`:

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="myGrid">
            <bean id="ObjectGridEventListener"
       className="com.company.org.MyObjectGridEventListener" />
            <backingMap name="Book"/>
        </objectGrid>
    </objectGrids>
</objectGridConfig>
```

Observe que as declarações de bean aparecem antes das declarações do backingMap. Forneça este arquivo para o plug-in ObjectGridManager para facilitar a criação desta configuração. O fragmento de código a seguir demonstra como criar uma instância do ObjectGrid utilizando este arquivo XML. A instância do ObjectGrid criada possui um listener ObjectGridEventListener configurado no ObjectGrid myGrid.

```
ObjectGridManager objectGridManager = ObjectGridManagerFactory.getObjectGridManager();
ObjectGrid myGrid = objectGridManager.createObjectGrid("myGrid", new URL("file:etc/test/myGrid.xml"), true, false);
```

Plug-in BackingMapLifecycleListener: Java

Um plug-in BackingMapLifecycleListener recebe a notificação de eventos de mudança de estado do ciclo de vida do WebSphere eXtreme Scale para o mapa de apoio.

O plug-in BackingMapLifecycleListener recebe um evento contendo um objeto BackingMapLifecycleListener.State para cada mudança de estado do mapa de apoio. Qualquer plug-in BackingMap que também implementa a interface BackingMapLifecycleListener será automaticamente ser incluído como um listener na instância do BackingMap na qual o plug-in está registrado.

Visão Geral

Um plug-in BackingMapLifecycleListener é útil quando um plug-in BackingMap existente precisa executar atividades referentes às atividades em um plug-in relacionado. Como exemplo, um plug-in do carregador precisar recuperar a configuração a partir de um plug-in MapIndexPlugin ou DataSerializer cooperantes.

Ao implementar a interface BackingMapLifecycleListener e detectar o evento BackingMapLifecycleListener.State.INITIALIZED, o carregador pode saber sobre o estado de outros plug-ins na instância do BackingMap. O carregador pode recuperar informações com segurança a partir do plug-in MapIndexPlugin ou DataSerializer cooperante, desde que o BackingMap esteja no estado INITIALIZED, significando que o método initialize() do outro plug-in foi chamado.

Um BackingMapLifecycleListener pode ser incluídos ou removidos a qualquer momento, seja antes ou depois do ObjectGrid e seus BackingMaps são inicializados.

Gravar o Plug-in BackingMapLifecycleListener

Um plug-in BackingMapLifecycleListener deve implementar a interface BackingMapLifecycleListener para receber notificações sobre eventos significativos do eXtreme Scale . Qualquer plug-in BackingMap pode implementar a interface BackingMapLifecycleListener e ser automaticamente incluído como um listener quando ele também for incluído no mapa de apoio.

Para obter mais informações sobre essas interfaces, consulte a Documentação da API.

Evento de Ciclo de Vida e Relacionamentos de Plug-in

O BackingMapLifecycleListener recupera o estado do ciclo de vida a partir do evento no método backingMapStateChanged, por exemplo:

```
public void backingMapStateChanged(BackingMap map,
                                   LifecycleEvent event)
throws LifecycleFailedException {
  switch(event.getState()) {
    case INITIALIZED: // All other plug-ins are initialized.
      // Retrieve reference to plug-in X for use from map.
      break;
    case DESTROYING:  // Destroy phase is starting
      // Eliminate reference to plug-in X it may be destroyed before this plug-in
      break;
  }
}
```

A ilustração a seguir resume os estados dos objetos BackingMap conforme eventos de ciclo de vida ocorrem e são enviados para um plug-in BackingMapLifecycleListener.

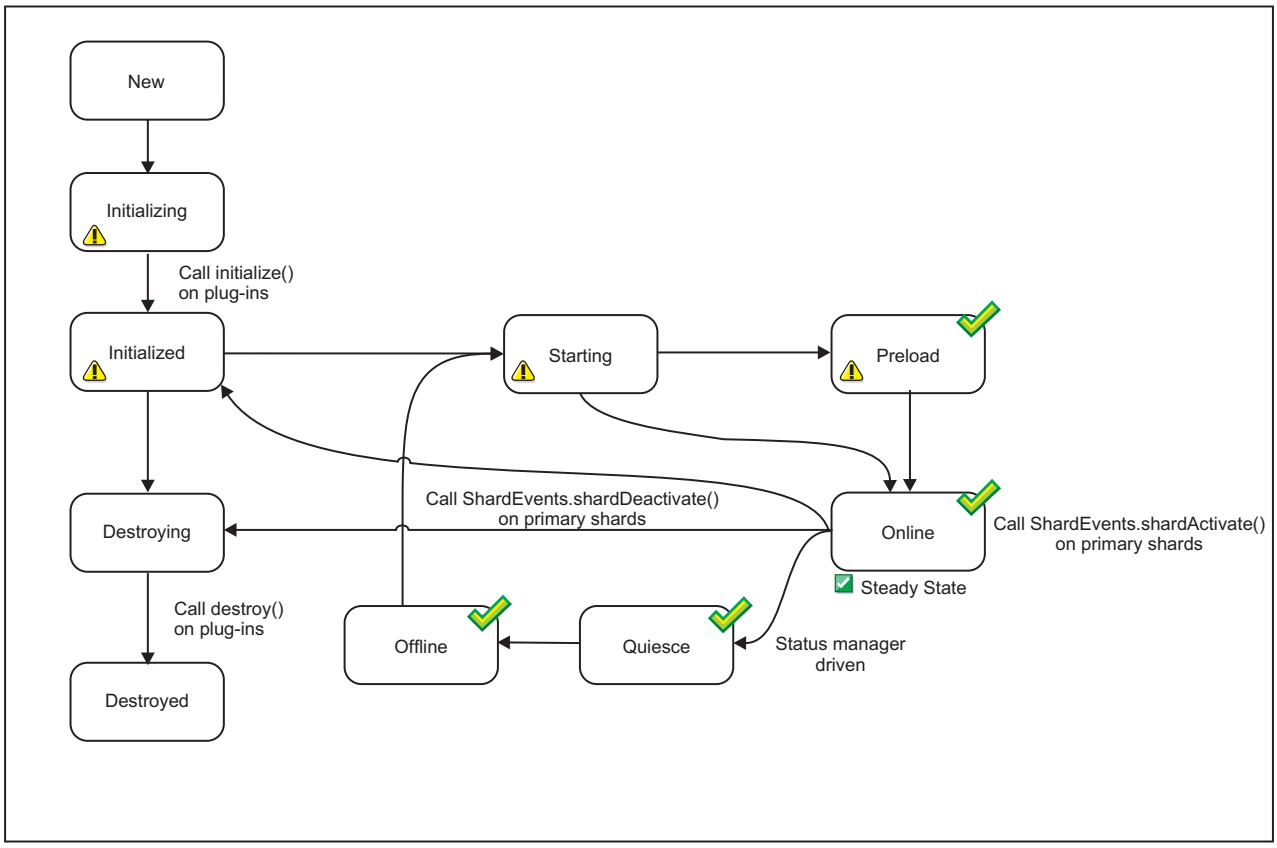


Figura 38. Resumo de Estado de BackingMap

A tabela a seguir descreve o relacionamento entre os eventos de ciclo de vida enviados para um plug-in BackingMapLifecycleListener e os estados do BackingMap e de outros objetos do plug-in.

Valor de BackingMapLifecycleListener.State	**Descrição**
INITIALIZING	A fase de inicialização do BackingMap está começando. O BackingMap e os plug-ins do BackingMap estão prestes a serem inicializados.
INITIALIZED	A fase de inicialização do BackingMap foi concluída. Todos os plug-ins do BackingMap foram inicializados. O estado INITIALIZED pode recorrer quando as atividades de posicionamento de shard (promoção ou rebaixamento) ocorrem.
STARTING	A instância do BackingMap está sendo ativada para uso como uma instância local, como uma instância do cliente ou como uma instância em um shard primário ou de réplica no servidor. Todos os plug-ins do ObjectGrid na instância do ObjectGrid que possuem esta instância do BackingMap foram inicializados. O estado STARTING pode recorrer quando as atividades de posicionamento de shard (promoção ou rebaixamento) ocorrem.
PRELOAD	A instância do BackingMap está configurada para o estado PRELOAD pela API StateManager para pré-carregamento ou o carregador configurado está pré-carregando dados no mapa de apoio.

Valor de BackingMapLifecycleListener.State	Descrição
ONLINE	A instância do BackingMap está pronta para funcionar como uma instância local, como uma instância do cliente ou como uma instância em um shard primário ou de réplica no servidor. Todos os plug-ins do ObjectGrid na instância do ObjectGrid que possuem esta instância do BackingMap foram inicializados. Esse estado estável é típico do BackingMap. O estado ONLINE pode recorrer quando as atividades de posicionamento de shard (promoção ou rebaixamento) ocorrem.
QUIESCE	O trabalho está parando no BackingMap como resultado da API StateManager ou de outro evento. Nenhum trabalho novo é permitido. Seu plug-in termina qualquer trabalho existente o mais breve possível.
OFFLINE	Todo o trabalho foi interrompido no BackingMap como resultado da API StateManager ou de outro evento. Nenhum trabalho novo é permitido.
DESTROYING	A instância do BackinMap está iniciando a fase de destruição. Os plug-ins do BackingMap para a instância estão prestes a serem destruídos.
DESTROYED	A instância do BackingMap e todos os plug-ins de BackingMap foram destruídos.

Configurar um Plug-in BackingMapLifecycleListener com XML

Suponha que o nome da classe do listener de eventos do eXtreme Scale seja a classe com.company.org.MyBackingMapLifecycleListener. Essa classe implementa a interface BackingMapLifecycleListener.

É possível configurar um plug-in BackingMapLifecycleListener usando XML. O texto a seguir deve estar no arquivo XML da grade de objeto:

```
<?xml version="1.0" encoding="UTF-8" ?>
<objectGridconfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
        xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="myGrid">
            <backingMap name="myMap" pluginCollectionRef="myPlugins" />
        </objectGrid>
    </objectGrids>
    <backingMapPluginCollections>
        <backingMapPluginCollection id="myPlugins">
            <bean id="BackingMapLifecycleListener"
                  className="com.company.org.MyBackingMapLifecycleListener" />
        </backingMapPluginCollection>
    </backingMapPluginCollections>
</objectGridConfig>
```

Forneça este arquivo para o plug-in ObjectGridManager para facilitar a criação desta configuração. A instância BackingMap criada possui um listener BackingMapLifecycleListener configurado no ObjectGrid myGrid.

Assim como o BackingMapLifecycleListener, outros plug-ins BackingMap, como Loader ou MapIndexPlugin, que são especificados usando XML e que também implementam a interface BackingMapLifecycleListener, serão incluídos automaticamente como listeners de ciclo de vida.

Referências relacionadas:

"Plug-in ObjectGridLifecycleListener"
Um plug-in ObjectGridLifecycleListener recebe a notificação de ciclo de vida do WebSphere eXtreme Scale, os eventos de mudança de estado para a grade de dados.

Plug-in ObjectGridLifecycleListener: Java

Um plug-in ObjectGridLifecycleListener recebe a notificação de ciclo de vida do WebSphere eXtreme Scale, os eventos de mudança de estado para a grade de dados.

O plug-in ObjectGridLifecycleListener recebe um evento contendo um objeto ObjectGridLifecycleListener.State para cada mudança de estado do ObjectGrid. Qualquer plug-in ObjectGrid que também implementa a interface ObjectGridLifecycleListener é incluído automaticamente como um listener na instância do ObjectGrid na qual o plug-in está registrado.

Visão Geral

Um plug-in ObjectGridLifecycleListener é útil quando um plug-in ObjectGrid existente precisa executar atividades ligadas às atividades de um plug-in relacionado. Como exemplo, um plug-in TransactionCallback pode precisar recuperar a configuração a partir de um plug-in ObjectGridEventListener ou ShardListener cooperantes.

Ao implementar a interface ObjectGridLifecycleListener e detectar o evento ObjectGridLifecycleListener.State.INITIALIZED, o plug-in TransactionCallback pode detectar o estado de outros plug-ins na instância do ObjectGrid. O plug-in TransactionCallback pode recuperar com segurança informações a partir do plug-in ObjectGridEventListener ou do plug-in ShardListener cooperante, desde que o ObjectGrid esteja em um estado INICIALIZADO, significando que o método initialize() do outro plug-in foi chamado.

É possível incluir um plug-in ObjectGridLifecycleListener a qualquer momento, antes ou depois de inicializar o ObjectGrid.

Gravar um Plug-in ObjectGridLifecycleListener

Um plug-in ObjectGridLifecycleListener deve implementar a interface ObjectGridLifecycleListener para receber notificações sobre eventos significativos do eXtreme Scale. Qualquer plug-in ObjectGrid pode implementar a interface ObjectGridLifecycleListener e ser incluído automaticamente como um listener quando ele também for incluído no ObjectGrid.

Para obter mais informações sobre essas interfaces, consulte a Documentação da API.

Evento de Ciclo de Vida e Relacionamentos de Plug-in

O ObjectGridLifecycleListener recupera o estado do ciclo de vida a partir do evento no método objectgridStateChanged, por exemplo:

```
public void objectGridStateChanged(ObjectGrid grid,
                                   LifecycleEvent event)
throws LifecycleFailedException {
  switch(event.getState()) {
```

```
    case INITIALIZED: // All other plug-ins are initialized.
      // Retrieve reference to plug-in X for use from grid.
      break;
    case DESTROYING:  // Destroy phase is starting
      // Eliminate reference to plug-in X it may be destroyed before this plug-in
      break;
  }
```

A ilustração a seguir resume os estados dos objetos ObjectGrid conforme eventos de ciclo de vida ocorrem e são enviados para um plug-in ObjectGridLifecycleListener.

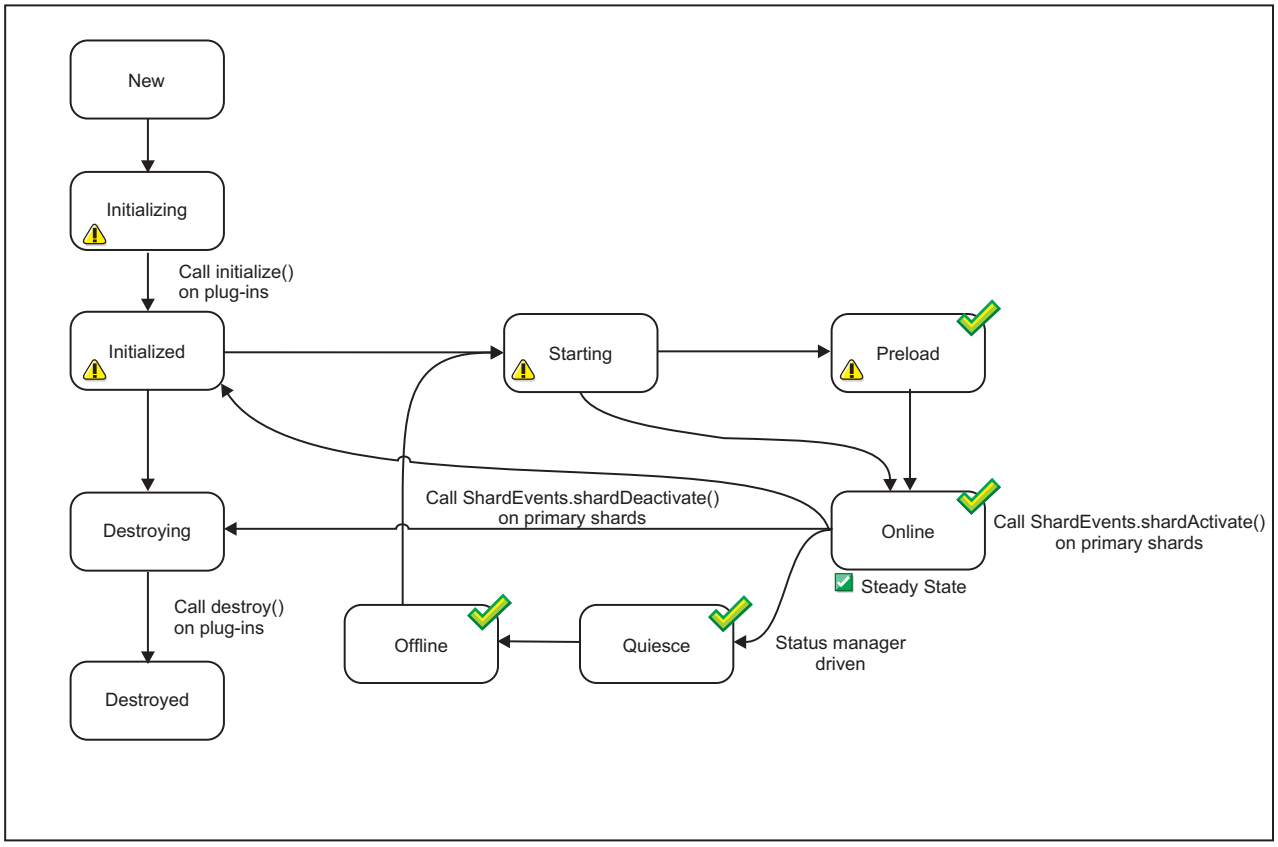


Figura 39. Resumo do Estado do ObjectGrid

A tabela a seguir descreve ainda mais o relacionamento entre eventos de ciclo de vida enviados para um ObjectGridLifecycleListener e os estados do ObjectGrid e de outros objetos de plug-in.

Valor de ObjectGridLifecycleListener.State	Descrição
INITIALIZING	A fase de inicialização do ObjectGrid está começando. O ObjectGrid e os plug-ins do ObjectGrid estão prestes a serem inicializados.
INITIALIZED	A fase de inicialização do ObjectGrid foi concluída. Todos os plug-ins do ObjectGrid foram inicializados. O estado INITIALIZED pode recorrer quando as atividades de posicionamento de shard (promoção ou rebaixamento) ocorrem. Todos os plug-ins de BackingMap nas instâncias do BackingMap de propriedade desta instância do ObjectGrid foram inicializados.

Valor de ObjectGridLifecycleListener.State	Descrição
STARTING	A instância do ObjectGrid está sendo ativada para uso como uma instância local, como uma instância do cliente ou como uma instância em um shard primário ou de réplica no servidor. O estado STARTING pode recorrer quando as atividades de posicionamento de shard (promoção ou rebaixamento) ocorrem.
PRELOAD	A instância do ObjectGrid está configurada para o estado PRELOAD pela API StateManager ou para outra configuração.
ONLINE	A instância do ObjectGrid está pronta para funcionar como uma instância local, como uma instância do cliente ou como uma instância em um shard primário ou de réplica no servidor. Esse estado estável é típico do ObjectGrid. O estado ONLINE pode recorrer quando as atividades de posicionamento de shard (promoção ou rebaixamento) ocorrem.
QUIESCE	O trabalho está parando no ObjectGrid como resultado da API StateManager ou de outro evento. Nenhum trabalho novo é permitido. Termine qualquer trabalho existente o mais breve possível.
OFFLINE	Todo o trabalho é interrompido no ObjectGrid como resultado da API StateManager ou de outro evento. Nenhum trabalho novo é permitido.
DESTROYING	A instância do ObjectGrid está iniciando a fase de destruição. Os plug-ins do ObjectGrid para a instância estão prestes a serem destruídos. Durante a fase de destruição, todas as instâncias do BackingMap possuídas por esta instância do ObjectGrid também serão destruídas.
DESTROYED	A instância do ObjectGrid, suas instâncias do BackingMap e todos os plug-ins do ObjectGrid forem destruídos.

Configurar um Plug-in ObjectGridLifecycleListener com XML

Suponha que o nome da classe do listener de eventos do eXtreme Scale seja a classe com.company.org.MyObjectGridLifecycleListener. Essa classe implementa a interface ObjectGridLifecycleListener.

É possível configurar um plug-in ObjectGridLifecycleListener usando XML. O XML a seguir cria uma configuração usando a interface ObjectGridLifecycleListener. O texto a seguir deve estar no arquivo xml da grade de objeto:

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="myGrid">
            <bean id="ObjectGridLifecycleListener"
                  className="com.company.org.MyObjectGridLifecycleListener" />
            <backingMap name="Book"/>
        </objectGrid>
    </objectGrids>
</objectGridConfig>
```

Observe que as declarações de bean aparecem antes das declarações do backingMap. Forneça este arquivo para o plug-in ObjectGridManager para facilitar a criação desta configuração.

Tal como o ObjectGridLifecycleListener registrado no exemplo anterior, outros plug-ins do ObjectGrid, CollisionArbiter ou TransactionCallback por exemplo, que são especificados usando XML que também implementa a interface

ObjectGridLifecycleListener, serão incluídos automaticamente como listeners de ciclo de vida.

Referências relacionadas:

"Plug-in BackingMapLifecycleListener" na página 573
Um plug-in BackingMapLifecycleListener recebe a notificação de eventos de mudança de estado do ciclo de vida do WebSphere eXtreme Scale para o mapa de apoio.

Plug-ins para Indexar Dados

Java

Dependendo do tipo de índices que você deseja construir, o WebSphere eXtreme Scale fornece plug-ins integrados que podem ser incluídos no BackingMap para construir um índice.

HashIndex

O HashIndex integrado, a classe com.ibm.websphere.objectgrid.plugins.index.HashIndex, é um plug-in MapIndexPlugin que pode ser incluído no BackingMap para construir índices estáticos ou dinâmicos. Essa classe suporta ambas as interfaces MapIndex e MapRangeIndex. A definição e a implementação de índices podem aprimorar significativamente o desempenho da consulta.

8.6+ InverseRangeIndex

O InverseRangeIndex integrado, a classe com.ibm.websphere.objectgrid.plugins.index.InverseRangeIndex, é um plug-in MapIndexPlugin que você pode incluir no BackingMap para construir índices estáticos. Esta classe suporta a interface MapIndex. A definição e implementação deste índice permite recuperar dados do intervalo a partir da grade.

Tarefas relacionadas:

Java "Configurando o Plug-in HashIndex" na página 586
É possível configurar o HashIndex integrado, a classe com.ibm.websphere.objectgrid.plugins.index.HashIndex, com um arquivo XML, programaticamente ou com uma anotação de entidade em um mapa de entidade.

Java "Acessando Dados com Índices (API de Índice)" na página 359
Use indexação para acesso a dados mais eficiente.

Referências relacionadas:

Java "Atributos do Plug-in HashIndex" na página 589
É possível usar os seguintes atributos para configurar o plug-in HashIndex. Esses atributos definem propriedades, como se você estiver usando um atributo ou HashIndex composto ou se a indexação do intervalo estiver ativada.

Java "Atributos do Plug-in InverseRangeIndex" na página 583
É possível usar os seguintes atributos para configurar o plug-in InverseRangeIndex. Esses atributos definem propriedades sobre como o índice é construído.

Java Interface GlobalIndex

Configurando o Plug-in InverseRangeIndex: Java

É possível configurar o InverseRangeIndex integrado, a classe com.ibm.websphere.objectgrid.plugins.index.InverseRangeIndex, com um arquivo XML ou programaticamente.

Antes de Iniciar

- Em um ambiente particionado, um dos requisitos-chave para InverseRangeIndex é o particionamento de dados baseado nos atributos sem intervalo configurados para um determinado índice. Todas as entradas de cache e chaves de procura com o mesmo valor de atributos sem intervalo devem ser roteadas para a mesma partição. Para obter informações adicionais sobre o particionamento, consulte "Roteando os Objetos de Cache para a Mesma Partição" na página 432.
- InverseRangeIndex é uma implementação de MapIndexPlugin. MapIndexPlugin pode ser acessado apenas a partir do lado do servidor da grade de objeto e não do lado do cliente. Para ativar as operações de procura no lado do cliente, é possível implementar a interface MapGridAgent. Para obter informações adicionais, consulte "Exemplo da API do DataGrid" na página 510.

Sobre Esta Tarefa

O plug-in InverseRangeIndex foi projetado para suportar consultas com uma chave de procura específica em dados de estilo de intervalo. Os dados de estilo de intervalo contêm atributos com valores limites. Considere a tabela de amostra a seguir que inclui dados de estilo não de intervalo e de intervalo. A tabela Dados do Produto contém atributos não de intervalo, incluindo ProductName, Condition e Country. Esses atributos são parte da chave de índice. A tabela também inclui atributos de estilo de intervalo, incluindo StartPromotionDate, EndPromotionDate, MinimumRAM e MaximumRAM, que também fazem parte da chave de índice. O atributo Price é o valor para o objeto armazenado em cache que não faz parte da chave de indexação ou da chave de procura na grade de dados. Para definir um índice de intervalo inverso, você deve utilizar a propriedade AttributeName que é uma lista de atributos delimitada por vírgulas, que deve conter um ou mais atributos não de intervalo e um ou mais atributos de estilo do intervalo. Os atributos de indexação podem fazer parte do valor da chave de cache ou de cache e especificados com a propriedade AddressableKeyName. Para obter mais informações sobre AttributeName, consulte "Atributos do Plug-in InverseRangeIndex" na página 583.

Tabela 17. Exemplo: Dados do Produto

Product Name	Start Promotion Date	End Promotion Date	Minimum RAM	Maximum RAM	Condição	País	Preço
PC01	01/01/11	31/12/11	2	4	Bom	CEP 22290-240	199
PC01	01/01/11	31/12/11	6	8	Bom	CEP 22290-240	259
PC01	01/01/12	31/12/12	2	4	Bom	CEP 22290-240	299
PC01	01/01/12	31/12/12	2	8	Bom	CEP 22290-240	499
PC02	01/01/08	31/12/10	2	4	Bom	CEP 22290-240	99

Tabela 17. Exemplo: Dados do Produto (continuação)

Product Name	Start Promotion Date	End Promotion Date	Minimum RAM	Maximum RAM	Condição	País	Preço
PC02	01/01/10	31/12/11	2	4	Bom	CEP 22290-240	289
PC02	01/01/12	31/12/12	4	6	Bom	CEP 22290-240	389

O ProductKey da classe da chave do índice possui três atributos sem intervalo: productName, condition e country. Ele também possui quatro atributos de estilo de intervalo com valores de limite: [startPromotionDate, endPromotionDate], [minimumRAM, maximumRAM]. As classes a seguir são utilizadas enquanto os objetos são colocados no mapa:

```
public class ProductKey {
String productName;
Date startPromotionDate;
Date endPromotionDate;
Integer minimumRAM;
Integer maximumRAM;
String condition;
String country;
}
```

O ProductSearchKey da classe de chave de procura possui cinco atributos que procuram dados de estilo de intervalo: productName, promotionDate, RAM, condition e country. Os seguintes objetos são utilizados na operação de MapIndexPlugin:

```
public class ProductSearchKey {
String productName;
Date promotionDate;
Integer RAM;
String condition;
String country;
}
```

Com base nessas classes, o InverseRangeIndex pode ser configurado com a propriedade AttributeName como:

```
key.productName, promotionDate[key.startPromotionDate, key.endPromotionDate], RAM[key.minimumRAM,key
condition[key.condition], key.country
```

Para obter mais informações sobre a sintaxe de AttributeName, consulte "Atributos do Plug-in InverseRangeIndex" na página 583.

Procedimento

- Configure um InverseRangeIndex no arquivo XML do descritor do ObjectGrid. Use o elemento backingMapPluginCollections para definir o plug-in:

```
<bean id="MapIndexPlugin"
   className="com.ibm.websphere.objectgrid.plugins.index.InverseRangeIndex">
 <property name="Name"
type="java.lang.String" value="productData"/>
 <property name="AttributeName"
type="java.lang.String" value="key.productName,
```

```
 promotionDate[key.startPromotionDate, key.endPromotionDate], RAM[key.minimumRAM,key.maximumRAM],

condition[key.condition], key.country"/>
</bean>
```

Para obter mais informações sobre o elemento backingMapPluginCollections, consulte Arquivo XML descritor do ObjectGrid.

- Configure um InverseRangeIndex programaticamente. O código de exemplo a seguir cria o mesmo índice de intervalo inverso:

  ```
  InverseRangeIndex mapIndex = new InverseRangeIndex();
  mapIndex.setName("productInfo");
  mapIndex.setAttributeName(("key.productName, promotionDate[key.startPromotionDate,
  key.endPromotionDate], RAM[key.minimumRAM,key.maximumRAM],
  condition[key.condition], key.country"));
  BackingMap bm = objectGrid.defineMap("mymap");
  bm.addMapIndexPlugin(mapIndex);
  ```

  É possível incluir o plug-in InverseRangeIndex em um mapa de apoio. No exemplo a seguir, é possível configurar o plug-in InverseRangeIndex incluindo plug-ins de índice estático em um arquivo XML:

  ```
  <backingMapPluginCollection id="product">
     <bean id="MapIndexPlugin"
        className="com.ibm.websphere.objectgrid.plugins.index.InverseRangeIndex">
           <property name="Name"
  type="java.lang.String" value="productData"
              description="index name" />
           <property name="AddressableKeyName"
  type="java.lang.String" value="key"
              description="key is default" />
           <property name="AttributeName" type="java.lang.String"
  value="key.productName, promotionDate[key.startPromotionDate, key.endPromotionDate],
  RAM[key.minimumRAM,key.maximumRAM],
  condition[key.condition], key.country"
              description="attribute names for indexing" />
     </bean>
  </backingMapPluginCollection>
  ```

  A classe InverseRangeIndex integrada é usada como o plug-in de índice. InverseRangeIndex suporta propriedades que os usuários podem configurar, como Name, AddressableKeyName, AttributeName e FieldAccessAttribute.

  A propriedade Name é configurada como productData, uma sequência que identifica este plug-in de índice. O valor da propriedade Name deve ser exclusivo dentro do escopo do mapa de apoio. O nome pode ser usado para recuperar o objeto de índice pelo nome da instância de ObjectMap para o BackingMap.

  A propriedade AttributeName é configurada como `"key.productName, promotionDate[key.startPromotionDate, key.endPromotionDate], RAM[key.minimumRAM,key.maximumRAM], condition[key.condition], key.country"`, que significa que productName, condition, country são atributos sem intervalo e startPromotionDate, endPromotionDate, minimumRAM, maximumRAM são atributos de intervalo do objeto de chave armazenado em cache para construir o índice.

  Se um aplicativo deve procurar objetos armazenados em cache com um nome de atributo diferente, um alias pode ser configurado para cada atributo, conforme mostrado no exemplo.

Atributos do Plug-in InverseRangeIndex: Java

É possível usar os seguintes atributos para configurar o plug-in InverseRangeIndex. Esses atributos definem propriedades sobre como o índice é construído.

Atributos

Nome Especifica o nome do índice. O nome deve ser exclusivo para cada mapa. O nome é usado para recuperar o objeto do da instância de mapa de objetos para o mapa de apoio.

AddressableKeyName
Especifica o prefixo para nomes de atributos a serem lidos a partir da chave de indexação. Se o prefixo for configurado, a lógica de indexação verificará os nomes de atributos que são prefixados com este valor e utilizará ponto como separador de caminho. Esse atributo é opcional e o valor padrão para este atributo é "key". Todos os nomes de atributos que não possuem este prefixo são tratados como atributos de valor. A propriedade não é aplicável ao utilizar o serializador.

Nota: A propriedade **AddressableKeyName** é aplicável apenas para indexar nomes de atributo-chave e não pode ser usada como um atributo de chave de procura.

AttributeName
Os valores delimitados por vírgula de nomes de atributos a serem incluídos na consulta para o índice de intervalo inverso. A sintaxe para **AttributeName** pode consistir em:

- um ou mais atributos sem intervalo e um ou mais atributos de intervalo simples;
- um ou mais atributos sem intervalo e apenas um atributo com diversos intervalos.

Portanto, a sintaxe para **AttributeName** é:

```
attribute_name_string ::= ({non_range_attribute}, {simple_range_attribute}) | ({non_range_at

non_range_attribute ::= (search_attribute_name,
"[", index_attribute_name, "]") | (index_attribute_name);


simple_range_attribute ::= search_attribute_name
"[" low_index_attribute_name "," high_index_attribute_name "]";

multi_range_attribute ::= [search_attribute_list_name]
"[[" index_attribute_list_name "]]";
```

Há três tipos de atributos:

- **non_range_attribute**
  Um atributo sem intervalo. A sintaxe é composta de um nome de chave de procura opcional e um nome de chave de indexação necessário.Use o **search_attribute_name** para procurar o nome do atributo em uma chave de procura de intervalo inversa. Quando este atributo não for especificado, o atributo **index_attribute_name** será utilizado. **O atributo index_attribute_name** é necessário e especifica um atributo sem intervalo como parte da chave do índice de intervalo inversa. O exemplo a seguir mostra um atributo sem intervalo para a seguinte definição de InverseRangeIndex:

```
<backingMapPluginCollection id="productData">
 <bean id="MapIndexPlugin"
   className="com.ibm.websphere.objectgrid.plugins.index.InverseRangeIndex">
```

```
  <property name="Name" type="java.lang.String"
    value="InverseRangeIndex"description="inverse range index"/>
  <property name="AddressableKeyName"
    type="java.lang.String"value="KeyAttribute" description="attribute name for range va
  <property name="AttributeName" type="java.lang.String"
     value="productName KeyAttribute.productName],promotionDate
     KeyAttribute.startPromotionDate,
    KeyAttribute.endPromotionDate],RAM[KeyAttribute.minRAM,KeyAttribute.maxRAM], conditi
    description="attribute name for inverse range index"/>
 </bean>
</backingMapPluginCollection>
```

- `productName`, `condition` e `country` são atributos sem intervalo consultados na chave e os mesmos nomes são usados para a chave de procura de índice.
- `startPromotionDate` e `endPromotionDate` são lidos a partir da chave e tratados como um atributo de intervalo simples. `promotionDate` é lido a partir da chave de procura para a operação **`findAll(Object searchKey)`**.
- `minRAM` e `maxRAM` são lidos a partir da chave e tratados como um atributo de intervalo simples. `RAM` é lido a partir da chave de procura para a operação **`findAll(Object searchKey)`**.

- **`simple_range_attribute`**

  Contém valores limites para um intervalo. A sintaxe é composta de um nome de chave de procura necessário e um nome de chave de indexação necessário. Use o atributo **`search_attribute_name`** para procurar o atributo de nome em uma chave de procura de intervalo inversa. O atributo **`low_index_attribute_name`** especifica um valor de limite baixo e o atributo **`high_index_attribute_name`** correspondente especifica um valor de limite alto. As chaves do índice são obrigatórias e utilizadas como parte da chave de índice de intervalo inversa.

- **`multi_range_attribute`**

  Uma matriz ou lista de atributos de intervalo na qual cada elemento ocorre novamente em uma matriz ou lista com dois valores limites.A sintaxe é composta de um nome de chave de procura opcional e um nome de chave de indexação necessário. Utilize o atributo **`search_attribute_list_names`** para procurar um nome de atributo em uma lista ou uma matriz como parte de uma chave de procura de intervalo inversa. Quando este atributo não é especificado, o **`index_attribute_list_name`** é usado. Esse atributo é obrigatório e deve ser utilizado como parte da chave de índice de intervalo inversa. Cada elemento na lista ou matriz deve ocorrer novamente na lista ou matriz com dois valores. Os dois valores são os valores de limite baixo e alto para um intervalo.

  O exemplo a seguir mostra um atributo com vários intervalos para InverseRangeIndex:

```
<backingMapPluginCollection id="productData">
  <bean id="MapIndexPlugin"
   <className="com.ibm.websphere.objectgrid.plugins.index.InverseRangeIndex">
   <property name="Name" type="java.lang.String"
   value="InverseRangeIndex"
   description="inverse range index "/>
   <property name="AttributeName" type="java.lang.String"
   value="key.identifier,rangeValues [[key.rangeValues]]"
   description="attribute name for inverse range index" />
  </bean>
</backingMapPluginCollection>
```

FieldAccessAttribute

Usado para mapas sem entidade. Se `true`, o objeto será acessado usando os campos diretamente. Se não for especificado ou se especificar `false`, o método getter para o atributo será usado para acessar os dados.

Conceitos relacionados:

Java "Plug-ins para Indexar Dados" na página 580
Dependendo do tipo de índices que você deseja construir, o WebSphere eXtreme Scale fornece plug-ins integrados que podem ser incluídos no BackingMap para construir um índice.

Java "Plug-ins para Indexação Customizada de Objetos de Cache" na página 593
Com um plug-in MapIndexPlugin, ou índice, é possível gravar estratégias de indexação customizadas que vão além de índices integrados fornecidos pelo eXtreme Scale.

Java "Usando um Índice Composto" na página 596
O HashIndex composto aprimora o desempenho da consulta e evita a custosa varredura de mapa. O recurso também fornece uma maneira conveniente para a API HashIndex localizar objetos em cache quando os critérios de busca envolvem muitos atributos.

Java "Indexação" na página 280
Use o plug-in MapIndexPlugin para construir um índice ou vários índices em um BackingMap para suportar acesso a dados sem chave.

Java "Utilizando o Índice Global" na página 599
O índice global pode melhorar o desempenho da procura de dados em ambiente particionado grande, por exemplo 100 partições.

"Utilizando o Índice Global" na página 599
O índice global pode melhorar o desempenho da procura de dados em ambiente particionado grande, por exemplo 100 partições.

"Otimização de Consulta do Cliente Utilizando Índices Globais" na página 759
Ao executar consultas a partir do ObjectGrid do cliente, é necessário configurar a partição se os mapas envolvidos são particionados. Em um grande ambiente do ObjectGrid particionado, o aplicativo geralmente precisa executar consultas paralelas simultaneamente em todas as partições para obter o resultado da consulta completo. Por exemplo, se houver 100 partições, o aplicativo deverá executar a mesma consulta em todas as 100 partições e mesclar os resultados da consulta para obter o resultado da consulta completo. Isto geralmente consome grandes quantidades de recurso do sistema.

"Ajustando o Desempenho de Consulta" na página 746
Para ajustar o desempenho de suas consultas, utilize as técnicas e dicas a seguir.

Tarefas relacionadas:

Java "Configurando o Plug-in HashIndex"
É possível configurar o HashIndex integrado, a classe com.ibm.websphere.objectgrid.plugins.index.HashIndex, com um arquivo XML, programaticamente ou com uma anotação de entidade em um mapa de entidade.

Java "Acessando Dados com Índices (API de Índice)" na página 359
Use indexação para acesso a dados mais eficiente.

Configurando o Plug-in HashIndex: Java

É possível configurar o HashIndex integrado, a classe com.ibm.websphere.objectgrid.plugins.index.HashIndex, com um arquivo XML, programaticamente ou com uma anotação de entidade em um mapa de entidade.

Sobre Esta Tarefa

Configurar um índice composto é o mesmo que configurar um índice regular com XML, exceto para o valor da propriedade **attributeName**. Em um índice composto, o valor da propriedade **attributeName** é uma lista de atributos delimitados por vírgulas. Por exemplo, a classe de valor Endereço tem três atributos: cidade, estado e CEP. Um índice composto pode ser definido com o valor da propriedade **attributeName** como `"city,state,zipcode"` indicando que a cidade, estado e CEP são incluídos no índice composto.

Também, note que o HashIndexes composto não suporta consultas de intervalo e, portanto, não pode ter a propriedade RangeIndex configurada para true.

Procedimento

- Configure um índice composto no arquivo descritor XML do ObjectGrid.

  Use o elemento backingMapPluginCollections para definir o plug-in:

```
<bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
 <property name="Name"
type="java.lang.String" value="Address.CityStateZip"/>
 <property name="AttributeName"
type="java.lang.String" value="city,state,zipcode"/>
</bean>
```

- Configure um índice composto programaticamente.

  O seguinte código de exemplo cria o mesmo índice composto:

```
   HashIndex mapIndex = new HashIndex();
    mapIndex.setName("Address.CityStateZip");
    mapIndex.setAttributeName(("city,state,zipcode"));
    mapIndex.setRangeIndex(true);

    BackingMap bm = objectGrid.defineMap("mymap");
    bm.addMapIndexPlugin(mapIndex);
```

- Configure um índice composto com notações de entidade.

  Se você estiver usando mapas de entidade, será possível usar uma abordagem de anotação para definir um índice composto. É possível definir uma lista de CompositeIndex dentro da anotação CompositeIndexes no nível da classe de entidade. O CompositeIndex possui um nome e a propriedade **attributeNames**. Cada CompositeIndex é associado a uma instância do HashIndex aplicada ao mapa de apoio que é associado à entidade. O HashIndex é configurado como um índice de não-intervalo.

```
@Entity
@CompositeIndexes({
    @CompositeIndex(name=" CityStateZip ", attributeNames=" city,state,zipcode"),
    @CompositeIndex(name="lastnameBirthday", attributeNames=" lastname,birthday ")
 })
public class Address {
    @Id int id;
    String street;
    String city;
    String state;
    String zipcode;
    String lastname;
    Date birthday;
}
```

  A propriedade nomeada para cada índice composto deve ser exclusiva dentro do mapa de entidade e de apoio. Se o nome não for especificado, um nome gerado será usado. A propriedade **attributeName** é usada para preencher o HashIndex attributeName com a lista de atributos delimitados por vírgulas. Os nomes de atributos coincidem com os nomes de campo persistente quando as entidades são configuradas para usar acesso à campo, ou o nome da propriedade como definida para as convenções de nomenclatura JavaBeans para entidades de

acesso à propriedade. Por exemplo: Se o nome do atributo for `street`, o método getter da propriedade será denominado getStreet.

Exemplo: Incluindo HashIndex no BackingMap

No exemplo a seguir, o plug-in HashIndex é configurado ao incluir plug-ins de índice estáticos no arquivo XML :

```
<backingMapPluginCollection id="person">
   <bean id="MapIndexPlugin"
      className="com.ibm.websphere.objectgrid.plugins.index.HashIndex">
         <property name="Name"
type="java.lang.String" value="CODE"
            description="index name" />
         <property name="RangeIndex" type="boolean" value="true"
            description="true for MapRangeIndex" />
         <property name="AttributeName"
type="java.lang.String" value="employeeCode" description="attribute name" />
   </bean>
</backingMapPluginCollection>
```

Neste exemplo de configuração XML, a classe HashIndex integrada é usada como o plug-in de índice. O HashIndex suporta propriedades que os usuários podem configurar, como Name, RangeIndex e AttributeName.

- A propriedade **`Name`** é configurada como `CODE`, uma sequência que identifica este plug-in de índice. O valor de propriedade **`Name`** deve ser exclusivo dentro do escopo do mapa de apoio. O nome pode ser usado para recuperar o objeto do índice pelo nome a partir da instância do ObjectMap do BackingMap.
- A propriedade **`RangeIndex`** é configurada como `true`, o que significa que o aplicativo pode efetuar cast do objeto do índice recuperado para a interface MapRangeIndex. Se a propriedade RangeIndex for configurada como `false`, o aplicativo poderá apenas efetuar cast do objeto do índice recuperado para a interface MapIndex. Um MapRangeIndex suporta funções para localizar dados usando funções de intervalo, como maior que, menor que, ou ambas, enquanto um MapIndex suporta apenas funções iguais. Se o índice precisar ser usado por consulta, a propriedade **`RangeIndex`** deverá ser configurada como `true` em índices de atributo único ou `false` em índices de relacionamento ou compostos. Para um índice de relacionamento e um índice composto, a propriedade **`RangeIndex`** deverá ser configurada para `false`.
- A propriedade **`AttributeName`** é configurada como `employeeCode`, o que significa que o atributo employeeCode do objeto em cache é usado para construir um índice de atributo único. Se um aplicativo precisar procurar por objetos em cache com diversos atributos, a propriedade **`AttributeName`** poderá ser configurada para uma lista de atributos delimitados por vírgula, rendendo um índice composto.

Em resumo, o exemplo anterior define um HashIndex do intervalo de atributo único. Ele é um HashIndex de atributo único porque o valor da propriedade **`AttributeName`** `employeeCode` inclui apenas um nome de atributo. É também um HashIndex de intervalo.

Conceitos relacionados:

Java "Plug-ins para Indexar Dados" na página 580
Dependendo do tipo de índices que você deseja construir, o WebSphere eXtreme Scale fornece plug-ins integrados que podem ser incluídos no BackingMap para construir um índice.

Java "Plug-ins para Indexação Customizada de Objetos de Cache" na página 593
Com um plug-in MapIndexPlugin, ou índice, é possível gravar estratégias de indexação customizadas que vão além de índices integrados fornecidos pelo eXtreme Scale.

Java "Usando um Índice Composto" na página 596
O HashIndex composto aprimora o desempenho da consulta e evita a custosa varredura de mapa. O recurso também fornece uma maneira conveniente para a API HashIndex localizar objetos em cache quando os critérios de busca envolvem muitos atributos.

Java "Indexação" na página 280
Use o plug-in MapIndexPlugin para construir um índice ou vários índices em um BackingMap para suportar acesso a dados sem chave.

Java "Utilizando o Índice Global" na página 599
O índice global pode melhorar o desempenho da procura de dados em ambiente particionado grande, por exemplo 100 partições.

"Utilizando o Índice Global" na página 599
O índice global pode melhorar o desempenho da procura de dados em ambiente particionado grande, por exemplo 100 partições.

"Otimização de Consulta do Cliente Utilizando Índices Globais" na página 759
Ao executar consultas a partir do ObjectGrid do cliente, é necessário configurar a partição se os mapas envolvidos são particionados. Em um grande ambiente do ObjectGrid particionado, o aplicativo geralmente precisa executar consultas paralelas simultaneamente em todas as partições para obter o resultado da consulta completo. Por exemplo, se houver 100 partições, o aplicativo deverá executar a mesma consulta em todas as 100 partições e mesclar os resultados da consulta para obter o resultado da consulta completo. Isto geralmente consome grandes quantidades de recurso do sistema.

"Ajustando o Desempenho de Consulta" na página 746
Para ajustar o desempenho de suas consultas, utilize as técnicas e dicas a seguir.

Referências relacionadas:

Java "Atributos do Plug-in HashIndex"
É possível usar os seguintes atributos para configurar o plug-in HashIndex. Esses atributos definem propriedades, como se você estiver usando um atributo ou HashIndex composto ou se a indexação do intervalo estiver ativada.

Java "Atributos do Plug-in InverseRangeIndex" na página 583
É possível usar os seguintes atributos para configurar o plug-in InverseRangeIndex. Esses atributos definem propriedades sobre como o índice é construído.

Java Interface GlobalIndex

Atributos do Plug-in HashIndex: Java

É possível usar os seguintes atributos para configurar o plug-in HashIndex. Esses atributos definem propriedades, como se você estiver usando um atributo ou HashIndex composto ou se a indexação do intervalo estiver ativada.

Atributos

Nome Especifica o nome do índice. O nome deve ser exclusivo para cada mapa. O nome é usado para recuperar o objeto do da instância de mapa de objetos para o mapa de apoio.

AttributeName
Especifica os nomes delimitados por vírgula dos atributos a serem indexados. Para índices acessados por campo, os nomes de atributos são equivalentes aos nomes de campo. Para índices acessados por propriedade, os nomes de atributos são os nomes da propriedade compatíveis com JavaBean. Se apenas um nome de atributo existir, o HashIndex será um índice de atributo único. Se este atributo for um relacionamento, ele também será um índice de relacionamento. Se múltiplos nomes de atributo são incluídos nos nomes de atributo, o HashIndex é um índice composto.

FieldAccessAttribute
Usado para mapas sem entidade. Se `true`, o objeto será acessado usando os campos diretamente. Se não for especificado ou se especificar `false`, o método getter para o atributo será usado para acessar os dados.

8.6+ GlobalIndexEnabled
Se true, o índice global será ativado e o aplicativo pode lançar o objeto do índice recuperado para a interface MapGlobalIndex

Quando a propriedade GlobalIndexEnabled do HashIndex é configurada como true, a função do índice global de HashIndex é ativada para suportar a interface MapGlobalIndex na parte superior de qualquer configuração do HashIndex. Ela fornece uma maneira eficiente de localizar dados no ambiente particionado grande.

O exemplo a seguir mostra que o índice global está ativado em um HashIndex de atributo único:

```
<bean id="MapIndexPlugin"
      className="com.ibm.websphere.objectgrid.plugins.index.HashIndex">
         <property name="Name"
type="java.lang.String" value="CODE"
            description="index name" />
         <property name="AttributeName"
type="java.lang.String" value="employeeCode" description="attribute name" />
  <property name="GlobalIndexEnabled" type="boolean" value="true"
            description="true for global index" />
   </bean>
```

POJOKeyIndex
Usado para mapas sem entidade. Se especificar `true`, o índice examinará o objeto na parte da chave do mapa. Esta configuração é útil quando a chave é uma chave composta e o valor não tem a chave integrada dentro dele. Se não for especificado ou se especificar `false`, o índice examinará o objeto na parte do valor do mapa.

RangeIndex
Se especificar `true`, a indexação do intervalo será ativada e o aplicativo poderá efetuar cast do objeto do índice recuperado para a interface MapRangeIndex. Se a propriedade **`RangeIndex`** for configurada como `false`, o aplicativo poderá efetuar cast do objeto do índice recuperado apenas para a interface MapIndex.

HashIndex de Atributo Único Versus HashIndex Composto

Quando a propriedade **AttributeName** de HashIndex inclui diversos nomes de atributos, o HashIndex será um índice composto. Caso contrário, se ela incluir somente um nome de atributo, ela é um índice de atributo único. Por exemplo, o valor da propriedade AttributeName de um HashIndex composto pode ser `city,state,zipcode`. Ela inclui três atributos delimitados por vírgulas. Se a propriedade valor **AttributeName** for apenas `zipcode` que tem apenas um atributo, ele será um HashIndex de atributo único.

O HashIndex composto fornece uma maneira eficiente de consultar objetos em cache quando os critérios de busca envolvem muitos atributos. No entanto, ele não suporta o índice de intervalo e sua propriedade RangeIndex deve ser configurada para `false`.

Para obter mais informações, consulte “Usando um Índice Composto” na página 596.

HashIndex de Relacionamento

Se o atributo indexado de um HashIndex de atributo único for um relacionamento, tanto com valor único ou múltiplos valores, o HashIndex é um HashIndex de relacionamento. Para HashIndex de relacionamento, a propriedade RangeIndex de HashIndex deve ser definida para “false”.

O HashIndex de relacionamento pode acelerar as consultas que usam referências cíclicas ou usam os filtros de consulta IS NULL, IS EMPTY, SIZE e MEMBER OF. Para obter mais informações, consulte o “Otimização de Consulta Utilizando Índices” na página 751.

HashIndex Principal

Para mapas sem entidade, quando a propriedade **POJOKeyIndex** do HashIndex é configurada para `true`, o HashIndex é um HashIndex principal e a parte da chave da entrada é usada para indexação. Quando a propriedade AttributeName do HashIndex não é especificada, a chave inteira é indexada; caso contrário, o HashIndex principal poderá ser apenas um HashIndex de atributo único.

Por exemplo, a inclusão da seguinte propriedade na amostra precedente faz com que o HashIndex se torne o HashIndex principal porque o valor da propriedade POJOKeyIndex é `true`.

```
<property name="POJOKeyIndex" type="boolean" value="true"
description="indicates if POJO key HashIndex" />
```

No exemplo do índice de chave anterior, como o valor da propriedade **AttributeName** é especificado como `employeeCode`, o atributo indexado é o campo **employeeCode** da parte da chave da entrada do mapa. Se você desejar construir o índice principal na parte da chave inteira da entrada do mapa, remova a propriedade **AttributeName**.

HashIndex de Intervalo

Quando a propriedade RangeIndex do HashIndex é configurada para `true`, o HashIndex é um índice de intervalo e pode suportar a interface MapRangeIndex. Uma implementação MapRangeIndex suporta funções para localizar dados usando funções de intervalo, como maior que, menor que, ou ambas, enquanto que um

MapIndex suporta apenas funções iguais. Para um índice de atributo único, a propriedade **RangeIndex** pode ser configurada para `true` apenas se o atributo indexado for do tipo Comparable. Se o índice de atributo único for usado pela consulta, a propriedade RangeIndex deverá ser configurada para `true` e o atributo indexado deverá ser do tipo Comparable. Para o HashIndex de relacionamento e o HashIndex composto, a propriedade RangeIndex deve ser configurada para `false`.

A amostra precedente é um HashIndex de intervalo porque o valor da propriedade RangeIndex é `true`.

A tabela a seguir fornece um resumo do uso do índice de intervalo.

Tabela 18. Suporte para Índice de Intervalo. Define se os tipos de HashIndex suportam o índice de intervalo.

Tipo HashIndex	**Suporta índice de intervalo**
HashIndex de atributo único: chave ou atributo indexado é do tipo Comparable	Sim
HashIndex de atributo único: chave ou atributo indexado não é do tipo Comparable	Não
HashIndex Composto	Não
HashIndex de Relacionamento	Não

Otimização de Consulta com Plug-ins HashIndex

Definir índices pode significativamente melhorar o desempenho da consulta. As consultas do WebSphere eXtreme Scale podem usar plug-insHashIndex integrados para melhorar o desempenho das consultas. Embora o uso de índices possa aprimorar significativamente o desempenho da consulta, isso pode ter um impacto no desempenho nas operações do mapa transacional.

Conceitos relacionados:

Java "Plug-ins para Indexar Dados" na página 580
Dependendo do tipo de índices que você deseja construir, o WebSphere eXtreme Scale fornece plug-ins integrados que podem ser incluídos no BackingMap para construir um índice.

Java "Plug-ins para Indexação Customizada de Objetos de Cache"
Com um plug-in MapIndexPlugin, ou índice, é possível gravar estratégias de indexação customizadas que vão além de índices integrados fornecidos pelo eXtreme Scale.

Java "Usando um Índice Composto" na página 596
O HashIndex composto aprimora o desempenho da consulta e evita a custosa varredura de mapa. O recurso também fornece uma maneira conveniente para a API HashIndex localizar objetos em cache quando os critérios de busca envolvem muitos atributos.

Java "Indexação" na página 280
Use o plug-in MapIndexPlugin para construir um índice ou vários índices em um BackingMap para suportar acesso a dados sem chave.

Java "Utilizando o Índice Global" na página 599
O índice global pode melhorar o desempenho da procura de dados em ambiente particionado grande, por exemplo 100 partições.

"Utilizando o Índice Global" na página 599
O índice global pode melhorar o desempenho da procura de dados em ambiente particionado grande, por exemplo 100 partições.

"Otimização de Consulta do Cliente Utilizando Índices Globais" na página 759
Ao executar consultas a partir do ObjectGrid do cliente, é necessário configurar a partição se os mapas envolvidos são particionados. Em um grande ambiente do ObjectGrid particionado, o aplicativo geralmente precisa executar consultas paralelas simultaneamente em todas as partições para obter o resultado da consulta completo. Por exemplo, se houver 100 partições, o aplicativo deverá executar a mesma consulta em todas as 100 partições e mesclar os resultados da consulta para obter o resultado da consulta completo. Isto geralmente consome grandes quantidades de recurso do sistema.

"Ajustando o Desempenho de Consulta" na página 746
Para ajustar o desempenho de suas consultas, utilize as técnicas e dicas a seguir.

Tarefas relacionadas:

Java "Configurando o Plug-in HashIndex" na página 586
É possível configurar o HashIndex integrado, a classe com.ibm.websphere.objectgrid.plugins.index.HashIndex, com um arquivo XML, programaticamente ou com uma anotação de entidade em um mapa de entidade.

Java "Acessando Dados com Índices (API de Índice)" na página 359
Use indexação para acesso a dados mais eficiente.

Plug-ins para Indexação Customizada de Objetos de Cache: Java

Com um plug-in MapIndexPlugin, ou índice, é possível gravar estratégias de indexação customizadas que vão além de índices integrados fornecidos pelo eXtreme Scale.

As implementações MapIndexPlugin devem usar a interface MapIndexPlugin e seguir as convenções comuns do plug-in do eXtreme Scale.

As seções a seguir incluem alguns dos métodos importantes da interface de índice.

Método setProperties

Use o método setProperties para inicializar programaticamente do plug-in de índice. O parâmetro Objeto de propriedades transmitido para o método deve conter as informações necessárias sobre configuração para inicializar o plug-in de índice adequadamente. A implementação do método setProperties, junto com a do método getProperties, são necessárias em um ambiente distribuído pois a configuração do plug-in de índice se move entre os processos do cliente e do servidor. A seguir está um exemplo de implementação deste método.

```
setProperties(Properties properties)

// setProperties method sample code
    public void setProperties(Properties properties) {
        ivIndexProperties = properties;

        String ivRangeIndexString = properties.getProperty("rangeIndex");
        if (ivRangeIndexString != null && ivRangeIndexString.equals("true")) {
            setRangeIndex(true);
        }
        setName(properties.getProperty("indexName"));
        setAttributeName(properties.getProperty("attributeName"));

        String ivFieldAccessAttributeString = properties.getProperty("fieldAccessAttribute");
        if (ivFieldAccessAttributeString != null && ivFieldAccessAttributeString.equals("true")) {
            setFieldAccessAttribute(true);
        }

        String ivPOJOKeyIndexString = properties.getProperty("POJOKeyIndex");
        if (ivPOJOKeyIndexString != null && ivPOJOKeyIndexString.equals("true")) {
            setPOJOKeyIndex(true);
        }
    }
```

Método getProperties

O método getProperties extrai a configuração do plug-in de índice de uma instância MapIndexPlugin. É possível usar as propriedades extraídas para inicializar outra instância do MapIndexPlugin para ter os mesmos estados internos. Os implementações dos métodos getProperties e setProperties são necessárias em um ambiente distribuído. A seguir há um exemplo de implementação do método getProperties.

```
getProperties()

// getProperties method sample code
    public Properties getProperties() {
        Properties p = new Properties();
        p.put("indexName", indexName);
        p.put("attributeName", attributeName);
        p.put("rangeIndex", ivRangeIndex ? "true" : "false");
        p.put("fieldAccessAttribute", ivFieldAccessAttribute ? "true" : "false");
        p.put("POJOKeyIndex", ivPOJOKeyIndex ? "true" : "false");
        return p;
    }
```

Método setEntityMetadata

O método setEntityMetadata é chamado pelo tempo de execução do WebSphere eXtreme Scale durante a inicialização para configurar EntityMetadata do BackingMap associado na instância MapIndexPlugin. O EntityMetadata é necessário para suportar a indexação de objetos de tupla. Uma tupla é um conjunto de dados que representa um objeto da entidade ou sua chave. Se o BackingMap for para uma entidade, então, é necessário implementar este método.

O código de amostra a seguir implementa o método setEntityMetadata.

```
setEntityMetadata(EntityMetadata entityMetadata)

// setEntityMetadata method sample code
    public void setEntityMetadata(EntityMetadata entityMetadata) {
        ivEntityMetadata = entityMetadata;
        if (ivEntityMetadata != null) {
            // este é um mapa de tupla
            TupleMetadata valueMetadata = ivEntityMetadata.getValueMetadata();
            int numAttributes = valueMetadata.getNumAttributes();
            for (int i = 0; i < numAttributes; i++) {
                String tupleAttributeName = valueMetadata.getAttribute(i).getName();
                if (attributeName.equals(tupleAttributeName)) {
                    ivTupleValueIndex = i;
                    break;
                }
            }

            if (ivTupleValueIndex == -1) {
                // did not find the attribute in value tuple, try to find it on key tuple.
                // if found on key tuple, implies key indexing on one of tuple key attributes.
                TupleMetadata keyMetadata = ivEntityMetadata.getKeyMetadata();
                numAttributes = keyMetadata.getNumAttributes();
                for (int i = 0; i < numAttributes; i++) {
                    String tupleAttributeName = keyMetadata.getAttribute(i).getName();
                    if (attributeName.equals(tupleAttributeName)) {
                        ivTupleValueIndex = i;
                        ivKeyTupleAttributeIndex = true;
                        break;
                    }
                }
            }

            if (ivTupleValueIndex == -1) {
                // if entityMetadata is not null and we could not find the
       // attributeName in entityMetadata, this is an
                // error
                throw new ObjectGridRuntimeException("Invalid attributeName.  Entity: " + ivEntityMetadata.getName());
            }
        }
    }
```

Métodos de Nome do Atributo

O método setAttributeName configura o nome do atributo a ser indexado. A classe de objeto de cache deve fornecer o método get para o atributo indexado. Por exemplo, se o objeto possuir um atributo employeeName ou EmployeeName, o índice chama o método getEmployeeName no objeto para extrair o valor de atributo. O nome do atributo deve ser o mesmo nome no método get e o atributo deve implementar a interface Comparable. Se o atributo for do tipo booleano, também é possível utilizar o método padrão isAttributeName.

O método getAttributeName retorna o nome do atributo indexado.

Método getAttribute

O método getAttribute retorna o valor de atributo indexado do objeto especificado. Por exemplo, se um objeto Employee possui um atributo denominado employeeName que é indexado, o método getAttribute pode ser utilizado para extrair o valor de atributo employeeName de um objeto Employee especificado. Este método é necessário em um ambiente WebSphere eXtreme Scale distribuído.

```
getAttribute(Object value)

// getAttribute method sample code
    public Object getAttribute(Object value) throws ObjectGridRuntimeException {
        if (ivPOJOKeyIndex) {
            // In the POJO key indexing case, no need to get attribute from value object.
            // The key itself is the attribute value used to build the index.
            return null;
        }

        try {
            Object attribute = null;
            if (value != null) {
                // handle Tuple value if ivTupleValueIndex != -1
                if (ivTupleValueIndex == -1) {
                    // regular value
                    if (ivFieldAccessAttribute) {
                        attribute = this.getAttributeField(value).get(value);
```

```
                } else {
                    attribute = getAttributeMethod(value).invoke(value, emptyArray);
                }
            } else {
                // Tuple value
                attribute = extractValueFromTuple(value);
            }
        }
        return attribute;
    } catch (InvocationTargetException e) {
        throw new ObjectGridRuntimeException(
                "Caught unexpected Throwable during index update processing, index name = " + indexName + ": " + t,
                t);
    } catch (Throwable t) {
        throw new ObjectGridRuntimeException(
                "Caught unexpected Throwable during index update processing, index name = " + indexName + ": " + t,
                t);
    }
}
```

Tarefas relacionadas:

Java "Configurando o Plug-in HashIndex" na página 586
É possível configurar o HashIndex integrado, a classe com.ibm.websphere.objectgrid.plugins.index.HashIndex, com um arquivo XML, programaticamente ou com uma anotação de entidade em um mapa de entidade.

Java "Acessando Dados com Índices (API de Índice)" na página 359
Use indexação para acesso a dados mais eficiente.

Referências relacionadas:

Java "Atributos do Plug-in HashIndex" na página 589
É possível usar os seguintes atributos para configurar o plug-in HashIndex. Esses atributos definem propriedades, como se você estiver usando um atributo ou HashIndex composto ou se a indexação do intervalo estiver ativada.

Java "Atributos do Plug-in InverseRangeIndex" na página 583
É possível usar os seguintes atributos para configurar o plug-in InverseRangeIndex. Esses atributos definem propriedades sobre como o índice é construído.

Java Interface GlobalIndex

Usando um Índice Composto: Java

O HashIndex composto aprimora o desempenho da consulta e evita a custosa varredura de mapa. O recurso também fornece uma maneira conveniente para a API HashIndex localizar objetos em cache quando os critérios de busca envolvem muitos atributos.

Desempenho Melhorado

Um HashIndex composto fornecer uma maneira rápida e conveniente de buscar objetos em cache com múltiplos atributos em critérios de busca de correspondência. O índice composto suporta todas as buscas de correspondência de atributo, mas não suportam buscas de intervalo.

Nota: Índices compostos não suportam o operador BETWEEN no idioma de consulta do ObjectGrid porque BETWEEN necessitaria de suporte de intervalo. Os condicionais maior que (>) e menor que (<) também não funcionam porque necessitam de índices de intervalo.

Um índice composto pode melhorar o desempenho de consultas se o índice composto apropriado estiver disponível para a condição WHERE. Isso significa que o índice composto tem exatamente os mesmos atributos envolvidos na condição WHERE com atributos integrais correspondidos.

Uma consulta pode ter muitos atributos envolvidos em uma condição como no exemplo a seguir.

```
SELECT a FROM Address a WHERE a.city='Rochester' AND a.state='MN' AND
a.zipcode='55901'
```

O índice composto pode melhorar o desempenho da consulta evitando a varredura de mapa ou unindo vários resultados de índice de atributo único. No exemplo, se o índice composto for definido com atributos (city,state,zipcode), o mecanismo de consulta poderá utilizar o índice composto para localizar a entrada com `city='Rochester'`, `state='MN'` e `zipcode='55901'`. Sem índice composto e índice de atributo nos atributos de cidade, estado e CEP, o mecanismo de consulta deve varrer o mapa ou unir várias procuras de atributo único, que geralmente possuem gasto adicional caro. Além disso, a consulta para o índice composto suporta apenas um padrão totalmente correspondido.

Configurando um Índice Composto

É possível configurar a indexação composta de três maneiras: usando XML, programaticamente, e com anotações de entidade apenas para mapas de entidade.

Configuração Programática

O exemplo a seguir cria um índice composto.

```
HashIndex mapIndex = new HashIndex();
 mapIndex.setName("Address.CityStateZip");
 mapIndex.setAttributeName(("city,state,zipcode"));
 mapIndex.setRangeIndex(false);

 BackingMap bm = objectGrid.defineMap("mymap");
 bm.addMapIndexPlugin(mapIndex);
```

Observe que a configuração de um índice composto é a mesma que a configuração de um índice regular com XML, exceto para o valor da propriedade attributeName. No caso de um índice composto, o valor de attributeName é uma lista de atributos delimitados por vírgulas. Por exemplo, a classe de valor Endereço tem 3 atributos: cidade, estado e código postal. Um índice composto pode ser definido com o valor da propriedade attributeName como `"city,state,zipcode"` indicando a cidade, estado e código postal são incluídos no índice composto.

HashIndexes compostos não suportam consultas de intervalo e, portanto, não podem ter a propriedade RangeIndex configurada como true.

Utilizando XML

Para configurar um índice composto com XML, inclua a configuração a seguir no elemento backingMapPluginCollections no arquivo XML do descritor do ObjectGrid.

```
Composite index - XML configuration approach
<bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
<property name="Name"
type="java.lang.String" value="Address.CityStateZip"/>
<property name="AttributeName"
type="java.lang.String" value="city,state,zipcode"/>
</bean>
```

Com anotações de entidade

No caso do mapa de entidade, a abordagem de anotação pode ser utilizada para definir um índice composto. É possível definir uma lista de CompositeIndex sem a anotaçãoCompositeIndexes no nível da classe de entidade. O CompositeIndex

possui uma propriedade name e attributeNames. Cada CompositeIndex está associado a uma instância HashIndex aplicada ao mapa de apoio que está associado à entidade. O HashIndex é configurado como um índice de não-intervalo.

```
@Entity
@CompositeIndexes({
    @CompositeIndex(name=" CityStateZip ", attributeNames=" city,state,zipcode"),
    @CompositeIndex(name="lastnameBirthday", attributeNames=" lastname,birthday ")
 })
public class Address {
    @Id int id;
    String street;
    String city;
    String state;
    String zipcode;
    String lastname;
    Date birthday;
}
```

A propriedade nomeada para cada índice composto deve ser única dentro da entidade e do BackingMap. Se o nome não for especificado, um nome gerado será usado. A propriedade attributeNames é utilizada para preencher o HashIndex attributeName com a lista de atributos delimitados por vírgulas. Os nomes de atributos coincidem com os nomes de campo persistente quando as entidades são configuradas para usar acesso à campo, ou o nome da propriedade como definida para as convenções de nomenclatura JavaBeans para entidades de acesso à propriedade. Por exemplo: Se o nome do atributo for "street", o método getter da propriedade é denominado getStreet.

Executando Consultas de Índice Composto

Após um índice composto ser configurado, um aplicativo pode usar o método findAll(Object) da interface MapIndex para executar consultas.

```
Session sess = objectgrid.getSession();
ObjectMap map = sess.getMap("MAP_NAME");
MapIndex codeIndex = (MapIndex) map.getIndex("INDEX_NAME");
Object[] compositeValue = new Object[]{ MapIndex.EMPTY_VALUE,
   "MN", "55901"};
Iterator iter = mapIndex.findAll(compositeValue);
// Close the session (optional in Version 7.1.1 and later) for improved performance
sess.close();
```

O MapIndex.EMPTY_VALUE é designado para o compositeValue[0] que indica que o atributo cidade é excluído da avaliação. Somente objetos com atributo de estado igual a `"MN"` e atributo de CEP igual a `"55901"` são incluídos no resultado.

As seguintes consultas se beneficiam da configuração do índice composto anterior:

```
SELECT a FROM Address a WHERE a.city='Rochester' AND a.state='MN' AND
a.zipcode='55901'

SELECT a FROM Address a WHERE a.state='MN' AND a.zipcode='55901'
```

O mecanismo de consulta localiza o índice composto apropriado e o usa para melhorar o desempenho da consulta em casos de correspondência do atributo completa.

Em alguns cenários, o aplicativo pode precisar definir múltiplos índices compostos com atributos sobrepostos para satisfazer todas as consultas com atributos integrais correspondidos. Uma desvantagem de aumentar o número de índices é o possível gasto adicional de desempenho em operações de mapa.

Migração e Interoperabilidade

A única restrição para o uso de um índice composto é que um aplicativo não pode configurá-lo em um ambiente distribuído com contêineres heterogêneos. Servidores de contêiner antigos e novos não podem ser combinados, pois servidores de contêiner mais antigos não reconhecem uma configuração de índice composto. O índice composto é exatamente igual ao índice de atributo regular existente, exceto que o anterior permite a indexação sobre vários atributos. Ao utilizar apenas o índice de atributo regular, um ambiente de contêineres combinados ainda é viável.

Tarefas relacionadas:

Java "Configurando o Plug-in HashIndex" na página 586
É possível configurar o HashIndex integrado, a classe com.ibm.websphere.objectgrid.plugins.index.HashIndex, com um arquivo XML, programaticamente ou com uma anotação de entidade em um mapa de entidade.

Java "Acessando Dados com Índices (API de Índice)" na página 359
Use indexação para acesso a dados mais eficiente.

Referências relacionadas:

Java "Atributos do Plug-in HashIndex" na página 589
É possível usar os seguintes atributos para configurar o plug-in HashIndex. Esses atributos definem propriedades, como se você estiver usando um atributo ou HashIndex composto ou se a indexação do intervalo estiver ativada.

Java "Atributos do Plug-in InverseRangeIndex" na página 583
É possível usar os seguintes atributos para configurar o plug-in InverseRangeIndex. Esses atributos definem propriedades sobre como o índice é construído.

Java Interface GlobalIndex

Utilizando o Índice Global:

O índice global pode melhorar o desempenho da procura de dados em ambiente particionado grande, por exemplo 100 partições.

O recurso também fornece uma maneira de localizar locais de atributos indexados e pode melhorar as operações de agentes ou consultas que estão relacionadas aos atributos indexados. Consulte a documentação da API MapGlobalIndex para obter detalhes de recursos de índice global.

Desempenho Melhorado

No ambiente particionado grande, os objetos armazenados em cache são difundidos em todas as partições. Para ter resultados completos, os índices regulares, consultas e agentes devem ser executados em todas as partições que são dispendiosas. De maneira ideal, essas operações devem ser executadas apenas em partições aplicáveis e, portanto, eliminar o gasto adicional desnecessário. O recurso de índice global pode controlar o local de atributos indexados e pode determinar partições aplicáveis para atributos de todas as partições. Geralmente, as partições aplicáveis são um subconjunto de todas as partições. Portanto, a execução de índices, consultas e agentes em partições aplicáveis é muito mais rápida do que a execução desses itens em todas as partições, mesmo quando há deslocamento pelo índice global.

Procurando Dados

Os aplicativos podem procurar dados com atributos utilizando índices e com as chaves. Tradicionalmente, os aplicativos podem usar um proxy de índice cliente para obter chaves de entrada de todas as partições ou utilizar um agente para fazer uma procura de índice em todas as partições e retornar chaves de cache, valores ou ambos. Com o recurso de índice global, os aplicativos podem localizar as chaves de entrada, os valores, ou ambos, através da API MapGlobalIndex em uma abordagem eficaz que executa operações apenas em partições aplicáveis.

Operação do Agente

Se uma operação do agente está relacionada aos atributos indexados, por exemplo, invalidando entradas utilizando atributos indexados, os aplicativos podem utilizar o índice global para localizar partições aplicáveis por atributos primeiro. Em seguida, o aplicativo pode enviar o agente para essas partições aplicáveis. Use o método MapGlobalIndex.findPartitions() para localizar partições aplicáveis usando atributos.

Operação de Consulta do Cliente

Ao executar consultas do cliente, você deve configurar partições. Geralmente, o aplicativo deve executar a mesma consulta em todas as partições para obter resultados da consulta completos. Com o recurso de índice global, os aplicativos podem utilizar o método MapGlobalIndex.findPartitions() para localizar partições aplicáveis utilizando atributos que estão em predicados de igualdade de consulta. Em seguida, é possível executar a consulta nestas partições aplicáveis.

Ativando o Índice Global

O índice global é uma extensão do plug-in HashIndex e pode ser ativado em qualquer configuração do HashIndex existente. Utilizando a configuração de XML como um exemplo, configurar a propriedade GlobalIndexEnabled do plug-in HashIndex como `true` ativa o índice global nesse plug-in HashIndex.

```
<bean id="MapIndexPlugin"
      className="com.ibm.websphere.objectgrid.plugins.index.HashIndex">
         <property name="Name"
type="java.lang.String" value="CODE"
            description="index name" />
         <property name="AttributeName"
type="java.lang.String" value="employeeCode" description="attribute name" />
  <property name="GlobalIndexEnabled" type="boolean" value="true"
            description="true for global index" />
   </bean>
```

Executando Consultas de Índice Global

A função de índice global está definida na API MapGlobalIndex. Depois que o índice global está ativado em um plug-in HashIndex, o aplicativo pode lançar um proxy do índice obtido para o tipo de MapGlobalIndex e começar a utilizá-lo.

```
// in client ObjectGrid process
MapGlobalIndex mapGlobalIndexCODE = (MapGlobalIndex)m.getIndex("CODE", false);
Object[] attributes = new Object[] {new Integer(1)};
Collection partitions = mapGlobalIndexCODE.findPartitions(attributes);
Set keys = mapGlobalIndexDependency.findKeys(attributes);
Set values = mapGlobalIndexDependency.findValues(attributes);
Map entries = mapGlobalIndexDependency.findEntries(attributes);
```

Migração e Interoperabilidade

A única restrição para o uso de um índice global é que um aplicativo não pode configurá-lo em um ambiente distribuído com contêineres heterogêneos. Servidores de contêiner antigos e novos não podem ser combinados, pois servidores de contêiner mais antigos não reconhecem uma configuração de índice global.

Para utilizar o índice global, você deve parar todos os servidores de contêiner e clientes para um aplicativo primeiro. Em seguida, ative o índice global na configuração de HashIndex e reinicie os servidores de contêiner e clientes.

Tarefas relacionadas:

Java "Configurando o Plug-in HashIndex" na página 586
É possível configurar o HashIndex integrado, a classe com.ibm.websphere.objectgrid.plugins.index.HashIndex, com um arquivo XML, programaticamente ou com uma anotação de entidade em um mapa de entidade.

Java "Acessando Dados com Índices (API de Índice)" na página 359
Use indexação para acesso a dados mais eficiente.

Referências relacionadas:

Java "Atributos do Plug-in HashIndex" na página 589
É possível usar os seguintes atributos para configurar o plug-in HashIndex. Esses atributos definem propriedades, como se você estiver usando um atributo ou HashIndex composto ou se a indexação do intervalo estiver ativada.

Java "Atributos do Plug-in InverseRangeIndex" na página 583
É possível usar os seguintes atributos para configurar o plug-in InverseRangeIndex. Esses atributos definem propriedades sobre como o índice é construído.

Java Interface GlobalIndex

Plug-ins para a Comunicação com os Bancos de Dados

Java

Com um plug-in Loader, um mapa ObjectGrid pode se comportar como um cache de memória para dados que são normalmente mantidos em um armazenamento persistente no mesmo sistema ou em algum outro sistema. Geralmente, um banco de dados ou sistema de arquivos é utilizado como o armazenamento persistente. Uma JVM (Java Virtual Machine) também pode ser usada como a origem de dados, permitindo que caches baseados em hub sejam construídos usando ObjectGrid. Um utilitário de carga possui a lógica para leitura e gravação de dados para um armazenamento persistente e a partir dele.

Os utilitários de carga são plug-ins de mapa de apoio que são chamados quando são feitas alterações no mapa de apoio ou quando o mapa de apoio não pode atender a um pedido de dados (um erro de cache).

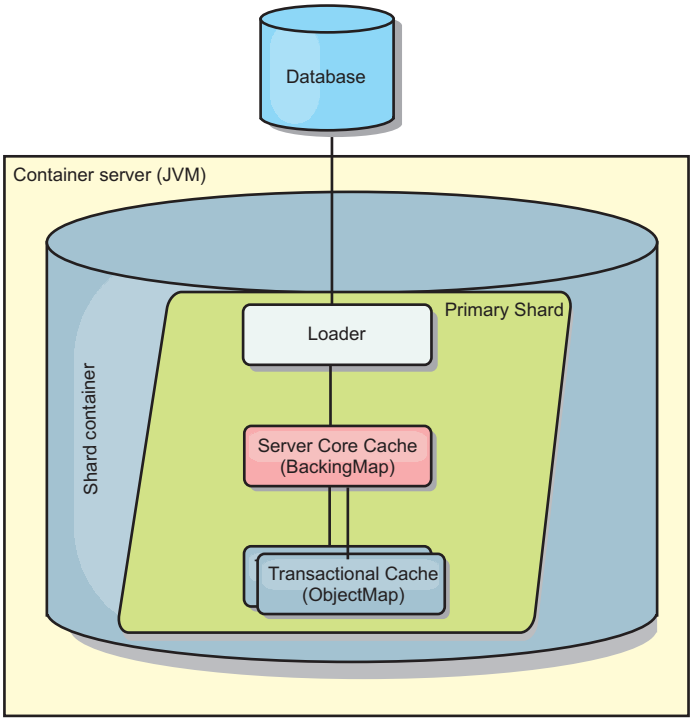


Figura 40. Utilitário de Carga

O WebSphere eXtreme Scale inclui dois utilitários de carga integrados para interagir com os backends de banco de dados relacional. Os utilitários de carga Java Persistence API (JPA) utilizam os recursos Object-Relational Mapping (ORM) das duas implementações OpenJPA e Hibernate da especificação JPA.

Utilizando um Utilitário de Carga

Para incluir um utilitário de carga na configuração do BackingMap, é possível utilizar a configuração programática ou a configuração do XML. Um utilitário de carga possui o seguinte relacionamento com um mapa de apoio:

- Um mapa de apoio pode ter apenas um utilitário de carga.
- Um mapa de apoio de cliente (cache local) não pode ter um utilitário de carga.
- Uma definição de utilitário de carga pode ser aplicado a múltiplos mapas de apoio, mas cada mapa de apoio possui sua própria instância do utilitário de carga.

Restrição: BackMaps configurados com um plug-in Loader podem ler mas não podem gravar no mapa em uma transação com diversas partições.

Carregadores em Configurações Multimestre

Para obter considerações sobre como usar os carregadores em configurações multimestre, consulte “Considerações Sobre o Carregador em uma Topologia Multimestre” na página 289.

Conectando um Utilitário de Carga Programaticamente

O trecho de código a seguir demonstra como conectar o Utilitário de Carga fornecido pelo aplicativo ao mapa de apoio para map1, por meio da API do ObjectGrid:

```
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
import com.ibm.websphere.objectgrid.ObjectGridManager;
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.BackingMap;
ObjectGridManager ogManager = ObjectGridManagerFactory.getObjectGridManager();
ObjectGrid og = ogManager.createObjectGrid("grid");
BackingMap bm = og.defineMap( "map1" );
MyLoader loader = new MyLoader();
loader.setDataBaseName("testdb");
loader.setIsolationLevel("read committed");
bm.setLoader( loader );
```

Este fragmento assume que a classe MyLoader é a classe fornecida pelo aplicativo que implementa a interface com.ibm.websphere.objectgrid.plugins.Loader. Como a associação de um Utilitário de Carga com um mapa de apoio não pode ser alterada após a inicialização de um ObjectGrid, o código deverá ser executado antes de chamar o método initialize da interface ObjectGrid que está sendo chamada. Uma exceção IllegalStateException ocorre em uma chamada de método setLoader se ela for chamada depois de a inicialização ocorrer.

O Utilitário de Carga fornecido pelo aplicativo pode ter propriedades configuradas. No exemplo, o utilitário de carga MyLoader é utilizado para ler e gravar dados de uma tabela em um banco de dados relacional. O utilitário de carga deve especificar o nome do banco de dados e o nível de isolamento do SQL. O loader MyLoader possui os métodos setDataBaseName e setIsolationLevel que permitem que o aplicativo configure estas duas propriedades do Loader.

Abordagem da Configuração XML para Conectar um Utilitário de Carga

Um Utilitário de Carga fornecido pelo aplicativo também pode ser conectado utilizando um arquivo XML. O exemplo a seguir demonstra como conectar o carregador MyLoader ao mapa de apoio map1 com o mesmo nome de banco de dados e propriedades do Carregador de nível de isolamento. É necessário especificar o className para seu utilitário de carga, os detalhes de nome e conexão do banco de dados e as propriedades do nível de isolamento. A mesma estrutura XML poderá ser usada se você estiver usando apenas um pré-carregador ao especificar o nome da classe do pré-carregador em vez de um nome da classe do carregador completo:

```
<?xml version="1.0" encoding="UTF-8" ?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">
<objectGrids>
    <objectGrid name="grid">
        <backingMap name="map1" pluginCollectionRef="map1"
" lockStrategy="OPTIMISTIC" />
    </objectGrid>
</objectGrids>
<backingMapPluginCollections>
    <backingMapPluginCollection id="map1">
        <bean id="Loader" className="com.myapplication.MyLoader">
            <property name="dataBaseName"
                      type="java.lang.String"
                      value="testdb"
                      description="database name" />
            <property name="isolationLevel"
                      type="java.lang.String"
                      value="read committed"
                      description="iso level" />
        </bean>
    </backingMapPluginCollection>
</backingMapPluginCollections>
</objectGridConfig>
```

Referências relacionadas:

Java "Considerações sobre a Programação do Utilitário de Carga do JPA" na página 628
Um Utilitário de Carga do Java Persistence API (JPA) é uma implementação do plug-in do utilitário de carga que usa o JPA para interagir com o banco de dados. Use as seguintes considerações ao desenvolver um aplicativo que usa um utilitário de carga do JPA.

Configurando Carregadores de Banco de Dados: Java

Os utilitários de carga são plug-ins de mapa de apoio que são chamados quando são feitas alterações no mapa de apoio ou quando o mapa de apoio não pode atender a um pedido de dados (um erro de cache).

Considerações sobre Pré-carregamento

Os utilitários de carga são plug-ins de mapa de apoio que são chamados quando são feitas alterações no mapa de apoio ou quando o mapa de apoio não pode atender a um pedido de dados (um erro de cache). Para obter uma visão geral de como o eXtreme Scale interage com um carregador, consulte o "Cache Sequencial" na página 268.

Cada mapa de apoio tem um atributo preloadMode booleano que é configurado para indicar se o pré-carregamento de um mapa é executado de forma assíncrona. Por padrão, o atributo preloadMode está configurado como false, o que indica que a inicialização do mapa de suporte não será concluída até que o pré-carregamento do mapa esteja concluído. Por exemplo, a inicialização do mapa de apoio não será concluída até que o método preloadMap seja retornado. Se o método preloadMap ler uma grande quantidade de dados no seu back end e carregá-los para o mapa, o tempo de conclusão desse procedimento pode ser relativamente longo. Neste caso, é possível configurar um mapa de suporte para utilizar o pré-carregamento assíncrono do mapa, configurando o atributo preloadMode como true. Essa configuração faz com que o código de inicialização do mapa de apoio inicie um encadeamento que chama o método preloadMap, permitindo que a inicialização de um mapa de apoio seja concluída enquanto o pré-carregamento do mapa ainda está em andamento.

Em um cenário eXtreme Scale distribuído, um dos padrões de pré-carregamento é o pré-carregamento de cliente. No padrão de pré-carregamento do cliente, um cliente eXtreme Scale é responsável por recuperar dados do backend e, em seguida, inserir os dados no servidor de contêiner distribuído usando agentes DataGrid. Além disso, o pré-carregamento de cliente poderia ser executado no método Loader.preloadMap em uma, e apenas uma, partição específica. Nesse caso, o carregamento assíncrono de dados para a grade se tornaria muito importante. Se o pré-carregamento do cliente fosse executado no mesmo encadeamento, o mapa de apoio nunca seria inicializado, assim, a partição na qual ele reside nunca ficaria ON-LINE. Portanto, o cliente eXtreme Scale não poderia enviar o pedido para a partição e, eventualmente, isso causaria uma exceção.

Se um cliente do eXtreme Scale for usado no método preloadMap, você deverá definir o atributo **preloadMode** como true. A alternativa é iniciar um encadeamento no código de pré-carregamento do cliente.

O trecho de código a seguir ilustra como o atributo preloadMode é configurado para ativar o pré-carregamento assíncrono:

```
BackingMap bm = og.defineMap( "map1" );
bm.setPreloadMode( true );
```

O atributo preloadMode também pode ser configurado utilizando um arquivo XML conforme ilustrado no seguinte exemplo:

```
<backingMap name="map1" preloadMode="true" pluginCollectionRef="map1"
" lockStrategy="OPTIMISTIC" />
```

TxID e Utilização da Interface TransactionCallback

Tanto o método get quanto o método batchUpdate na interface do Loader são transmitidos para um objeto TxID que representa a transação Session que requer que a operação get ou batchUpdate seja executada. Os métodos get e batchUpdate podem ser chamados mais de uma vez por transação. Portanto, os objetos com escopo definido pela transação requeridos pelo Loader geralmente são mantidos em um slot do objeto TxID. Um utilitário de carga JDBC (Java Database Connectivity) é usado para ilustrar como um utilitário de carga usa as interfaces TxID e TransactionCallback.

Vários mapas do ObjectGrid podem ser armazenados no mesmo banco de dados. Cada mapa possui seu próprio carregador, e cada carregador pode precisar se conectar ao mesmo banco de dados. Quando os carregadores se conectam com o banco de dados, eles devem usar a mesma conexão JDBC. Usar a mesma conexão confirma as mudanças em cada tabela como parte da mesma transação do banco de dados. Geralmente, a mesma pessoa que grava a implementação Loader também grava a implementação TransactionCallback. O melhor método é quando a interface TransactionCallback é estendida para incluir os métodos que o Loader precisa para obter uma conexão com o banco de dados e para armazenar em cache as instruções preparadas. O motivo para esta metodologia torna-se aparente à medida que você visualiza como as interfaces TransactionCallback e TxID são utilizadas pelo utilitário de carga.

Como um exemplo, o utilitário de carga pode precisar da interface TransactionCallback para ser estendido conforme a seguir:

```
import java.sql.Connection;
import java.sql.PreparedStatement;
import java.sql.SQLException;
import com.ibm.websphere.objectgrid.TxID;
public interface MyTransactionCallback extends TransactionCallback
{
    Connection getAutoCommitConnection(TxID tx, String databaseName) throws SQLException;
    Connection getConnection(TxID tx, String databaseName, int isolationLevel ) throws SQLException;
    PreparedStatement getPreparedStatement(TxID tx, Connection conn, String tableName, String sql)
   throws SQLException;
    Collection getPreparedStatementCollection( TxID tx, Connection conn,  String tableName );
}
```

Com tais novos métodos, os métodos get e batchUpdate do Loader podem obter uma conexão da seguinte forma:

```
import java.sql.Connection;
import java.sql.PreparedStatement;
import java.sql.SQLException;
import com.ibm.websphere.objectgrid.TxID;
private Connection getConnection(TxID tx, int isolationLevel)
{
    Connection conn = ivTcb.getConnection(tx, databaseName, isolationLevel );
    return conn;
}
```

No exemplo anterior e nos exemplos que seguem, vTcb e ivOcb são variáveis da instância do Carregador que foram inicializadas conforme descrito na seção Considerações de Pré-carregamento. A variável ivTcb é uma referência à instância

MyTransactionCallback e ivOcb é uma referência à instância MyOptimisticCallback. A variável databaseName é uma variável da instância do Utilitário de Carga que foi configurada como uma propriedade do Utilitário de Carga durante a inicialização do mapa de suporte. O argumento isolationLevel é uma das constantes da Conexão JDBC que estão definidas para os diversos níveis de isolamento suportados pelo JDBC. Se o Utilitário de Carga estiver utilizando uma implementação otimista, o método get geralmente utilizará uma conexão de autoconfirmação JDBC para buscar os dados do banco de dados. Nesse caso, o Utilitário de Carga pode ter um método getAutoCommitConnection que seja implementado da seguinte forma:

```
import java.sql.Connection;
import java.sql.PreparedStatement;
import java.sql.SQLException;
import com.ibm.websphere.objectgrid.TxID;
private Connection getAutoCommitConnection(TxID tx)
{
    Connection conn = ivTcb.getAutoCommitConnection(tx, databaseName);
    return conn;
}
```

Lembre-se de que o método batchUpdate possui a seguinte instrução switch:

```
switch ( logElement.getType().getCode() )
{
    case LogElement.CODE_INSERT:
        buildBatchSQLInsert( tx, key, value, conn );
        break;
    case LogElement.CODE_UPDATE:
        buildBatchSQLUpdate( tx, key, value, conn );
        break;
    case LogElement.CODE_DELETE:
        buildBatchSQLDelete( tx, key, conn );
        break;
}
```

Cada um dos métodos buildBatchSQL utiliza a interface MyTransactionCallback para obter uma instrução preparada. Este é um trecho de código que mostra o método buildBatchSQLUpdate construindo uma instrução SQL update para atualizar uma entrada EmployeeRecord e incluindo-a na atualização de batch:

```
private void buildBatchSQLUpdate( TxID tx, Object key, Object value, Connection conn )
throws SQLException, LoaderException
{
    String sql = "update EMPLOYEE set LASTNAME = ?, FIRSTNAME = ?, DEPTNO = ?,
    SEQNO = ?, MGRNO = ? where EMPNO = ?";
    PreparedStatement sqlUpdate = ivTcb.getPreparedStatement( tx, conn,
   "employee", sql );
    EmployeeRecord emp = (EmployeeRecord) value;
    sqlUpdate.setString(1, emp.getLastName());
    sqlUpdate.setString(2, emp.getFirstName());
    sqlUpdate.setString(3, emp.getDepartmentName());
    sqlUpdate.setLong(4, emp.getSequenceNumber());
    sqlUpdate.setInt(5, emp.getManagerNumber());
    sqlUpdate.setInt(6, key);
    sqlUpdate.addBatch();
}
```

Quando o loop batchUpdate tiver construído todas as instruções preparadas, ele chamará o método getPreparedStatementCollection. Esse método é implementado como segue:

```
private Collection getPreparedStatementCollection( TxID tx, Connection conn )
{
    return ( ivTcb.getPreparedStatementCollection( tx, conn, "employee" ) );
}
```

Quando o aplicativo chama o método commit no objeto Session, o código do Session chamará o método commit, no método TransactionCallback, depois de enviar todas as alterações feitas pela transação fora do Utilitário de Carga para cada mapa alterado pela transação. Como todos os Loaders utilizaram o método MyTransactionCallback para obter todas as conexões e instruções preparadas necessárias, o método TransactionCallback sabe qual conexão utilizar para solicitar que o back end confirme as alterações. Portanto, estender a interface TransactionCallback com métodos requeridos por cada um dos Loaders tem as seguintes vantagens:

- O objeto TransactionCallback encapsula a utilização de slots TxID para dados com escopo definido pela transação e o Loader não requer informações sobre os slots TxID. O Loader apenas precisa saber sobre os métodos que foram incluídos no TransactionCallback utilizando a interface MyTransactionCallback para as funções de suporte requeridas pelo Loader.
- O objeto TransactionCallback pode assegurar que o compartilhamento da conexão ocorra entre cada Loader que se conecta ao mesmo backend para que um protocolo de confirmação de duas fases seja evitado.
- O objeto TransactionCallback pode assegurar que a conexão com o backend seja orientada para conclusão por meio de uma confirmação ou rollback chamado na conexão quando apropriado.
- O TransactionCallback garante a limpeza dos recursos do banco de dados após a conclusão de uma transação.
- O TransactionCallback fica oculto se ele estiver obtendo uma conexão gerenciada a partir de um ambiente gerenciado como WebSphere Application Server ou algum outro servidor de aplicativos compatível com Java 2 Platform, Enterprise Edition (J2EE). Esta vantagem permite que o mesmo código do Loader seja utilizado em ambientes gerenciados e não gerenciados. Apenas o plug-in TransactionCallback deve ser alterado.
- Para obter informações detalhadas sobre como a implementação do TransactionCallback utiliza os slots TxID para dados dentro do escopo da transação, consulte Plug-in do TransactionCallback.

OptimisticCallback

Conforme mencionado anteriormente, o Utilitário de Carga pode utilizar uma abordagem otimista para controle de simultaneidade. Nesse caso, o exemplo do método buildBatchSQLUpdate precisará ser modificado ligeiramente para implementar uma abordagem otimista. Existem várias maneiras possíveis para utilizar uma abordagem otimista. Uma maneira típica é ter uma coluna de time stamp ou uma coluna do contador de números de sequência para o controle de versões de cada atualização da linha. Suponha que a tabela de funcionários tenha uma coluna de números de sequência que aumenta sempre que a linha é atualizada. Em seguida, você modifica a assinatura do método buildBatchSQLUpdate para que ela seja transmitida para o objeto LogElement em vez do par chave e valor. Ele também precisa utilizar o objeto OptimisticCallback que está conectado ao mapa de suporte para obter o objeto da versão inicial e para atualizar o objeto da versão. Este é um exemplo de método buildBatchSQLUpdate modificado que utiliza a variável da instância ivOcb inicializada conforme descrito na seção preloadMap:

exemplo de código do método batch-update modificado

```
private void buildBatchSQLUpdate( TxID tx, LogElement le, Connection conn )
 throws SQLException, LoaderException
{
    // Obter o objeto da versão inicial quando esta entrada do mapa foi lida
 pela última vez ou
    // atualizada no banco de dados.
    Employee emp = (Employee) le.getCurrentValue();
    long initialVersion = ((Long) le.getVersionedValue()).longValue();
    // Obter o objeto da versão de Employee atualizado para a operação SQL
    //update.
    Long currentVersion = (Long)ivOcb.getVersionedObjectForValue( emp );
    long nextVersion = currentVersion.longValue();
    // Agora construa o SQL update que inclui o objeto de versão na cláusula where
    // para verificação otimista.
    String sql = "update EMPLOYEE set LASTNAME = ?, FIRSTNAME = ?,
    DEPTNO = ?,SEQNO = ?, MGRNO = ? where EMPNO = ? and SEQNO = ?";
    PreparedStatement sqlUpdate = ivTcb.getPreparedStatement( tx, conn,
   "employee", sql );
    sqlUpdate.setString(1, emp.getLastName());
    sqlUpdate.setString(2, emp.getFirstName());
    sqlUpdate.setString(3, emp.getDepartmentName());
    sqlUpdate.setLong(4, nextVersion );
    sqlUpdate.setInt(5, emp.getManagerNumber());
    sqlUpdate.setInt(6, key);
    sqlUpdate.setLong(7, initialVersion);
    sqlUpdate.addBatch();
}
```

O exemplo mostra que o LogElement é utilizado para obter o valor de versão inicial. Quando a transação acessa pela primeira vez a entrada do mapa, é criado um LogElement com o objeto Employee inicial obtido do mapa. O objeto Employee inicial também é transmitido para o método getVersionedObjectForValue na interface OptimisticCallback e o resultado é salvo no LogElement. Este processamento ocorre antes de um aplicativo receber uma referência ao objeto Employee inicial e de chamar algum método que altere o estado do objeto Employee inicial.

O exemplo mostra que o Loader utiliza o método getVersiondObjectForValue para obter o objeto de versão para o objeto Employee atual atualizado. Antes de chamar o método batchUpdate na interface do utilitário de carga, eXtreme Scale chama o método updateVersionedObjectForValue na interface OptimisticCallback para gerar um novo objeto de versão a ser gerado para o objeto Employee atualizado. Quando o método batchUpdate retornar ao ObjectGrid, o LogElement será atualizado com o objeto de versão atual e se tornará o novo objeto de versão inicial. Esta etapa é necessária porque o aplicativo pode ter chamado o método flush no mapa em vez do método commit na Session. É possível que o Loader seja chamado várias vezes por uma única transação para a mesma chave. Por este motivo, o eXtreme Scale assegura que o LogElement seja atualizado com o novo objeto de versão toda vez que a linha for atualizada na tabela de funcionários.

Agora que o Utilitário de Carga tem o objeto de versão inicial e o próximo objeto de versão, ele pode executar uma instrução SQL update que configura a coluna SEQNO para o próximo valor do objeto de versão e utiliza o valor do objeto de versão inicial na cláusula where. Essa abordagem, às vezes, é referida como uma instrução update super qualificada. A utilização da instrução update super qualificada permite que o banco de dados relacional verifique se a linha não foi alterada por alguma outra transação entre o tempo de leitura do banco de dados por parte da transação e o momento em que esta o atualizou. Se outra transação modificou a linha, a matriz de contagem retornada pela atualização de batch indica que zero linhas foram atualizadas para esta chave. O Utilitário de Carga é

responsável por verificar se a operação SQL update atualizou a linha. Se isso não ocorreu, ele exibirá uma exceção com.ibm.websphere.objectgrid.plugins. OptimisticCollisionException para informar o objeto Session que o método batchUpdate falhou porque mais de uma transação simultânea está tentando atualizar a mesma linha na tabela de banco de dados. Esta exceção faz a Session efetuar rollback e o aplicativo deve tentar novamente a transação inteira. O fundamento lógico é que a nova tentativa será bem-sucedida, motivo pelo qual esta abordagem é chamada de otimista. A abordagem otimista apresenta um desempenho melhor quando os dados não sofrem alterações frequentes ou transações simultâneas raramente tentam atualizar a mesma linha.

É importante que o Utilitário de Carga utilize o parâmetro key do construtor OptimisticCollisionException para identificar qual chave ou conjunto de chaves causou a falha do método batchUpdate otimista. O parâmetro de chave pode ser o próprio objeto de chave ou uma matriz de objetos de chave se mais de uma chave resultar em uma falha de atualização otimista. E o eXtreme Scale usa o método getKey do construtor
OptimisticCollisionException para determinar quais entradas de mapa contêm dados desatualizados e causaram a exceção. Parte do processamento de rollback é liberar cada entrada do mapa stale do mapa. A liberação de entradas stale é necessária para que qualquer transação subsequente que acessa a mesma chave ou chaves resulte no método get da interface do Loader que está sendo chamada para atualizar as entradas do mapa com os dados atuais do banco de dados.

Outras maneiras para um Loader implementar uma abordagem otimista incluem:

- Não existe nenhuma coluna de time stamp ou de número de sequência. Neste caso, o método getVersionObjectForValue na interface OptimisticCallback apenas retorna o próprio objeto de valor como a versão. Com essa abordagem, o Utilitário de Carga precisa construir uma cláusula WHERE que inclua cada um dos campos do objeto de versão inicial. Essa abordagem não é eficiente e nem todos os tipos de colunas estão qualificados para serem utilizados na cláusula WHERE de uma instrução SQL update super qualificada. Esta abordagem geralmente não é utilizada.
- Não existe nenhuma coluna de time stamp ou de número de sequência. No entanto, diferente da abordagem anterior, a cláusula WHERE contém apenas os campos de valores modificados pela transação. Um método para detectar quais campos foram modificados é configurar o modo de cópia no mapa de suporte como CopyMode.COPY_ON_WRITE. Esse modo de cópia requer que uma interface de valor seja transmitida para o método setCopyMode na interface BackingMap. O BackingMap cria objetos de proxy dinâmicos que implementam a interface de valor fornecida. Com este modo de cópia, o Loader pode lançar cada valor em um objeto com.ibm.websphere.objectgrid.plugins.ValueProxyInfo. A interface ValueProxyInfo possui um método que permite que o Loader obtenha a Lista de nomes de atributos que foram alterados pela transação. Esse método permite que o Utilitário de Carga chame os métodos get na interface de valor para os nomes de atributos a fim de obter os dados alterados e construa uma instrução SQL update que configure apenas os atributos alterados. A cláusula WHERE agora pode ser construída de modo a ter a coluna-chave primária e cada uma das colunas de atributos alteradas. Esta abordagem é mais eficiente do que a abordagem anterior, mas requer que mais código seja gravado no Loader e gera a possibilidade de que o cache de instrução preparado precise ser maior para manipular as diferentes permutações. No entanto, se as transações geralmente modificarem apenas alguns dos atributos, esta limitação pode não ser um problema.

- Alguns bancos de dados relacionais podem ter uma API para ajudar na manutenção automática de dados da coluna que são úteis para o controle de versões otimista. Consulte a documentação do banco de dados para determinar se existe esta possibilidade.

Criando um Utilitário de Carga: Java

É possível gravar sua própria implementação de plug-in de utilitário de carga em seus aplicativos, que deve seguir as convenções de plug-in do WebSphere eXtreme Scale comuns.

Incluindo um Plug-in do Utilitário de Carga

A interface do Utilitário de Carga possui a seguinte definição:

```
public interface Loader
{
    static final SpecialValue KEY_NOT_FOUND;
    List get(TxID txid, List keyList, boolean forUpdate) throws LoaderException;
    void batchUpdate(TxID txid, LogSequence sequence) throws LoaderException,
OptimisticCollisionException;
    void preloadMap(Session session, BackingMap backingMap) throws LoaderException;
}
```

Consulte o “Utilitários de Carga” na página 273 para obter informações adicionais.

Método get

O mapa de apoio chama o método get do utilitário de carga para obter os valores associados a uma lista de chaves, que é transmitida como o argumento keyList. O método get é necessário para retornar uma lista de valores java.lang.util.List, um valor para cada chave que estiver na lista de chaves. O primeiro valor retornado na lista de valores corresponde à primeira chave na lista de chaves, o segundo valor retornado na lista de valores corresponde à segunda chave na lista de chaves e assim por diante. Se o utilitário de carga não localizar o valor para uma chave na lista de chaves, ele precisará retornar o objeto de valor especial KEY_NOT_FOUND definido na interface do Utilitário de Carga. Como um mapa de apoio pode ser configurado para permitir `null` como um valor válido, é muito importante para o utilitário de carga retornar o objeto especial KEY_NOT_FOUND quando ele não puder localizar a chave. Este valor especial permite que o mapa de apoio faça a distinção entre um valor null e um valor inexistente porque a chave não foi localizada. Se um mapa de suporte não suportar valores null, um utilitário de carga que retorna um valor nulo em vez do objeto KEY_NOT_FOUND para uma chave que não existe resultará em uma exceção.

O argumento forUpdate informa o utilitário de carga se o aplicativo chamou um método get no mapa ou um método getForUpdate no mapa. Consulte a Interface ObjectMap para obter mais informações. O Loader é responsável por implementar uma política de controle de simultaneidade que controla o acesso simultâneo ao armazenamento persistente. Por exemplo, muitos sistemas de gerenciamento de banco de dados relacional suportam a sintaxe for update na instrução SQL select utilizada para ler dados a partir de uma tabela relacional. O utilitário de carga pode optar por utilizar a sintaxe for update na instrução SQL select com base se um `true` `booleano` foi transmitido como o valor de argumento para o parâmetro forUpdate deste método. Geralmente, o Utilitário de Carga utiliza a sintaxe for update apenas quando a política de controle de simultaneidade pessimista for utilizada. Para um controle de simultaneidade otimista, o Utilitário de Carga nunca utiliza a sintaxe `for update` na instrução SQL select. O utilitário de carga é responsável por decidir utilizar o argumento forUpdate com base na política de controle de simultaneidade que está sendo utilizada pelo utilitário de carga.

Para obter uma explicação do parâmetro txid, consulte “Plug-ins para o Gerenciamento de Eventos de Ciclo de Vida da Transação” na página 644.

Método batchUpdate

O método batchUpdate é importante na interface Loader. Este método é chamado sempre que o eXtreme Scale precisa aplicar todas as alterações atuais no Utilitário de Carga. O Utilitário de Carga recebe uma lista de alterações para o Mapa selecionado. As alterações são iteradas e aplicadas ao backend. O método recebe o valor TxID atual e as alterações a serem aplicadas. A amostra a seguir interage sobre o conjunto de alterações e três instruções JDBC (Java Database Connectivity) em lote, uma com insert, outra com update e uma com delete.

```
import java.util.Collection;
import java.util.Map;
import java.sql.PreparedStatement;
import java.sql.SQLException;
import com.ibm.websphere.objectgrid.TxID;
import com.ibm.websphere.objectgrid.plugins.Loader;
import com.ibm.websphere.objectgrid.plugins.LoaderException;
import com.ibm.websphere.objectgrid.plugins.LogElement;
import com.ibm.websphere.objectgrid.plugins.LogSequence;

    public void batchUpdate(TxID tx, LogSequence sequence) throws LoaderException {
        // Obter uma conexão SQL para utilizar.
        Connection conn = getConnection(tx);
        try {
            // Processar a lista de alterações e construir um conjunto de instruções preparadas
            // para executar uma operação SQL update, insert ou delete
            // de batch.
            Iterator iter = sequence.getPendingChanges();
            while (iter.hasNext()) {
                LogElement logElement = (LogElement)iter.next();
                Object key = logElement.getKey();
                Object value = logElement.getCurrentValue();
                switch (logElement.getType().getCode()) {
                case LogElement.CODE_INSERT:
                    buildBatchSQLInsert( tx, key, value, conn );
                    break;
                case LogElement.CODE_UPDATE:
                    buildBatchSQLUpdate( tx, key, value, conn );
                    break;
                case LogElement.CODE_DELETE:
                    buildBatchSQLDelete( tx, key, conn );
                    break;
                }
            }
            // Executar as instruções de batch que foram construídas pelo loop acima.
            Collection statements = getPreparedStatementCollection( tx, conn );
            iter = statements.iterator();
            while (iter.hasNext()) {
                PreparedStatement pstmt = (PreparedStatement) iter.next();
                pstmt.executeBatch();
            }
        } catch (SQLException e) {
            LoaderException ex = new LoaderException(e);
            throw ex;
        }
    }
```

A amostra anterior ilustra a lógica de alto nível de processamento do argumento LogSequence, mas os detalhes de como uma instrução SQL insert, update ou delete é construída não são ilustrados. Alguns dos pontos-chave que estão ilustrados incluem:

- O método getPendingChanges é chamado no argumento LogSequence para obter um iterador sobre a lista de LogElements que o Utilitário de Carga precisa processar.
- O método LogElement.getType().getCode() é utilizado para determinar se o LogElement serve para uma operação SQL insert, update ou delete.
- Uma exceção SQLException é capturada e encadeada em uma exceção LoaderException exibida para reportar que ocorreu uma exceção durante a atualização do batch.

- O suporte à atualização do batch JDBC é utilizado para reduzir o número de consultas para o backend que devem ser feitas.

Método preloadMap

Durante a inicialização do eXtreme Scale, cada mapa de apoio que é definido é inicializado. Se um Utilitário de Carga for conectado a um mapa de apoio, o mapa de apoio chamará o método preloadMap na interface do Utilitário de Carga para permitir que o utilitário de carga faça a pré-busca de dados de seu backend e carregue os dados no mapa. A amostra a seguir assume que as primeiras 100 linhas de uma tabela Employee são lidas a partir do banco de dados e carregadas no mapa. A classe EmployeeRecord é uma classe fornecida pelo aplicativo que contém os dados de funcionários lidos a partir da tabela de funcionários.

Nota: Essa amostra busca todos os dados do banco de dados e depois os insere no mapa base de uma partição. Em um cenário de implementação do eXtreme Scale distribuído real, os dados devem ser distribuídos em todas as partições. Consulte "Desenvolvendo Carregadores JPA Baseados em Cliente" na página 661 para obter informações adicionais.

```
import java.sql.PreparedStatement;
import java.sql.SQLException;
import com.ibm.websphere.objectgrid.Session;
import com.ibm.websphere.objectgrid.TxID;
import com.ibm.websphere.objectgrid.plugins.Loader;
import com.ibm.websphere.objectgrid.plugins.LoaderException

    public void preloadMap(Session session, BackingMap backingMap) throws LoaderException {
        boolean tranActive = false;
        ResultSet results = null;
        Statement stmt = null;
        Connection conn = null;
        try {
            session.beginNoWriteThrough();
            tranActive = true;
            ObjectMap map = session.getMap( backingMap.getName() );
            TxID tx = session.getTxID();
            // Obter uma conexão de autoconfirmação para utilização que esteja configurada para
            // um nível de isolamento confirmado por leitura.
            conn = getAutoCommitConnection(tx);
            // Pré-carregar o Mapa Employee com objetos EmployeeRecord.
            // Ler todos os Funcionários a partir da tabela, mas
            // limitar o pré-carregamento às primeiras 100 linhas.
            stmt = conn.createStatement();
            results = stmt.executeQuery( SELECT_ALL );
            int rows = 0;
            while (results.next() && rows < 100) {
                int key = results.getInt(EMPNO_INDEX);
                EmployeeRecord emp = new EmployeeRecord( key );
                emp.setLastName( results.getString(LASTNAME_INDEX) );
                emp.setFirstName( results.getString(FIRSTNAME_INDEX) );
                emp.setDepartmentName( results.getString(DEPTNAME_INDEX) );
                emp.updateSequenceNumber( results.getLong(SEQNO_INDEX) );
                emp.setManagerNumber( results.getInt(MGRNO_INDEX) );
                map.put( new Integer(key), emp );
                ++rows;
            }
            // Confirmar a transação.
            session.commit();
            tranActive = false;
        } catch (Throwable t) {
            throw new LoaderException("preload failure: " + t, t);
        } finally {
            if (tranActive) {
                try {
                    session.rollback();
                } catch (Throwable t2) {
                    // Tolerar falhas de rollback e
                    // permitir que o Throwable original seja emitido.
                }
            }
            // Certificar-se de limpar outros recursos do banco de dados aqui,
            // bem como instruções de fechamento, conjuntos de resultados, etc.
        }
    }
```

Esta amostra ilustra os seguintes pontos-chave:

- O mapa de suporte preloadMap utiliza o objeto Session transmitido para ele como o argumento de sessão.
- O método Session.beginNoWriteThrough é utilizado para iniciar a transação em vez do método begin.
- O Utilitário de Carga não pode ser chamado para cada operação put que ocorrer neste método para carregar o mapa.
- O utilitário de carga pode mapear colunas da tabela de funcionários em um campo no objeto Java EmployeeRecord. O Utilitário de Carga captura todas as exceções que podem ser emitidas que ocorrem e emite uma exceção LoaderException com a exceção que pode ser emitida capturada encadeada a ele.
- O bloco finally assegura que qualquer exceção que possa ser emitida, e que ocorre entre o tempo em que os métodos beginNoWriteThrough e commit são chamados, faça o bloco finally recuperar a transação ativa. Esta ação é importante para assegurar que qualquer transação que tenha sido iniciada pelo método preloadMap seja concluída antes de retornar ao responsável pela chamada. O bloco finally é um bom local para você executar outras ações de limpeza que podem ser necessárias, como o fechamento da conexão Java Database Connectivity (JDBC) e de outros objetos JDBC.

A amostra preloadMap está utilizando uma instrução SQL select que seleciona todas as linhas da tabela. Em seu Utilitário de Carga fornecido pelo aplicativo, pode ser necessário configurar uma ou mais propriedades do Utilitário de Carga para controlar a quantidade da tabela que precisa ser pré-carregada no mapa.

Como o método preloadMap é chamado apenas uma vez durante a inicialização de BackingMap, ele também é um bom local para executar o código de inicialização do Utilitário de Carga em uma etapa. Mesmo que o Utilitário de Carga opte por não fazer a pré-busca de dados do backend e carregar os dados no mapa, provavelmente, ele precisará desempenhar alguma outra inicialização em uma etapa para tornar outros métodos do Utilitário de Carga mais eficientes. O exemplo a seguir ilustra o armazenamento em cache do objeto TransactionCallback e do objeto OptimisticCallback como variáveis da instância do Utilitário de Carga para que os outros métodos do Utilitário de Carga não precisem fazer chamadas de método para obter acesso a estes objetos. Este armazenamento em cache de valores de plug-in do ObjectGrid pode ser desempenhado pois, após a inicialização do BackingMap, os objetos TransactionCallback e OptimisticCallback não podem ser alterados ou substituídos. É aceitável armazenar em cache estas referências do objeto como variáveis da instância do Loader.

```
import com.ibm.websphere.objectgrid.Session;
import com.ibm.websphere.objectgrid.BackingMap;
import com.ibm.websphere.objectgrid.plugins.OptimisticCallback;
import com.ibm.websphere.objectgrid.plugins.TransactionCallback;

    // Variáveis da instância do Loader.
    MyTransactionCallback ivTcb; // MyTransactionCallback

    // estende TransactionCallback
    MyOptimisticCallback ivOcb; // MyOptimisticCallback

    // implementa OptimisticCallback
    // ...
    public void preloadMap(Session session, BackingMap backingMap) throws LoaderException [Replication programming]
        // Armazenar em cache os objetos TransactionCallback e OptimisticCallback
        // em variáveis da instância deste Loader.
        ivTcb = (MyTransactionCallback) session.getObjectGrid().getTransactionCallback();
        ivOcb = (MyOptimisticCallback) backingMap.getOptimisticCallback();
        // O restante do código preloadMap (conforme mostrado no exemplo anterior).
    }
```

Para obter informações sobre o pré-carregamento e o pré-carregamento recuperável pertencentes ao failover de replicação, consulte o Replicação para

Disponibilidadeinformações sobre a replicação no *Visão Geral do Produto*.

Utilitários de Carga com Mapas de Entidade

Se o utilitário de carga for conectado a um mapa de entidade, o utilitário de carga deverá lidar com os objetos de tupla. Os objetos de tupla são um formato de dados de entidade especial. O utilitário de carga deve converter os dados entre a tupla e outros formatos de dados. Por exemplo, o método get retorna uma lista de valores que correspondem ao conjunto de chaves que são transmitidas para o método. As chaves transmitidas estão no tipo de Tupla, chamadas de tuplas de chaves. Assumindo que o utilitário de carga mantém o mapa com um banco de dados utilizando JDBC, o método get deve converter cada tupla de chave em uma lista de valores de atributos que corresponda às colunas de chaves primárias da tabela que é mapeada para o mapa de entidade, executar a instrução SELECT com a cláusula WHERE que utiliza os valores de atributos convertidos como critérios para procurar dados no banco de dados e, em seguida, converter os dados retornados em tuplas de valores. O método get obtém dados do banco de dados e converte os dados em tuplas de valores para as tuplas de chaves transmitidas e, em seguida, retorna uma lista de tuplas de valores que corresponde ao conjunto de chaves de tuplas que são transmitidas para o responsável pela chamada. O método get pode executar uma instrução SELECT para procurar todos os dados de uma vez ou executar uma instrução SELECT para cada tupla de chave. Para obter detalhes sobre a programação que mostra como usar o utilitário de carga quando os dados são armazenados usando um gerenciador de entidades, consulte "Utilizando um Utilitário de Carga com Mapas de Entidade e Tuplas" na página 634.

Referências relacionadas:

Java "Considerações sobre a Programação do Utilitário de Carga do JPA" na página 628
Um Utilitário de Carga do Java Persistence API (JPA) é uma implementação do plug-in do utilitário de carga que usa o JPA para interagir com o banco de dados. Use as seguintes considerações ao desenvolver um aplicativo que usa um utilitário de carga do JPA.

Pré-carregamento de Mapa: Java

Mapas podem ser associados aos utilitários de carga. Um utilitário de carga é utilizado para buscar objetos quando eles não podem ser localizados no mapa (uma ocorrência de cache) e também para gravar alterações em um backend quando ocorre o commit de uma transação. Os carregadores também podem ser usados para pré-carregar dados em um mapa. O método preloadMap da interface do Carregador é chamado em cada mapa quando sua partição correspondente no conjunto de mapas se torna um primário. O método preloadMap não é chamado nas réplicas. Ele tenta carregar todos os dados referenciados destinados a partir do backend no mapa utilizando a sessão fornecida. O mapa relevante é identificado pelo argumento BackingMap que é transmitido ao método preloadMap.

```
void preloadMap(Session session, BackingMap backingMap) throws LoaderException;
```

Pré-carregamento no Conjunto de Mapas Particionados

Os mapas podem ser particionados em N partições. Portanto, os mapas podem ser divididos em vários servidores, com cada entrada identifica por uma chave que é armazenada apenas em um destes servidores. Mapas muito grandes podem ser mantidos em uma grade de dados porque o aplicativo não é mais limitado pelo tamanho de heap de um Java Virtual Machine (JVM) único para reter todas as

entradas de um Mapa. Aplicativos que desejam o pré-carregamento com o método preloadMap da interface Loader deve identificar o subconjunto de dados que ele pré-carrega. Sempre existe um número fixo de partições. É possível determinar este número utilizando o seguinte exemplo de código:

```
int numPartitions = backingMap.getPartitionManager().getNumOfPartitions();
int myPartition = backingMap.getPartitionId();
```

Este exemplo de código mostra como um aplicativo pode identificar o subconjunto de dados para pré-carregar a partir do banco de dados. Os aplicativos sempre devem utilizar estes métodos mesmo quando o mapa não é inicialmente particionado. Estes métodos permitem flexibilidade: Se o mapa for posteriormente particionado pelos administradores, então, o utilitário de carga continua a funcionar corretamente.

O aplicativo deve emitir consultas para recuperar o subconjunto *myPartition* a partir do backend. Se um banco de dados for utilizado, então, pode ser mais fácil ter uma coluna com o identificador de partições para um determinado registro, a menos que haja alguma consulta natural que permita que os dados na tabela sejam particionados facilmente.

Consulte o “Gravando um Utilitário de Carga com um Controlador de Pré-carregamento de Réplica” na página 639 para obter um exemplo de como implementar um Carregador para uma grade de dados replicada.

Desempenho

A implementação de pré-carregamento copia dados do backend para o mapa, armazenando vários objetos no mapa em uma única transação. O número ideal de registros a serem armazenados por transação depende de vários fatores, incluindo complexidade e tamanho. Por exemplo, após a transação incluir blocos de mais de 100 entradas, o benefício do desempenho diminui conforme você aumenta o número de entradas. Para determinar o número ideal, comece com 100 entradas e, em seguida, aumente o número até que não sejam mais percebidos ganhos de desempenho. Transações maiores resultam em melhor desempenho de replicação. Lembre-se, apenas o primário executa o código de pré-carregamento. Os dados pré-carregados são replicados do primário para quaisquer réplicas que estão on-line.

Pré-carregando o Conjunto de Mapas

Se o aplicativo usar um conjunto de mapas com diversos mapas, cada mapa terá seu próprio carregador. Cada utilitário de carga possui um método preload. Cada mapa é carregado de forma serial pela grade de dados. Pode ser mais eficiente pré-carregar todos os mapas designando um único mapa como o mapa de pré-carregamento. Esse processo é uma convenção do aplicativo. Por exemplo, dois mapas, department e employee, podem utilizar o Utilitário de Carga de department para pré-carregar os mapas department e employee. Isto assegura que, transacionalmente, se um aplicativo desejar um departamento, os funcionários desse departamento estarão no cache. Quando o Utilitário de Carga do departamento pré-carregar um departamento do backend, ele também buscará os funcionários para esse departamento. O objeto department e seus objetos employee associados são, então, incluídos no mapa utilizando uma transação única.

Pré-carregamento recuperável

Alguns clientes têm conjuntos de dados muito grandes que precisam ser armazenados em cache. O pré-carregamento desses dados pode consumir muito tempo. Às vezes, o pré-carregamento deve ser concluído antes de o aplicativo ficar online. É possível beneficiar-se ao tornar o pré-carregamento recuperável. Suponha que haja um milhão de registros para pré-carregar. O primário está pré-carregando estes registros e falha no registro de número 800.000. Normalmente, a réplica escolhida para ser o novo primário limpa qualquer estado replicado e começa do início. O eXtreme Scale pode usar uma interface ReplicaPreloadController. O carregador para o aplicativo também precisa implementar a interface ReplicaPreloadController. Este exemplo inclui um método único no Utilitário de Carga: `Status checkPreloadStatus(Session session, BackingMap bmap);`. Este método é chamado pelo tempo de execução do eXtreme Scale antes do método preload da interface do Utilitário de Carga ser chamada normalmente. O eXtreme Scale testa o resultado deste método (Status) para determinar seu comportamento sempre que uma réplica é promovida para um primário.

Tabela 19. Valor de Status e Resposta

Valor do Status Retornado	Resposta do eXtreme Scale
`Status.PRELOADED_ALREADY`	O eXtreme Scale não chama o método preload porque este valor do status indica que o mapa foi totalmente pré-carregado.
`Status.FULL_PRELOAD_NEEDED`	O eXtreme Scale limpa o mapa e chama o método preload normalmente.
`Status.PARTIAL_PRELOAD_NEEDED`	O eXtreme Scale deixa o mapa no estado em que se encontra e chama o pré-carregamento. Essa estratégia permite que o carregador do aplicativo continue o pré-carregamento desse ponto em diante.

Claramente, enquanto um primário está pré-carregando o mapa, ele deve deixar algum estado em um mapa no MapSet que está sendo replicado de forma que a réplica determine qual status retornar. É possível usar um mapa extra denominado, por exemplo, RecoveryMap. Este mapa RecoveryMap deve fazer parte do mesmo mapa MapSet que está sendo pré-carregado para assegurar que o mapa seja replicado de forma consistente com os dados que estão sendo pré-carregados. A seguir, está uma implementação sugerida.

À medida que ocorre a confirmação de pré-carregamento cada bloco de registros, o processo também atualiza um contador ou valor no mapa RecoveryMap como parte de tal transação. Os dados pré-carregados e os dados do mapa RecoveryMap são replicados atomicamente para as réplicas. Quando a réplica é promovida para o primário, ela pode verificar o mapa RecoveryMap para saber o que aconteceu.

O mapa RecoveryMap pode conter uma única entrada com a chave de estado. Se nenhum objeto existir para esta chave, será necessário um pré-carregamento (checkPreloadStatus returns FULL_PRELOAD_NEEDED) integral. Se um objeto existir para esta chave de estado e o valor for COMPLETE, o pré-carregamento é concluído e o método checkPreloadStatus retorna `PRELOADED_ALREADY`. Caso contrário, o objeto de valor indica onde o pré-carregamento reinicia e o método checkPreloadStatus retorna `PARTIAL_PRELOAD_NEEDED`. O utilitário de carga pode armazenar o ponto de recuperação em uma variável de instância para o utilitário de carga para que, quando o pré-carregamento for chamado, ele saiba o ponto de partida. O mapa RecoveryMap também pode conter uma entrada por mapa se cada mapa for pré-carregado de maneira independente.

Manipulando a recuperação no modo de replicação síncrono com um Utilitário de Carga

O tempo de execução doeXtreme Scale é projetado para não perder dados com commit quando o primário falha. A seção a seguir mostra os algoritmos utilizados. Estes algoritmos se aplicam apenas quando um grupo de replicação utiliza a replicação síncrona. Um utilitário de carga é opcional.

O tempo de execução do eXtreme Scale pode ser configurado para replicar todas as alterações a partir de um primário para as réplicas de maneira síncrona. Quando uma réplica síncrona é posicionada ela recebe uma cópia dos dados existentes no shard primário. Durante este período, o primário continua a receber transações e copiá-las assincronamente para a réplica. A réplica não é considerada como estando on-line neste período.

Depois de a réplica capturar o primário, ela entre no modo peer e começa a replicação síncrona. Cada transação consolidada no primário é enviada às réplicas síncronas e o primário aguarda por uma resposta de cada réplica. Uma sequência de consolidação síncrona com um utilitário de carga no primário se parece com o conjunto e etapas a seguir:

Tabela 20. Sequência de Commit no Primário

Etapa com o Utilitário de Carga	**Etapa sem o Utilitário de Carga**
Obter bloqueios para entradas	igual
Limpar alterações no utilitário de carga	no-op
Salvar alterações no cache	igual
Enviar alterações para réplicas e esperar confirmação	igual
Confirmar para o utilitário de carga por meio do Plug-in TransactionCallback	commit do plug-in chamado, mas não faz nada
Liberar bloqueios para entradas	igual

Observe que as alterações são enviadas para a réplica antes de serem confirmadas para o utilitário de carga. Para determinar quando ocorre o commit das alterações na réplica, revise esta sequência: No momento da inicialização, inicialize as listas tx no primário, conforme abaixo.

```
CommitedTx = {}, RolledBackTx = {}
```

Durante o processamento de confirmação síncrona, utilize a seguinte sequência:

Tabela 21. Processamento de Commit Síncrono

Etapa com o Utilitário de Carga	**Etapa sem o Utilitário de Carga**
Obter bloqueios para entradas	igual
Limpar alterações no utilitário de carga	no-op
Salvar alterações no cache	igual
Enviar alterações com uma transação confirmada, efetuar rollback da transação para a réplica e esperar confirmação	igual
Limpar lista de transações confirmadas e de transações que receberam rollback	igual
Confirmar o utilitário de carga por meio do plug-in TransactionCallBack	A confirmação do plug-in TransactionCallBack ainda é chamada mas, geralmente, não faz nada

Tabela 21. Processamento de Commit Síncrono (continuação)

Etapa com o Utilitário de Carga	Etapa sem o Utilitário de Carga
Se a confirmação for bem-sucedida, inclua a transação nas transações confirmadas; caso contrário, inclua nas transações que receberam rollback	no-op
Liberar bloqueios para entradas	igual

Para processamento de réplica, utilize a seguinte sequência:

1. Receber alterações
2. Confirmar todas as transações recebidas na lista de transações confirmadas
3. Efetuar rollback de todas as transações recebidas na lista de transações que receberam rollback
4. Iniciar uma transação ou sessão
5. Aplicar alterações à transação ou sessão
6. Salvar a transação ou sessão na lista pendente
7. Retornar resposta

Observe que, na réplica, não existem interações do Utilitário de Carga enquanto ele está no modo de réplica. O primário deve enviar todas as alterações por meio do Utilitário de Carga. A réplica não altera os dados. Um efeito secundário deste algoritmo é que a réplica sempre tem as transações, mas elas não são confirmadas, até que a próxima transação primária envie o status de confirmação destas transações. Elas são então confirmadas ou recebem rollback na réplica. Mas, até então, as transações não são confirmadas. É possível incluir um cronômetro no primário que envia o resultado da transação após um pequeno período (alguns segundos). Esse cronômetro limita, mas não elimina, nenhuma deterioração desse espaço de tempo Este staleness é um problemas apenas ao utilizar o modo de leitura de réplica. Do contrário, a deterioração não tem impacto sobre o aplicativo.

Quando o primário falha, é provável que poucos commits ou rollback tenham ocorrido nas transações no primário, mas a mensagem nunca fez isto para a réplica com estas saídas. Quando uma réplica for promovida para o novo primário, uma de suas primeiras ações será manipular esta condição. Cada transação pendente é processada novamente junto ao novo conjunto de mapas do primário. Se houver um Utilitário de Carga, então, cada transação é fornecida para o Utilitário de Carga. Estas transações são aplicadas na ordem FIFO (primeiro a entrar, primeiro a sair) estrita. Se uma transação falhar, ela será ignorada. Se três transações estiverem pendentes, A, B e C, A poderá ser confirmada, B poderá ser retrocedida e C também poderá ser confirmada. Nenhuma transação tem impacto sobre as outras. Suponha que elas sejam independentes.

Um utilitário de carga talvez queira utilizar uma lógica um pouco diferente quando no modo recuperação de failover versus modo normal. O carregador pode saber facilmente quando está em modo de recuperação de failover, implementando a interface ReplicaPreloadController. O método checkPreloadStatus só é chamado quando a recuperação de failover é concluída. Portanto, se o método de aplicação da interface do Carregador for chamado antes do método checkPreloadStatus, ele será uma transação de recuperação. Após o método checkPreloadStatus ser chamado, a recuperação de failover será concluída.

Configurando o Suporte do Carregador Write-behind: Java

Você pode ativar o suporte write-behind usando o arquivo XML descritor do ObjectGrid ou programaticamente usando a interface BackingMap.

Use o arquivo XML descritor do ObjectGrid para ativar o suporte write-behind ou programaticamente usando a interface BackingMap.

Arquivo XML descritor do ObjectGrid

Ao configurar um ObjectGrid usando o arquivo XML descritor do ObjectGrid, o utilitário de carga write-behind é ativado configurando-se o atributo writeBehind na tag backingMap. Este é um exemplo:

```
<objectGrid name="library" >
     <backingMap name="book" writeBehind="T300;C900" pluginCollectionRef="bookPlugins"/>
```

No exemplo anterior, o suporte para write-behind do mapa de apoio book está ativado com o parâmetro T300;C900. O atributo write-behind especifica a duração da atualização máxima e/ou uma contagem máxima de atualização de chave. O formato do parâmetro write-behind é:

```
write-behind attribute  ::= <defaults> | <update time> | <update key count> | <update time> ";" <update key count>
update time  ::= "T" <positive integer>
update key count  ::= "C" <positive integer>
defaults  ::= "" {table}
```

Ocorrem atualizações no utilitário de carga quando um dos seguintes eventos ocorre:

1. O tempo máximo de atualização em segundos decorreu desde a última atualização.
2. O número de chaves atualizadas no mapa de fila alcançou a contagem de chaves de atualização.

Estes parâmetros são apenas dicas. A contagem de atualização real e a duração da atualização estarão dentro do intervalo próximo dos parâmetros. Entretanto, não garantimos que a contagem de atualização real ou a duração da atualização sejam as mesmas que as definidas nos parâmetros. Além disso, a primeira atualização behind pode ocorrer após até o dobro da duração da atualização. Isto ocorre porque ObjectGrid escolhe aleatoriamente o momento de início da atualização para que todas as partições não cheguem no banco de dados simultaneamente.

No exemplo anterior T300;C900, o utilitário de carga grava os dados no backend quando 300 segundos decorreram desde a última atualização ou quando 900 chaves estão pendentes para serem atualizadas. A duração da atualização padrão é 300 segundos e a contagem de chaves de atualização padrão é de 1000.

Tabela 22. Algumas Opções de write-behind

Valor do Atributo	Tempo
T100	A duração da atualização é 100 segundos e a contagem de chaves de atualização é de 1000 (o valor padrão)
C2000	A duração da atualização é de 300 segundos (o valor padrão) e a contagem de chaves de atualização é de 2000.
T300;C900	A duração da atualização é de 300 segundos e a contagem de chaves de atualização é de 900.
""	A duração da atualização é de 300 segundos (o valor padrão) e a contagem de chaves de atualização é de 1000 (o valor padrão). **Nota:** Se você configurar o utilitário de carga write-behind como uma cadeia vazia: `writeBehind=""`, o utilitário de carga write-behind é ativado usando os valores padrão. Portanto, não especifique o atributo writeBehind se não desejar que o suporte write-behind seja ativado.

Ativando o Suporte Write-behind Programaticamente

Quando estiver criando um mapa de apoio programaticamente para um eXtreme Scale em memória local, o método a seguir pode ser usado na interface BackingMap para ativar e desativar o suporte para write-behind.

```
public void setWriteBehind(String writeBehindParam);
```

Para obter mais detalhes sobre como usar o método setWriteBehind, consulte o Interface BackingMap.

Referências relacionadas:

Java "Exemplo: Gravando uma Classe Dumper no Modo write-behind" na página 625
Essa amostra de código de origem mostra como gravar um watcher (dumper) para manipular atualizações write-behind com falhas.

Armazenamento em Cache Write-behind: Java

É possível utilizar armazenamento em cache write-behind para reduzir o gasto adicional que ocorre durante a atualização de um banco de dados que você está utilizando como back end.

Visão Geral do Armazenamento em Cache Write-Behind

O armazenamento em cache write-behind enfileira assincronamente as atualizações no plug-in do Utilitário de Carga. É possível melhorar o desempenho desconectando atualizações, inserções e remoções para um mapa, a sobrecarga de atualização do banco de dados de backend. A atualização assíncrona é executada após um atraso baseado em tempo (por exemplo, cinco minutos) ou um atraso baseado em entradas (1000 entradas).

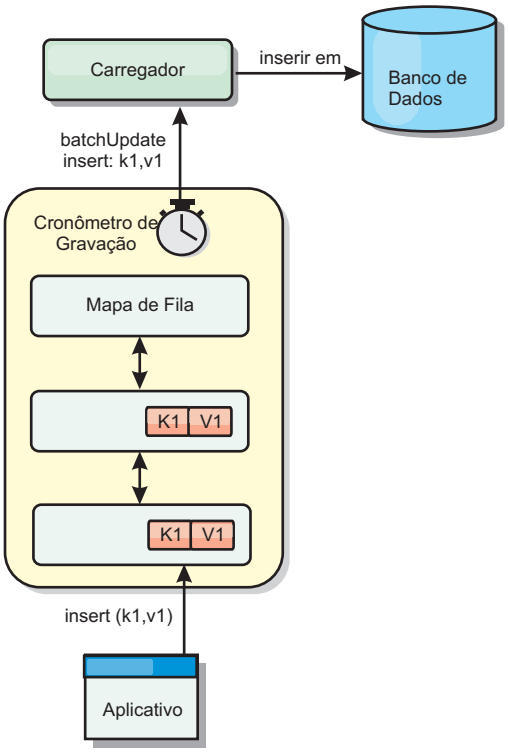


Figura 41. Armazenamento em Cache Write-behind

A configuração write-behind em um BackingMap cria um encadeamento entre o utilitário de carga e o mapa. O utilitário de carga então delega pedidos de dados através do encadeamento de acordo com as definições da configuração no método BackingMap.setWriteBehind. Quando uma transação do eXtreme Scale insere, atualiza ou remove uma entrada de um mapa, um objeto LogElement é criado para cada um destes registros. Estes elementos são enviados para o utilitário de carga write-behind e enfileirados em um ObjectMap especial denominado mapa de fila. Cada mapa de apoio com a configuração write-behind ativada possui seus próprios mapas de fila. Um encadeamento write-behind remove periodicamente os dados enfileirados dos mapas de fila e executa o push deles para o utilitário de carga de backend real.

O utilitário de carga write-behind enviará apenas os tipos insert, update e delete dos objetos LogElement para o utilitário de carga real. Todos os outros tipos de objetos LogElement, por exemplo, o tipo EVICT, são ignorados.

O suporte write-behind *é* uma extensão do plug-in do Carregador, que você usa para integrar o eXtreme Scale ao banco de dados. Por exemplo, consulte as informações do Configurando Utilitários de Carga do JPA sobre como configurar um carregador JPA.

Benefícios

Ativar o suporte write-behind possui os seguintes benefícios:

- **Isolamento de falha de backend:** O armazenamento em cache write-behind fornece uma camada de isolamento das falhas de backend. Quando o banco de dados de backend falha, as atualizações são enfileiradas no mapa de fila. Os

aplicativos podem continuar a conduzir transações para o eXtreme Scale. Quando o backend se recupera, os dados no mapa de fila são enviados para o backend.

- **Carga de backend reduzida:** O utilitário de carga write-behind mescla as atualizações em uma base de chave, portanto, apenas uma atualização mesclada por chave existe no mapa de fila. Esta mesclagem diminui o número de atualizações no backend.
- **Desempenho de transação aprimorado:** Tempos de transação do eXtreme Scale individuais são reduzidos porque a transação não precisa aguardar até que os dados sejam sincronizados com o backend.

Referências relacionadas:

Java "Exemplo: Gravando uma Classe Dumper no Modo write-behind" na página 625
Essa amostra de código de origem mostra como gravar um watcher (dumper) para manipular atualizações write-behind com falhas.

Considerações de Design do Aplicativo do Carregador Write-behind: Java

Ao implementar carregadores write-behind, você deve considerar várias questões, como restrição de integridade, comportamento de bloqueio e desempenho.

Considerações de Design do Aplicativo

Ativar o suporte write-behind é simples, mas o design de um aplicativo para trabalhar com o suporte write-behind precisa de consideração cuidadosa. Sem o suporte de write-behind, a transação de ObjectGrid engloba a transação de backend. A transação do ObjectGrid inicia antes da transação de backend iniciar e termina após a transação de backend terminar.

Com suporte write-behind ativado, a transação do ObjectGrid é concluída antes que a transação de backend inicie. A transação do ObjectGrid e a transação de backend não estão acopladas.

Limitadores de Integridade Referencial

Cada mapa de apoio que é configurado com suporte write-behind possui seu próprio encadeamento write-behind para enviar os dados para o backend. Portanto, os dados que são atualizados em diferentes mapas em uma transação do ObjectGrid são atualizadas no backend em diferentes transações de backend. Por exemplo, a transação T1 atualiza a chave key1 no mapa Map1 e a chave key2 no mapa Map2. A atualização da key1 para o mapa Map1 é atualizada no backend em uma transação de backend e a key2 atualizada para o mapa Map2 é atualizada no backend em outra transação de backend por encadeamentos write-behind diferentes. Se os dados armazenados no Map1 e Map2 possuírem relações, tais como limitadores de chave estrangeira no backend, as atualizações podem falhar.

Ao projetar os limitadores de integridade referencial em seu banco de dados de backend, certifique-se de que atualizações fora de ordem sejam permitidas.

Comportamento do Bloqueio de Mapa de Fila

Outra grande diferença de comportamento da transação é o comportamento do bloqueio. O ObjectGrid suporta três diferentes estratégias de bloqueio: PESSIMISTIC, OPTIMISITIC e NONE. Os mapas de fila write-behind utilizam a estratégia de bloqueio pessimista não importando qual estratégia de bloqueio está

configurada para seu mapa de apoio. Existem dois diferentes tipos de operações que adquirem um bloqueio no mapa de fila:

- Quando uma transação do ObjectGrid é confirmada ou um flush (flush de mapa ou flush de sessão) acontece, a transação lê a chave no mapa de fila e coloca um bloqueio S na chave.
- Quando uma transação do ObjectGrid é confirmada, a transação tenta atualizar o bloqueio S para o bloqueio X na chave.

Devido a este comportamento do mapa de fila extra, é possível visualizar algumas diferenças de comportamento de bloqueio.

- Se o mapa do usuário for configurado como a estratégia de bloqueio PESSIMISTIC, não há muita diferença no comportamento de bloqueio. Sempre que um flush ou commit é chamado, um bloqueio S é colocado na mesma chave no mapa de fila. Durante o momento do commit, um bloqueio X não é adquirido apenas para a chave no mapa do usuário, ele também é adquirido para a chave no mapa de fila.
- Se o mapa do usuário for configurado com a estratégia de bloqueio OPTIMISTIC ou NONE, a transação do usuário seguirá o padrão de estratégia de bloqueio PESSIMISTIC. Sempre que um flush ou commit é chamado, um bloqueio S é adquirido para a mesma chave no mapa de fila. Durante o momento do commit, um bloqueio X é adquirido para a chave no mapa de fila utilizando a mesma transação.

Novas Tentativas de Transações do Utilitário de Carga

O ObjectGrid não suporta transações 2-phase ou XA. O encadeamento write-behind remove registros do mapa de fila e atualiza os registros no backend. Se o servidor falhar no meio da transação, algumas atualizações de backend podem ser perdidas.

O utilitário de carga write-behind automaticamente tentará gravar novamente transações falhas e enviará uma LogSequence duvidosa para o backend para evitar a perda de dados. Esta ação requer que o utilitário de carga seja idempotente, o que significa que o Loader.batchUpdate(TxId, LogSequence) é chamado duas vezes com o mesmo valor, ele fornece o mesmo resultado como se tivesse sido aplicado uma vez. As implementações do utilitário de carga devem implementar a interface RetryableLoader para ativar este recurso. Consulte a documentação da API para obter mais detalhes.

Considerações de Desempenho de Armazenamento em Cache Write-behind

O suporte de armazenamento em cache Write-behind melhora o tempo de resposta removendo da transação a atualização do carregador. Ele também aumenta o rendimento do banco de dados porque as atualizações de banco de dados são combinadas. É importante compreender o gasto adicional introduzido pelo encadeamento write-behind, que executa o pull dos dados da mapa de fila e executa o push para o utilitário de carga.

A contagem máxima de atualização ou o tempo máximo de atualização necessário a ser ajustado com base nos padrões de uso e no ambiente esperados. Se o valor da contagem máxima de atualização ou o tempo máximo de atualização for muito pequeno, o gasto adicional do encadeamento write-behind pode exceder os benefícios. Configurar um valor maior para estes dois parâmetros também pode aumentar o uso da memória para enfileirar os dados e aumentar o tempo de envelhecimento dos registros do banco de dados.

Para obter um melhor desempenho, ajuste os parâmetros write-behind com base nos seguintes fatores:

- Proporção de transações de leitura e gravação
- Mesma frequência de atualização de registro
- Latência de atualização de banco de dados.

Manipulando Atualizações Write-Behind Falhas: Java

Como a transação do WebSphere eXtreme Scale termina antes de a transação de backend iniciar, é possível que ocorra um falso sucesso da transação.

Se você tentar inserir uma entrada em uma transação do eXtreme Scale que não exista no mapa de apoio mas existe no banco de dados backend, causando uma chave duplicada, a transação do eXtreme Scale será bem-sucedida. Entretanto, a transação na qual o encadeamento write-behind insere o objeto no banco de dados backend falha com uma exceção de chave duplicada.

Manipulando Atualizações write-behind com Falha: Lado do Cliente

Uma atualização deste tipo, ou qualquer outra atualização de backend falha, é uma atualização write-behind falha. Atualizações write-behind falhas são armazenadas em um mapa de atualização write-behind falho. Este mapa funciona como uma fila de eventos para atualizações falhas. A chave da atualização é um objeto Integer exclusivo e o valor é uma instância do FailedUpdateElement. O mapa de atualização write-behind com falha é configurado com um evictor, que despeja os registros uma hora depois de terem sido inseridos. Assim, os registros de atualização com falha serão perdidos se eles não forem recuperados dentro de 1 hora.

A API do ObjectMap pode ser utilizada para recuperar as entradas do mapa de atualização write-behind falho. O nome do mapa de atualização write-behind com falha é: `IBM_WB_FAILED_UPDATES_<map name>`. Consulte a documentação da API do WriteBehindLoaderConstants para os nomes de prefixo de cada um dos mapas do sistema write-behind. A seguir há um exemplo.

processo com falha - código de exemplo

```
ObjectMap failedMap = session.getMap(
    WriteBehindLoaderConstants.WRITE_BEHIND_FAILED_UPDATES_MAP_PREFIX + "Employee");
Object key = null;

session.begin();
while(key = failedMap.getNextKey(ObjectMap.QUEUE_TIMEOUT_NONE)) {
    FailedUpdateElement element = (FailedUpdateElement) failedMap .get(key);
    Throwable throwable = element.getThrowable();
    Object failedKey = element.getKey();
    Object failedValue = element.getAfterImage();
    failedMap .remove(key);
    // Faça algo interessante com a chave, o valor ou a exceção.

}
session.commit();
```

Uma chamada de método getNextKey funciona com uma partição específica para cada transação eXtreme Scale. Em um ambiente distribuído, para obter chaves de todas as partições, você deve iniciar diversas transações, como mostrado no exemplo a seguir :

obtendo chaves de todas as partições - código de exemplo

```
ObjectMap failedMap = session.getMap(
    WriteBehindLoaderConstants.WRITE_BEHIND_FAILED_UPDATES_MAP_PREFIX + "Employee");
```

```
while (true) {
    session.begin();
    Object key = null;
    while(( key = failedMap.getNextKey(5000) )!= null ) {
        FailedUpdateElement element = (FailedUpdateElement) failedMap .get(key);
    Throwable throwable = element.getThrowable();
        Object failedKey = element.getKey();
        Object failedValue = element.getAfterImage();
        failedMap .remove(key);
        // Faça algo interessante com a chave, o valor ou a exceção.

    }
    Session.commit();
}
```

Nota: O mapa de atualização com falha fornece uma maneira de monitorar o funcionamento do aplicativo. Se um sistema produzir muitos registros no mapa de atualização com falha, significa que é necessário revisar o aplicativo ou a arquitetura para usar o suporte write-behind. É possível usar o comando **xscmd -showMapSizes** para ver o tamanho da entrada do mapa de atualização com falha.

Manipulando atualizações write-behind com Falha: Listener do Shard

É importante detectar e registrar quando uma transação write-behind falha. Todo aplicativo utilizando write-behind precisa implementar um watcher para manipular atualizações write-behind falhas. Isto evita potencialmente ficar sem memória já os registros no Mapa de atualização inválido não são despejados porque o aplicativo é esperado para manipulá-los.

O código a seguir mostra como conectar tal watcher, ou "dumper ", que deve ser incluído no descritor XML do ObjectGrid como no fragmento.

```
<objectGrid name="Grid">
 <bean id="ObjectGridEventListener" className="utils.WriteBehindDumper"/>
```

É possível visualizar o bean ObjectGridEventListener que foi incluído, que é o watcher write-behind referido acima. O watcher interage nos Mapas para todos os shards principais em um JVM procurando por aqueles com write-behind ativado. Se ele localizar um, então, ele tenta registrar até 100 atualizações inválidas. Ele continua observando um shard principal até que o shard seja movido para um JVM diferente. Todos os aplicativos que usam write-behind devem usar um watcher semelhante a este. Caso contrário, o Java Virtual Machines fica sem memória porque este mapa de erro nunca é despejado.

Consulte o “Exemplo: Gravando uma Classe Dumper no Modo write-behind” para obter informações adicionais.

Referências relacionadas:

Java “Exemplo: Gravando uma Classe Dumper no Modo write-behind”
Essa amostra de código de origem mostra como gravar um watcher (dumper) para manipular atualizações write-behind com falhas.

Exemplo: Gravando uma Classe Dumper no Modo write-behind: Java

Essa amostra de código de origem mostra como gravar um watcher (dumper) para manipular atualizações write-behind com falhas.

```
//
//This sample program is provided AS IS and may be used, executed, copied and
//modified without royalty payment by customer (a) for its own instruction and
//study, (b) in order to develop applications designed to run with an IBM
//WebSphere product, either for customer's own internal use or for redistribution
```

```
//by customer, as part of such an application, in customer's own products. "
//
//5724-J34 (C) COPYRIGHT International Business Machines Corp. 2009
//All Rights Reserved * Licensed Materials - Property of IBM
//
package utils;

import java.util.Collection;
import java.util.Iterator;
import java.util.concurrent.Callable;
import java.util.concurrent.ScheduledExecutorService;
import java.util.concurrent.ScheduledFuture;
import java.util.concurrent.ScheduledThreadPoolExecutor;
import java.util.concurrent.TimeUnit;
import java.util.logging.Logger;

import com.ibm.websphere.objectgrid.BackingMap;
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.ObjectGridException;
import com.ibm.websphere.objectgrid.ObjectGridRuntimeException;
import com.ibm.websphere.objectgrid.ObjectMap;
import com.ibm.websphere.objectgrid.Session;
import com.ibm.websphere.objectgrid.UndefinedMapException;
import com.ibm.websphere.objectgrid.plugins.ObjectGridEventGroup;
import com.ibm.websphere.objectgrid.plugins.ObjectGridEventListener;
import com.ibm.websphere.objectgrid.writebehind.FailedUpdateElement;
import com.ibm.websphere.objectgrid.writebehind.WriteBehindLoaderConstants;

/**
 * Write behind expects transactions to the Loader to succeed. If a transaction for a key fails then
 * it inserts an entry in a Map called PREFIX + mapName. The application should be checking this
 * map for entries to dump out write behind transaction failures. The application is responsible for
 * analyzing and then removing these entries. These entries can be large as they include the key, before
 * and after images of the value and the exception itself. Exceptions can easily be 20k on their own.
 *
 * The class is registered with the grid and an instance is created per primary shard in a JVM. Isso cria
 * um único encadeamento
 * e depois esse encadeamento verifica cada mapa de erro write behind
para o shard, imprime o problema e
 * depois remove a entrada.
 *
 * Isso significa que existirá um encadeamento por shard. Se o shard for
movido para outra JVM, o método deactivate
 * irá parar o encadeamento.
 * method stops the thread.
 * @author bnewport
 *
 */
public class WriteBehindDumper implements ObjectGridEventListener,
ObjectGridEventGroup.ShardEvents, Callable<Boolean>
{
 static Logger logger = Logger.getLogger(WriteBehindDumper.class.getName());

 ObjectGrid grid;

 /**
  * Thread pool to handle table checkers. If the application has it's own pool
  * then change this to reuse the existing pool
  */
 static ScheduledExecutorService pool = new ScheduledThreadPoolExecutor(2); // two threads to dump records

 // the future for this shard
 ScheduledFuture<Boolean> future;

 // true if this shard is active
 volatile boolean isShardActive;

 /**
  * Normal time between checking Maps for write behind errors
  */
 final long BLOCKTIME_SECS = 20L;

 /**
  * An allocated session for this shard. No point in allocating them again and again
  */
 Session session;
 /**
  * When a primary shard is activated then schedule the checks to periodically check
  * the write behind error maps and print out any problems
  */
 public void shardActivated(ObjectGrid grid)
 {
  try
  {
   this.grid = grid;
   session = grid.getSession();

   isShardActive = true;
   future = pool.schedule(this, BLOCKTIME_SECS, TimeUnit.SECONDS); // check every BLOCKTIME_SECS seconds initially
  }
  catch(ObjectGridException e)
```

```
 {
  throw new ObjectGridRuntimeException("Exception activating write dumper", e);
 }
}

/**
 * Mark shard as inactive and then cancel the checker
 */
public void shardDeactivate(ObjectGrid arg0)
{
 isShardActive = false;
 // if it's cancelled then cancel returns true
 if(future.cancel(false) == false)
 {
  // otherwise just block until the checker completes
  while(future.isDone() == false) // wait for the task to finish one way or the other
  {
   try
   {
    Thread.sleep(1000L); // check every second
   }
   catch (InterruptedException e)
   {
   }
  }
 }
}

/**
 * Simple test to see if the map has write behind enabled and if so then return
 * the name of the error map for it.
 * @param mapName The map to test
 * @return The name of the write behind error map if it exists otherwise null
 */
static public String getWriteBehindNameIfPossible(ObjectGrid grid, String mapName)
{
 BackingMap map = grid.getMap(mapName);
 if(map != null && map.getWriteBehind() != null)
 {
  return WriteBehindLoaderConstants.WRITE_BEHIND_FAILED_UPDATES_MAP_PREFIX + mapName;
 }
 else
  return null;
}

/**
 * This runs for each shard. It checks if each map has write behind enabled and if it does
  * then it prints out any write behind
 * transaction errors and then removes the record.
 */
public Boolean call()
{
 logger.fine("Called for " + grid.toString());
 try
 {
  // while the primary shard is present in this JVM
  // only user defined maps are returned here, no system maps like write behind maps are in
  // this list.
  Iterator<String> iter = grid.getListOfMapNames().iterator();
  boolean foundErrors = false;
  // iterate over all the current Maps
  while(iter.hasNext() && isShardActive)
  {
   String origName = iter.next();

   // if it's a write behind error map
   String name = getWriteBehindNameIfPossible(grid, origName);
   if(name != null)
   {
    // try to remove blocks of N errors at a time
    ObjectMap errorMap = null;
    try
    {
     errorMap = session.getMap(name);
    }
    catch(UndefinedMapException e)
    {
     // at startup, the error maps may not exist yet, patience...
     continue;
    }
    // try to dump out up to N records at once
    session.begin();
    for(int counter = 0; counter < 100; ++counter)
    {
     Integer seqKey = (Integer)errorMap.getNextKey(1L);
     if(seqKey != null)
     {
      foundErrors = true;
      FailedUpdateElement elem = (FailedUpdateElement)errorMap.get(seqKey);
      //
      // Your application should log the problem here
```

```
      logger.info("WriteBehindDumper ( " + origName + ") for key (" + elem.getKey() + ") Exception: " +
       elem.getThrowable().toString());
      //
      //
      errorMap.remove(seqKey);
     }
     else
      break;
    }
    session.commit();
   }
  } // do next map
  // loop faster if there are errors
  if(isShardActive)
  {
   // reschedule after one second if there were bad records
   // otherwise, wait 20 seconds.
   if(foundErrors)
    future = pool.schedule(this, 1L, TimeUnit.SECONDS);
   else
    future = pool.schedule(this, BLOCKTIME_SECS, TimeUnit.SECONDS);
  }
 }
 catch(ObjectGridException e)
 {
  logger.fine("Exception in WriteBehindDumper" + e.toString());
  e.printStackTrace();

  //don't leave a transaction on the session.
  if(session.isTransactionActive())
  {
   try { session.rollback(); } catch(Exception e2) {}
  }
 }
 return true;
}

public void destroy() {
 // TODO Auto-generated method stub

}

public void initialize(Session arg0) {
 // TODO Auto-generated method stub

}

public void transactionBegin(String arg0, boolean arg1) {
 // TODO Auto-generated method stub

}

public void transactionEnd(String arg0, boolean arg1, boolean arg2,
  Collection arg3) {
 // TODO Auto-generated method stub

}
}
```

Conceitos relacionados:

Java "Configurando o Suporte do Carregador Write-behind" na página 618
Você pode ativar o suporte write-behind usando o arquivo XML descritor do ObjectGrid ou programaticamente usando a interface BackingMap.

Java "Armazenamento em Cache Write-behind" na página 271
É possível utilizar armazenamento em cache write-behind para reduzir o gasto adicional que ocorre durante a atualização de um banco de dados que você está utilizando como back end.

Java "Manipulando Atualizações Write-Behind Falhas" na página 624
Como a transação do WebSphere eXtreme Scale termina antes de a transação de backend iniciar, é possível que ocorra um falso sucesso da transação.

Considerações sobre a Programação do Utilitário de Carga do JPA: Java

Um Utilitário de Carga do Java Persistence API (JPA) é uma implementação do plug-in do utilitário de carga que usa o JPA para interagir com o banco de dados. Use as seguintes considerações ao desenvolver um aplicativo que usa um utilitário de carga do JPA.

Entidade eXtreme Scale e Entidade do JPA

É possível designar qualquer classe POJO como uma entidade eXtreme Scale usando as anotações de entidade eXtreme Scale, uma configuração XML ou ambos. Também é possível designar a mesma classe POJO como uma entidade do JPA utilizando anotações de entidades JPA, a configuração XML ou ambas.

Entidade eXtreme Scale : Uma entidade eXtreme Scale representa dados persistentes que são armazenados em mapas ObjectGrid. Um objeto de entidade é transformado em uma tupla de chave e em uma tupla de valor, que então são armazenadas como pares chave-valor nos mapas. Uma tupla é uma matriz de atributos primitivos.

Entidade do JPA: Uma entidade do JPA representa dados persistentes que são armazenados em um banco de dados relacional automaticamente usando uma persistência gerenciada por contêiner. Os dados são persistidos em algum tipo sistema de armazenamento de dados no formato apropriado, como tuplas de banco de dados em um banco de dados.

Quando uma entidade do eXtreme Scale é persistida, suas relações serão armazenadas em outros mapas de entidade. Por exemplo, se você estiver persistindo uma entidade Consumer com uma relação de um para muitos em uma entidade ShippingAddress, se a persistência em cascata for ativada, a entidade ShippingAddress será armazenada no mapa shippingAddress em formato de tupla. Se você estiver persistindo uma entidade JPA, as entidades do JPA relacionadas também serão persistidas para as tabelas de banco de dados se a persistência em cascata estiver ativada. Quando uma classe POJO é designada como entidade do eXtreme Scale e entidade do JPA, os dados podem ser persistidos para os mapas e bancos de dados da entidade ObjectGrid. Os usos comuns são:

- **Cenário de Pré-Carregamento**: Uma entidade é carregada de um banco de dados usando um provedor do JPA e é persistida nos mapas de entidade do ObjectGrid.
- **Cenário do Utilitário de Carga**: Uma implementação do Utilitário de Carga é conectada aos mapas de entidade ObjectGrid para que uma entidade armazenada nos mapas de entidade ObjectGrid possa ser persistida ou carregada a partir de um banco de dados usando provedores do JPA.

Também é comum que uma classe POJO seja designada apenas como uma entidade JPA. Neste caso, o que é armazenado nos mapas do ObjectGrid são as instâncias do POJO, versus as tuplas de entidade no caso da entidade do ObjectGrid.

Considerações de Design do Aplicativo para Mapas de Entidade

Ao conectar uma instância do JPALoader, as instâncias de objeto serão diretamente armazenadas nos mapas do ObjectGrid.

Porém, ao conectar a um JPAEntityLoader, a classe de entidade é designada como uma entidade do eXtreme Scale e uma entidade do JPA. Neste caso, trate esta entidade como se ela tivesse dois armazenamentos de persistência: os mapas de entidade do ObjectGrid e o armazenamento de persistência do JPA. A arquitetura torna-se mais complicado do que o caso do JPALoader.

Para obter mais informações sobre o plug-in JPAEntityLoader e considerações sobre o design de aplicativo, consulte o “Plug-in JPAEntityLoader” na página 631.

Essas informações também podem ajudar se você planejar implementar seu próprio utilitário de carga para os mapas de entidade.

Considerações sobre Desempenho

Certifique-se de configurar o tipo de busca ávido ou lento adequado para os relacionamentos. Por exemplo, um relacionamento um-para-muitos bidirecional de Consumer com ShippingAddress, com o OpenJPA para ajudar a explicar as diferenças de desempenho. Neste exemplo, uma consulta JPA tenta `select o from Consumer o where . . .` efetuar um carregamento em massa e também carregar todos os objetos ShippingAddress relacionados. Um relacionamento um para muitos definido na classe Consumer é o seguinte:

```
@Entity
public class Consumer implements Serializable {

    @OneToMany(mappedBy="consumer",cascade=CascadeType.ALL, fetch =FetchType.EAGER)
    ArrayList <ShippingAddress> addresses;
```

A seguir há o consumidor da relação muitos-para-um definido na classe do ShippingAddress:

```
@Entity
public class ShippingAddress implements Serializable{

    @ManyToOne(fetch=FetchType.EAGER)
    Consumer consumer;
}
```

Se os tipos de busca de ambos os relacionamentos estiverem configurados como `ávido`, o OpenJPA utilizará consultas N+1+1 para obter todos os objetos Consumer e objetos ShippingAddress, em que N é o número de objetos ShippingAddress. Entretanto, se ShippingAddress for alterado para utilizar o tipo de busca lento conforme a seguir, ele fará apenas duas consultas para obter todos os dados.

```
@Entity
public class ShippingAddress implements Serializable{

    @ManyToOne(fetch=FetchType.LAZY)
    Consumer consumer;
}
```

Embora a consulta retorne os mesmos resultados, ter um número baixo de consultas diminui significativamente a interação com o banco de dados, o que pode aumentar o desempenho do aplicativo.

Conceitos relacionados:

Java "Plug-ins para a Comunicação com os Bancos de Dados" na página 601
Com um plug-in Loader, um mapa ObjectGrid pode se comportar como um cache de memória para dados que são normalmente mantidos em um armazenamento persistente no mesmo sistema ou em algum outro sistema. Geralmente, um banco de dados ou sistema de arquivos é utilizado como o armazenamento persistente. Uma JVM (Java Virtual Machine) também pode ser usada como a origem de dados, permitindo que caches baseados em hub sejam construídos usando ObjectGrid. Um utilitário de carga possui a lógica para leitura e gravação de dados para um armazenamento persistente e a partir dele.

Java "Criando um Utilitário de Carga" na página 610
É possível gravar sua própria implementação de plug-in de utilitário de carga em seus aplicativos, que deve seguir as convenções de plug-in do WebSphere eXtreme Scale comuns.

Java "Plug-in JPAEntityLoader"
O plug-in JPAEntityLoader é uma implementação Loader integrada que usa o Java Persistence API (JPA) para se comunicar com o banco de dados quando usar a API EntityManager. Ao utilizar a API do ObjectMap, utilize o utilitário de carga JPALoader.

Java "Utilizando um Utilitário de Carga com Mapas de Entidade e Tuplas" na página 634
O gerenciador de entidades converte todos os objetos de entidade em objetos de tupla antes que eles sejam armazenados em um mapa do WebSphere eXtreme Scale. Cada entidade tem uma tupla de chave e uma tupla de valor. Este par chave-valor é armazenado no mapa do eXtreme Scale associado à entidade. Ao usar um mapa do eXtreme Scale com um utilitário de carga, o utilitário de carga deve interagir com os objetos da tupla.

Java "Gravando um Utilitário de Carga com um Controlador de Pré-carregamento de Réplica" na página 639
Um utilitário de carga com um controlador de pré-carregamento de réplica é um utilitário de carga que implementa a interface ReplicaPreloadController além da interface do utilitário de carga.

Java "Utilitários de Carga" na página 273
Com um plug-in Carregador, uma grade de dados pode se comportar como um cache de memória para dados que normalmente são mantidos em um armazenamento persistente no mesmo sistema ou em outro sistema. Geralmente, um banco de dados ou sistema de arquivos é utilizado como o armazenamento persistente. Uma JVM (Java Virtual Machine) também pode ser usada como a origem de dados, permitindo que caches baseados em hub seja construído usando o eXtreme Scale. Um utilitário de carga possui a lógica para leitura e gravação de dados para um armazenamento persistente e a partir dele.

Plug-in JPAEntityLoader: Java

O plug-in JPAEntityLoader é uma implementação Loader integrada que usa o Java Persistence API (JPA) para se comunicar com o banco de dados quando usar a API EntityManager. Ao utilizar a API do ObjectMap, utilize o utilitário de carga JPALoader.

Detalhes do Utilitário de Carga

Use o plug-in do JPAEntityLoader ao armazenar dados usando a API ObjectMap. Use o plug-in do JPAEntityLoader ao armazenar dados usando a API EntityManager.

Os Utilitários de Carga fornecem duas funções principais:

1. **get**: No método get, o primeiro plug-in JPAEntityLoader chama o método javax.persistence.EntityManager.find(Class entityClass, Object key) para localizar a entidade JPA. Em seguida, o plug-in projeta esta entidade do JPA nas tuplas de entidades. Durante a projeção, ambos os atributos de tuplas e as chaves de associação são armazenados na tupla de valor. Após o processamento de cada chave, o método get retorna uma lista de tuplas de valor de entidades.
2. **batchUpdate**: O método batchUpdate usa um objeto LogSequence que contém uma lista de objetos LogElement. Cada objeto LogElement contém uma tupla de chave uma tupla de valor. Para interagir com o provedor JPA, primeiro é necessário localizar a entidade eXtreme Scale com base na tupla de chave. Com base no tipo LogElement, execute as seguintes chamadas JPA:
   - **insert**: javax.persistence.EntityManager.persist(Object o)
   - **update**: javax.persistence.EntityManager.merge(Object o)
   - **remove**: javax.persistence.EntityManager.remove(Object o)

Um LogElement com tipo **update** faz o JPAEntityLoader chamar javax.persistence.EntityManager.merge(Object o) para mesclar a entidade. Além disso, um LogElement com tipo **update** pode ser o resultado de uma chamada com.ibm.websphere.objectgrid.em.EntityManager.merge(object o) ou uma mudança de atributo da instância gerenciada EntityManager de eXtreme Scale. Consulte o seguinte exemplo:

```
com.ibm.websphere.objectgrid.em.EntityManager em = og.getSession().getEntityManager();
em.getTransaction().begin();
Consumer c1 = (Consumer) em.find(Consumer.class, c.getConsumerId());
c1.setName("New Name");
em.getTransaction().commit();
```

Neste exemplo, um LogElement de tipo atualizar é enviado para o JPAEntityLoader do consumidor do mapa. O método javax.persistence.EntityManager.merge(Object o) será chamado para o gerenciador de entidade do JPA em vez de um atributo atualizar para a entidade gerenciada do JPA. Devido a esta mudança de comportamento, há algumas limitações na utilização deste modelo de programação.

Regras de Design do Aplicativo

Entidades possuem relacionamentos com outras entidades. Projetar um aplicativo com relacionamentos envolvidos e com JPAEntityLoader conectado requer considerações adicionais. O aplicativo deve seguir as quatro regras a seguir, descritas nas seções a seguir.

Suporte à Profundidade de Relacionamentos Limitado

O JPAEntityLoader é suportado apenas ao utilizar entidades sem nenhum relacionamento ou entidades com relacionamentos de nível único. Relacionamentos com mais de um nível, como por exemplo, `Company > Department > Employee` não são suportados.

Um Utilitário de Carga por Mapa

Utilizando os relacionamentos da entidade Consumer-ShippingAddress como um exemplo, quando você carrega um consumidor com a busca ávida ativada, é possível carregar todos os objetos ShippingAddress relacionados. Quando você persiste ou funde um objeto Consumer, é possível persistir ou fundir objetos ShippingAddress relacionados se cascade-persist ou cascade-merge estiver ativado.

Não é possível conectar um utilitário de carga para o mapa da entidade-raiz que armazena as tuplas da entidade Consumer. É necessário configurar um utilitário de carga para cada mapa de entidade.

Mesmo tipo de cascata para JPA e eXtreme Scale

Considere novamente o cenário no qual a entidade Consumer possui um relacionamento um-para-muitos com ShippingAddress. É possível examinar o cenário no qual cascade-persist está ativado para este relacionamento. Quando um objeto Consumer é persistido no eXtreme Scale, o número N associado de objetos ShippingAddress será também será persistido no eXtreme Scale.

Uma chamada de persistência do objeto Consumer com um relacionamento cascade-persist com ShippingAddress converte-se em um método javax.persistence.EntityManager.persist(consumer) e *N* chamadas javax.persistence.EntityManager.persist(shippingAddress) pela camada JPAEntityLoader. Entretanto, estas N chamadas de persistência extra para ShippingAddress são desnecessárias devido à configuração cascade-persist do ponto de vista do provedor JPA. Para solucionar este problema, o eXtreme Scale fornece um novo método isCascaded na instância LogElement. O método isCascaded indica se LogElement é um resultado de uma operação em cascata EntityManager do eXtreme Scale. Neste exemplo, o JPAEntityLoader do mapa ShippingAddress recebe *N* objetos LogElement devido às chamadas de persistência em cascata. O JPAEntityLoader descobre que o método isCascaded retorna true e, em seguida, ignora-os sem fazer nenhuma chamada JPA. Portanto, a partir de um ponto de vista do JPA, apenas uma chamada javax.persistence.EntityManager.persist(consumer) é recebida.

O mesmo comportamento é exibido se você fundir uma entidade ou remover uma entidade com cascata ativada. As operações em cascata são ignoradas pelo plug-in JPAEntityLoader.

A estrutura do suporte de cascata é para reproduzir as operações EntityManager do eXtreme Scale para os provedores JPA. Estas operações incluem operações persist, merge e remove. Para ativar o suporte de cascata, verifique se a configuração de cascata para o JPA e o EntityManager do eXtreme Scale sejam os mesmos.

Utilize a Atualização de Entidades com Cuidado

Como descrito anteriormente, a estrutura do suporte em cascata é para reproduzir as operações EntityManager do eXtreme Scale para os provedores do JPA. Se o aplicativo chamar o método ogEM.persist(consumer) para o EntityManager do eXtreme Scale, mesmos os objetos ShippingAddress associados serão persistidos devido à configuração cascade-persist e o JPAEntityLoader chama apenas o método jpAEM.persist(consumer) para os provedores JPA.

Entretanto, se o aplicativo atualizar uma entidade gerenciada, essa atualização será convertida em uma chamada de mesclagem JPA pelo plug-in JPAEntityLoader. Neste cenário, o suporte para vários níveis de relacionamentos e associações-chave não é garantido. Neste caso, a boa prática é utilizar o método javax.persistence.EntityManager.merge(o) em vez de atualizar uma entidade gerenciada.

Referências relacionadas:

Java "Considerações sobre a Programação do Utilitário de Carga do JPA" na página 628
Um Utilitário de Carga do Java Persistence API (JPA) é uma implementação do plug-in do utilitário de carga que usa o JPA para interagir com o banco de dados. Use as seguintes considerações ao desenvolver um aplicativo que usa um utilitário de carga do JPA.

Utilizando um Utilitário de Carga com Mapas de Entidade e Tuplas: Java

O gerenciador de entidades converte todos os objetos de entidade em objetos de tupla antes que eles sejam armazenados em um mapa do WebSphere eXtreme Scale. Cada entidade tem uma tupla de chave e uma tupla de valor. Este par chave-valor é armazenado no mapa do eXtreme Scale associado à entidade. Ao usar um mapa do eXtreme Scale com um utilitário de carga, o utilitário de carga deve interagir com os objetos da tupla.

O eXtreme Scale inclui plug-ins do utilitário de carga que simplificam a integração com bancos de dados relacionais. Os Utilitários de Carga da Java Persistence API (JPA) usam uma Java Persistence API para interagir com o banco de dados e criar os objetos de entidade. Os utilitários de carga JPA são compatíveis com as entidades doeXtreme Scale.

Tuplas

Uma tupla contém informações sobre os atributos e associações de uma entidade. Os valores primitivos são armazenados utilizando seus wrappers primitivos. Outros tipos de objeto suportados são armazenados em seu formato nativo. A associações com outras entidades são armazenadas como uma coleta de objetos de tupla de chave que representam as chaves das entidades de destino.

Cada atributo ou associação é armazenado utilizado um índice baseado em zero. É possível recuperar o índice de cada atributo usando os métodos getAttributePosition ou getAssociationPosition. Depois que a posição ser recuperada, ela permanecerá inalterada durante o ciclo de vida do eXtreme Scale. A posição poderá ser alterada quando o eXtreme Scale for reiniciado. Os métodos setAttribute, setAssociation e setAssociations são usados para atualizar os elementos na tupla.

Atenção: Quando você criar ou atualizar objetos da tupla, atualize cada campo de primitiva com um valor não-nulo. Os valores de primitivas como `int` não devem ser nulos. Se você não alterar o valor para um padrão, poderão ocorrer problemas de desempenho ruim, afetando também campos marcados com a anotação @Version ou atributo de versão no arquivo XML descritor da entidade.

O exemplo a seguir explica como processar as tuplas. Para obter mais informações sobre a definição de entidades para esse exemplo, consulte o "Tutorial do Entity Manager: Esquema da Entidade Order" na página 14. WebSphere eXtreme Scale é configurado para usar os utilitários de carga em cada uma das entidades. Além

disso, apenas a entidade Order será usada e esta entidade específica possui um relacionamento muitos-para-um com a entidade Customer. O nome do atributo é `customer` e ele possui um relacionamento um-para-muitos com a entidade OrderLine.

Utilize o Projector para criar objetos de Tupla automaticamente a partir das entidades. A utilização do Projector simplifica os utilitários de carga ao usar um utilitário de mapeamento relacional de objeto, como Hibernate ou JPA.

order.java

```
@Entity
public class Order {
    @Id String orderNumber;
    java.util.Date date;
    @OneToOne(cascade=CascadeType.PERSIST) Customer customer;
    @OneToMany(cascade=CascadeType.ALL, mappedBy="order") @OrderBy("lineNumber") List<OrderLine> lines;
}
```

customer.java

```
@Entity
public class Customer {
    @Id String id;
    String firstName;
    String surname;
    String address;
    String phoneNumber;
}
```

orderLine.java

```
@Entity
public class OrderLine
{
    @Id @ManyToOne(cascade=CascadeType.PERSIST) Order order;
    @Id int lineNumber;
    @OneToOne(cascade=CascadeType.PERSIST) Item item;
    int quantity;
    double price;
}
```

Uma classe OrderLoader que implementa a interface do utilitário de carga é mostrada no código a seguir. O seguinte exemplo assume que um plug-in TransactionCallback associado esteja definido.

orderLoader.java

```
public class OrderLoader implements com.ibm.websphere.objectgrid.plugins.Loader {

 private EntityMetadata entityMetaData;
 public void batchUpdate(TxID txid, LogSequence sequence)
           throws LoaderException,
OptimisticCollisionException {
        ...
        }
        public List get(TxID txid, List keyList, boolean forUpdate)
            throws LoaderException {
        ...
        }
        public void preloadMap(Session session, BackingMap backingMap)
            throws LoaderException {
  this.entityMetaData=backingMap.getEntityMetadata();
 }

}
```

A variável da instância entityMetaData é inicializada durante a chamada de método preLoadMap a partir do eXtreme Scale. A variável *entityMetaData* não será nula se o Mapa for configurado para usar entidades. Caso contrário, o valor será nulo.

Método batchUpdate

O método batchUpdate fornece a habilidade de saber que ação o aplicativo pretende executar. Com base em uma operação de inserção, atualização ou exclusão, uma conexão pode ser aberta com o banco de dados e o trabalho ser executado. Como a chave e os valores são do tipo Tupla, eles devem ser transformados para que os valores façam sentido na instrução SQL.

A tabela ORDER foi criada com a definição de DDL (Data Definition Language) mostrada no código a seguir:

```
CREATE TABLE ORDER (ORDERNUMBER VARCHAR(250) NOT NULL, DATE TIMESTAMP, CUSTOMER_ID VARCHAR(250))
ALTER TABLE ORDER ADD CONSTRAINT PK_ORDER PRIMARY KEY (ORDERNUMBER)
```

O código a seguir demonstra como converter uma Tupla em um Objeto:

```
public void batchUpdate(TxID txid, LogSequence sequence)
        throws LoaderException,
OptimisticCollisionException {
        Iterator iter = sequence.getPendingChanges();
        while (iter.hasNext()) {
            LogElement logElement = (LogElement)iter.next();
            Object key = logElement.getKey();
            Object value = logElement.getCurrentValue();

            switch (logElement.getType().getCode()) {
            case LogElement.CODE_INSERT:

1)              if (entityMetaData!=null) {

// The order has just one key orderNumber
2)                  String ORDERNUMBER=(String) getKeyAttribute("orderNumber", (Tuple) key);
// Get the value of date
3)                  java.util.Date unFormattedDate = (java.util.Date) getValueAttribute("date",(Tuple)value);
// The values are 2 associations. Lets process customer because
// the our table contains customer.id as primary key
4)                  Object[] keys= getForeignKeyForValueAssociation("customer","id",(Tuple) value);
                    //Order to Customer is M to 1. There can only be 1 key
5)                  String CUSTOMER_ID=(String)keys[0];
// parse variable unFormattedDate and format it for the database as formattedDate
6)                   String formattedDate = "2007-05-08-14.01.59.780272"; // formatted for DB2
// Finally, the following SQL statement to insert the record
7) //INSERT INTO ORDER (ORDERNUMBER, DATE, CUSTOMER_ID) VALUES(ORDERNUMBER,formattedDate, CUSTOMER_ID)
                }
                break;
            case LogElement.CODE_UPDATE:
                break;
            case LogElement.CODE_DELETE:
                break;
            }
        }

    }
// returns the value to attribute as stored in the key Tuple
 private Object getKeyAttribute(String attr, Tuple key) {
        //get key metadata
        TupleMetadata keyMD = entityMetaData.getKeyMetadata();
        //get position of the attribute
        int keyAt = keyMD.getAttributePosition(attr);
        if (keyAt > -1) {
            return key.getAttribute(keyAt);
        } else { // attribute undefined
            throw new IllegalArgumentException("Invalid position index for  "+attr);
        }

    }
// returns the value to attribute as stored in the value Tuple
    private Object getValueAttribute(String attr, Tuple value) {
        //similar to above, except we work with value metadata instead
        TupleMetadata valueMD = entityMetaData.getValueMetadata();

        int keyAt = valueMD.getAttributePosition(attr);
        if (keyAt > -1) {
            return value.getAttribute(keyAt);
        } else {
            throw new IllegalArgumentException("Invalid position index for  "+attr);
        }
    }
// returns an array of keys that refer to association.
    private Object[] getForeignKeyForValueAssociation(String attr, String fk_attr, Tuple value) {
        TupleMetadata valueMD = entityMetaData.getValueMetadata();
        Object[] ro;

        int customerAssociation = valueMD.getAssociationPosition(attr);
        TupleAssociation tupleAssociation = valueMD.getAssociation(customerAssociation);
```

```
        EntityMetadata targetEntityMetaData = tupleAssociation.getTargetEntityMetadata();

        Tuple[] customerKeyTuple = ((Tuple) value).getAssociations(customerAssociation);

        int numberOfKeys = customerKeyTuple.length;
        ro = new Object[numberOfKeys];

        TupleMetadata keyMD = targetEntityMetaData.getKeyMetadata();
        int keyAt = keyMD.getAttributePosition(fk_attr);
        if (keyAt < 0) {
            throw new IllegalArgumentException("Invalid position index for  "+attr);
        }
        for (int i = 0; i < numberOfKeys; ++i) {
            ro[i] = customerKeyTuple[i].getAttribute(keyAt);
        }

        return ro;

    }
```

1. Certifique-se de que entityMetaData não seja nulo, o que implica na entradas do cache de chave e valor serem do tipo Tuple. A partir de entityMetaData, Key TupleMetaData é recuperado, o que realmente reflete apenas a parte principal dos metadados Order.
2. Processe o KeyTuple e obtenha o valor do Atributo-chave orderNumber
3. Processe o ValueTuple e obtenha o valor da data do atributo
4. Processe o ValueTuple e obtenha o valor das chaves do consumidor da associação
5. Extraia CUSTOMER_ID. Com base no relacionamento, uma ordem pode ter apenas um consumidor; portanto, teremos apenas uma chave. Por isso, o tamanho das chaves é 1. Por simplicidade, ignoramos a análise da data para verificar se o formato está correto.
6. Como esta é uma operação insert, a instrução SQL é transmitida para a conexão da origem de dados para concluir a operação insert.

A demarcação da transação e o acesso ao banco de dados são abordados em “Criando um Utilitário de Carga” na página 610.

Método get

Se a chave não for localizada no cache, chame o método get no plug-in do Utilitário de Carga para localizar a chave.

A chave é uma Tupla. A primeira etapa é converter a Tupla para valores primitivos que possam ser transmitidos na instrução SELECT SQL. Depois de todos os atributos serem recuperados do banco de dados, converta-os em Tuplas. O código a seguir demonstra a classe Order.

```
public List get(TxID txid, List keyList, boolean forUpdate) throws LoaderException {
  System.out.println("OrderLoader: Get called");
  ArrayList returnList = new ArrayList();

1)  if (entityMetaData != null) {
   int index=0;
   for (Iterator iter = keyList.iterator(); iter.hasNext();) {
2)    Tuple orderKeyTuple=(Tuple) iter.next();

    // The order has just one key orderNumber
3)    String ORDERNUMBERKEY = (String) getKeyAttribute("orderNumber",orderKeyTuple);
    //We need to run a query to get values of
4)    // SELECT CUSTOMER_ID, date FROM ORDER WHERE ORDERNUMBER='ORDERNUMBERKEY'

5)    //1) Foreign key: CUSTOMER_ID
6)    //2) date
    // Assuming those two are returned as
7)                            String  CUSTOMER_ID = "C001"; // Assuming Retrieved and initialized
8)    java.util.Date retrievedDate = new java.util.Date();
                              // Assuming this date reflects the one in database

    // We now need to convert this data into a tuple before returning

    //create a value tuple
```

```
9)    TupleMetadata valueMD = entityMetaData.getValueMetadata();
    Tuple valueTuple=valueMD.createTuple();


    //add retrievedDate object to Tuple
    int datePosition = valueMD.getAttributePosition("date");
10)    valueTuple.setAttribute(datePosition, retrievedDate);

    //Next need to add the Association
11)    int customerPosition=valueMD.getAssociationPosition("customer");
    TupleAssociation customerTupleAssociation =
                                valueMD.getAssociation(customerPosition);
    EntityMetadata customerEMD = customerTupleAssociation.getTargetEntityMetadata();
    TupleMetadata customerTupleMDForKEY=customerEMD.getKeyMetadata();
12)    int customerKeyAt=customerTupleMDForKEY.getAttributePosition("id");


    Tuple customerKeyTuple=customerTupleMDForKEY.createTuple();
    customerKeyTuple.setAttribute(customerKeyAt, CUSTOMER_ID);
13)    valueTuple.addAssociationKeys(customerPosition, new Tuple[] {customerKeyTuple});


14)    int linesPosition = valueMD.getAssociationPosition("lines");
    TupleAssociation linesTupleAssociation = valueMD.getAssociation(linesPosition);
    EntityMetadata orderLineEMD = linesTupleAssociation.getTargetEntityMetadata();
    TupleMetadata orderLineTupleMDForKEY = orderLineEMD.getKeyMetadata();
    int lineNumberAt = orderLineTupleMDForKEY.getAttributePosition("lineNumber");
    int orderAt = orderLineTupleMDForKEY.getAssociationPosition("order");

    if (lineNumberAt < 0 || orderAt < 0) {
     throw new IllegalArgumentException(
                                      "Invalid position index for lineNumber or order "+
                                      lineNumberAt + " " + orderAt);
    }
15) // SELECT LINENUMBER FROM ORDERLINE WHERE ORDERNUMBER='ORDERNUMBERKEY'
    // Assuming two rows of line number are returned with values 1 and 2

    Tuple orderLineKeyTuple1 = orderLineTupleMDForKEY.createTuple();
    orderLineKeyTuple1.setAttribute(lineNumberAt, new Integer(1));// set Key
    orderLineKeyTuple1.addAssociationKey(orderAt, orderKeyTuple);

    Tuple orderLineKeyTuple2 = orderLineTupleMDForKEY.createTuple();
    orderLineKeyTuple2.setAttribute(lineNumberAt, new Integer(2));// Init Key
    orderLineKeyTuple2.addAssociationKey(orderAt, orderKeyTuple);

16)    valueTuple.addAssociationKeys(linesPosition, new Tuple[]
                                  {orderLineKeyTuple1, orderLineKeyTuple2 });

    returnList.add(index, valueTuple);

    index++;

   }
  }else {
   // does not support tuples
  }
  return returnList;
 }
```

1. O método get é chamado quando o cache do ObjectGrid não consegue localizar a chave e solicita que o utilitário de carga faça a busca. Teste o valor para entityMetaData e continue se ele não for nulo.
2. A keyList contém Tuplas.
3. Recupere o valor de atributo orderNumber.
4. Execute a consulta para recuperar a data (valor) e o ID do cliente (chave estrangeira).
5. CUSTOMER_ID é uma chave estrangeira que deve ser configurada na tupla de associação.
6. A data é um valor e já deverá estar configurada.
7. Como este exemplo não executa chamadas JDBC, CUSTOMER_ID é assumido.
8. Como este exemplo não executa chamadas JDBC, a data é assumida.
9. Crie a Tupla de valor.
10. Configure o valor da data na Tupla, com base em sua posição.
11. O pedido possui duas associações. Inicie com o atributo customer que faz referência à entidade do cliente. Você deve ter o valor do ID para configurar na Tupla.

12. Localize a posição do ID na entidade do cliente.
13. Configure os valores apenas das chaves de associação.
14. Além disso, as linhas são uma associação que devem ser configuradas como grupo de chaves de associação, da mesma forma como é feito para a associação do cliente.
15. Como é necessário configurar as chaves para o lineNumber associado a este pedido, execute o SQL para recuperar os valores de lineNumber.
16. Configure as chaves de associação no valueTuple. Isto conclui a criação da Tupla que é retornada ao BackingMap

Este tópico oferece as etapas para criação de tuplas, e uma descrição apenas para a entidade Order. Execute etapas semelhantes para as outras entidades e todo o processo que está ligado ao plug-in TransactionCallback. Consulte "Plug-ins para o Gerenciamento de Eventos de Ciclo de Vida da Transação" na página 644 para obter detalhes.

Referências relacionadas:

Java "Considerações sobre a Programação do Utilitário de Carga do JPA" na página 628
Um Utilitário de Carga do Java Persistence API (JPA) é uma implementação do plug-in do utilitário de carga que usa o JPA para interagir com o banco de dados. Use as seguintes considerações ao desenvolver um aplicativo que usa um utilitário de carga do JPA.

Gravando um Utilitário de Carga com um Controlador de Pré-carregamento de Réplica: Java

Um utilitário de carga com um controlador de pré-carregamento de réplica é um utilitário de carga que implementa a interface ReplicaPreloadController além da interface do utilitário de carga.

A interface ReplicaPreloadController é projetada para fornecer uma maneira para uma réplica que se torna o shard primário saber se o shard primário anterior concluiu o processo de pré-carregamento. Se o pré-carregamento estiver parcialmente concluído, as informações para continuar onde o primário anterior parou são fornecidas. Com a implementação da interface ReplicaPreloadController, uma réplica que se torna o shard primário continua o processo de pré-carregamento onde o shard primário anterior parou e continua a conclusão do pré-carregamento geral.

Em um ambiente distribuído de WebSphere eXtreme Scale, um mapa pode ter réplicas e pode pré-carregar grandes volumes de dados durante a inicialização. O pré-carregamento é uma atividade do utilitário de carga e pode ocorrer apenas no mapa primário durante a inicialização. O pré-carregamento pode demorar muito para concluir, se um grande volume de dados for pré-carregado. Se o mapa primário concluiu uma grande parte dos dados pré-carregados, mas for parado por motivos desconhecidos durante a inicialização, uma réplica torna-se primária. Nessa situação, os dados de pré-carregamento que foram concluídos pela primária anterior são perdidos, pois a nova primária, em geral, desempenha um pré-carregamento incondicional. Com um pré-carregamento incondicional, a nova primária inicia o processo de pré-carregamento do início e os dados pré-carregados anteriormente são ignorados. Se desejar que o novo shard primário continue onde o shard primário anterior parou durante o processo de pré-carregamento, forneça um Utilitário de carga que implemente a interface ReplicaPreloadController. Para obter mais informações, consulte a documentação da API.

Para obter mais informações sobre os Loaders, consulte “Utilitários de Carga” na página 273. Se você estiver interessado em gravar um plug-in do Utilitário de Carga comum, consulte “Criando um Utilitário de Carga” na página 610.

A interface ReplicaPreloadController possui a seguinte definição:

```
public interface ReplicaPreloadController
{
    public static final class Status
    {
        static public final Status PRELOADED_ALREADY = new Status(K_PRELOADED_ALREADY);
        static public final Status FULL_PRELOAD_NEEDED = new Status(K_FULL_PRELOAD_NEEDED);
        static public final Status PARTIAL_PRELOAD_NEEDED = new Status(K_PARTIAL_PRELOAD_NEEDED);
    }

    Status checkPreloadStatus(Session session, BackingMap bmap);
}
```

As seções a seguir abordam alguns dos métodos da interface Utilitário de Carga e ReplicaPreloadController.

Método checkPreloadStatus

Quando um Utilitário de Carga implementa a interface ReplicaPreloadController, o método checkPreloadStatus é chamado antes do método preloadMap durante a inicialização do mapa. O status de retorno deste método determina se o método preloadMap é chamado. Se este método retornar `Status#PRELOADED_ALREADY`, o método de pré-carregamento não é chamado. Caso contrário, o método preload será executado. Devido a este comportamento, este método deve servir como o método de inicialização do Utilitário de Carga. Você deve inicializar as propriedades do Utilitário de Carga neste método. Este método deve retornar o status correto, ou o pré-carregamento pode não funcionar conforme esperado.

```
public Status checkPreloadStatus(Session session, BackingMap backingMap) {
        // When a loader implements ReplicaPreloadController interface,
    // this method will be called before preloadMap method during
    // map initialization. Whether the preloadMap method will be
    // called depends on teh returned status of this method. So, this
    // method also serve as Loader's initialization method. This method
    // has to return the right staus, otherwise the preload may not
    // work as expected.

        // Note: must initialize this loader instance here.
        ivOptimisticCallback = backingMap.getOptimisticCallback();
        ivBackingMapName = backingMap.getName();
        ivPartitionId = backingMap.getPartitionId();
        ivPartitionManager = backingMap.getPartitionManager();
        ivTransformer = backingMap.getObjectTransformer();
        preloadStatusKey = ivBackingMapName + "_" + ivPartitionId;

        try {
            // get the preloadStatusMap to retrieve preload status that
      // could be set by other JVMs.
            ObjectMap preloadStatusMap = session.getMap(ivPreloadStatusMapName);

            // retrieve last recorded preload data chunk index.
            Integer lastPreloadedDataChunk = (Integer) preloadStatusMap.get(preloadStatusKey);

            if (lastPreloadedDataChunk == null) {
                preloadStatus = Status.FULL_PRELOAD_NEEDED;
            } else {
                preloadedLastDataChunkIndex = lastPreloadedDataChunk.intValue();
                if (preloadedLastDataChunkIndex == preloadCompleteMark) {
                    preloadStatus = Status.PRELOADED_ALREADY;
                } else {
                    preloadStatus = Status.PARTIAL_PRELOAD_NEEDED;
                }
            }

            System.out.println("TupleHeapCacheWithReplicaPreloadControllerLoader.checkPreloadStatus()
     -> map = " + ivBackingMapName + ", preloadStatusKey = " + preloadStatusKey
                    + ", retrieved lastPreloadedDataChunk =" + lastPreloadedDataChunk + ",
```

```
determined preloadStatus = "
                    + getStatusString(preloadStatus));

        } catch (Throwable t) {
            t.printStackTrace();
        }

        return preloadStatus;
    }
```

Método preloadMap

A execução do método preloadMap depende do resultado retornado do método checkPreloadStatus. Se o método preloadMap for chamado, ele geralmente deve recuperar as informações de status do pré-carregamento a partir do mapa de status do pré-carregamento designado e determinar como continuar. A forma ideal seria o método preloadMap saber se o pré-carregamento foi parcialmente concluído e onde exatamente deve iniciar. Durante o pré-carregamento de dados, o método preloadMap deve atualizar o status do pré-carregamento no mapa de status do pré-carregamento designado. O status do pré-carregamento que é armazenado no mapa de status de pré-carregamento é recuperado pelo método checkPreloadStatus quando ele precisar verificar o status de pré-carregamento.

```
public void preloadMap(Session session, BackingMap backingMap)
     throws LoaderException {
        EntityMetadata emd = backingMap.getEntityMetadata();
        if (emd != null && tupleHeapPreloadData != null) {
            // The getPreLoadData method is similar to fetching data
      // from database. These data will be push into cache as
      // preload process.
            ivPreloadData = tupleHeapPreloadData.getPreLoadData(emd);

            ivOptimisticCallback = backingMap.getOptimisticCallback();
            ivBackingMapName = backingMap.getName();
            ivPartitionId = backingMap.getPartitionId();
            ivPartitionManager = backingMap.getPartitionManager();
            ivTransformer = backingMap.getObjectTransformer();
            Map preloadMap;

            if (ivPreloadData != null) {
                try {
                    ObjectMap map = session.getMap(ivBackingMapName);

                    // obter o preloadStatusMap para registrar o status pré-carregado.
                    ObjectMap preloadStatusMap = session.getMap(ivPreloadStatusMapName);

                    // Note: when this preloadMap method is invoked, the
         // checkPreloadStatus has been called, Both preloadStatus
         // and preloadedLastDataChunkIndex have been set. And the
         // preloadStatus must be either PARTIAL_PRELOAD_NEEDED
         // or FULL_PRELOAD_NEEDED that will require a preload again.

                    // If large amount of data will be preloaded, the data usually
         // is divided into few chunks and the preload process will
         // process each chunk within its own tran. This sample only
         // preload few entries and assuming each entry represent a chunk.
                    // so that the preload process an entry in a tran to simulate
         // chunk preloading.

                    Set entrySet = ivPreloadData.entrySet();
                    preloadMap = new HashMap();
                    ivMap = preloadMap;

                    // The dataChunkIndex represent the data chunk that is in
         // processing
                    int dataChunkIndex = -1;
                    boolean shouldRecordPreloadStatus = false;
                    int numberOfDataChunk = entrySet.size();
                    System.out.println("    numberOfDataChunk to be preloaded = " + numberOfDataChunk);

                    Iterator it = entrySet.iterator();
                    int whileCounter = 0;
                    while (it.hasNext()) {
                        whileCounter++;
                        System.out.println("preloadStatusKey = " + preloadStatusKey + " ,
```

```
whileCounter = " + whileCounter);

                        dataChunkIndex++;

                        // if the current dataChunkIndex <= preloadedLastDataChunkIndex
                        // no need to process, becasue it has been preloaded by
                    // other JVM before. only need to process dataChunkIndex
                    // > preloadedLastDataChunkIndex
                        if (dataChunkIndex <= preloadedLastDataChunkIndex) {
                            System.out.println("ignore current dataChunkIndex =
                        " + dataChunkIndex + " that has been previously
                        preloaded.");
                            continue;
                        }

                        // Note: This sample simulate data chunk as an entry.
                        // each key represent a data chunk for simplicity.
                        // If the primary server or shard stopped for unknown
                     // reason, the preload status that indicates the progress
                     // of preload should be available in preloadStatusMap. A
                    // replica that become a primary can get the preload status
                    // and determine how to preload again.
                        // Note: recording preload status should be in the same
                     // tran as putting data into cache; so that if tran
                    // rollback or error, the recorded preload status is the
                    // actual status.

                        Map.Entry entry = (Entry) it.next();
                        Object key = entry.getKey();
                        Object value = entry.getValue();
                        boolean tranActive = false;

                        System.out.println("processing data chunk. map = " +
                      this.ivBackingMapName + ", current dataChunkIndex = " +
                      dataChunkIndex + ", key = " + key);

                        try {
                            shouldRecordPreloadStatus = false; // re-set to false
                            session.beginNoWriteThrough();
                            tranActive = true;

                            if (ivPartitionManager.getNumOfPartitions() == 1) {
                                // if just only 1 partition, no need to deal with
                       // partition.
                                // just push data into cache
                                map.put(key, value);
                                preloadMap.put(key, value);
                                shouldRecordPreloadStatus = true;
                            } else if (ivPartitionManager.getPartition(key) == ivPartitionId) {
                                // if map is partitioned, need to consider the
                       // partition key only preload data that belongs
                       // to this partition.
                                map.put(key, value);
                                preloadMap.put(key, value);
                                shouldRecordPreloadStatus = true;
                            } else {
                                // ignore this entry, because it does not belong to
                       // this partition.
                            }

                            if (shouldRecordPreloadStatus) {
                                System.out.println("record preload status. map = " +
                          this.ivBackingMapName + ", preloadStatusKey = " +
                          preloadStatusKey + ", current dataChunkIndex ="
                          + dataChunkIndex);
                                if (dataChunkIndex == numberOfDataChunk) {
                                    System.out.println("record preload status. map = " +
                             this.ivBackingMapName + ", preloadStatusKey = " +
                            preloadStatusKey + ", mark complete =" +
                            preloadCompleteMark);
                                    // means we are at the lastest data chunk, if commit
                         // successfully, record preload complete.
                         // at this point, the preload is considered to be done
                                    // use -99 as special mark for preload complete status.

                                    preloadStatusMap.get(preloadStatusKey);

                                    // a put follow a get will become update if the get
                          // return an object, otherwise, it will be insert.
                                    preloadStatusMap.put(preloadStatusKey, new Integer(preloadCompleteMark));
```

```
                                } else {
                                    // record preloaded current dataChunkIndex into
                    // preloadStatusMap a put follow a get will become
                    // update if teh get return an object, otherwise, it
                    // will be insert.
                                    preloadStatusMap.get(preloadStatusKey);
                                    preloadStatusMap.put(preloadStatusKey, new Integer(dataChunkIndex));
                                }
                            }

                            session.commit();
                            tranActive = false;

                            // to simulate preloading large amount of data
                            // put this thread into sleep for 30 secs.
                            // The real app should NOT put this thread to sleep
                            Thread.sleep(10000);

                        } catch (Throwable e) {
                            e.printStackTrace();
                            throw new LoaderException("preload failed with exception: " + e, e);
                        } finally {
                            if (tranActive && session != null) {
                                try {
                                    session.rollback();
                                } catch (Throwable e1) {
                                    // preload ignoring exception from rollback
                                }
                            }
                        }
                    }

                    // at this point, the preload is considered to be done for sure
                    // use -99 as special mark for preload complete status.
                    // this is a insurance to make sure the complete mark is set.
                    // besides, when partitioning, each partition does not know when
            // is its last data chunk. so the following block serves as the
            // overall preload status complete reporting.
                    System.out.println("Overall preload status complete -> record preload status.
map = " + this.ivBackingMapName + ",
                 preloadStatusKey = " + preloadStatusKey + ", mark complete =" +
                preloadCompleteMark);
                    session.begin();
                    preloadStatusMap.get(preloadStatusKey);
                    // a put follow a get will become update if teh get return an object,
                    // caso contrário, ele será inserido.
                    preloadStatusMap.put(preloadStatusKey, new Integer(preloadCompleteMark));
                    session.commit();

                    ivMap = preloadMap;
                } catch (Throwable e) {
                    e.printStackTrace();
                    throw new LoaderException("preload failed with exception: " + e, e);
                }
            }
        }
    }
```

Mapa de Status do Pré-carregamento

É necessário utilizar um mapa de status do pré-carregamento para suportar a implementação da interface ReplicaPreloadController. O método preloadMap deve sempre verificar primeiro o status do pré-carregamento armazenado no mapa de status do pré-carregamento e atualizar o status do pré-carregamento no mapa de status do pré-carregamento sempre que ele enviar os dados para o cache. O método checkPreloadStatus pode recuperar o status do pré-carregamento a partir do mapa de status do pré-carregamento, determinar o status de pré-carregamento e retornar o status para o responsável pela chamada. O mapa de status do pré-carregamento deve estar no mesmo mapSet que outros mapas que possuem utilitários de carga do controlador de pré-carregamento de réplica.

Referências relacionadas:

Java "Considerações sobre a Programação do Utilitário de Carga do JPA" na página 628
Um Utilitário de Carga do Java Persistence API (JPA) é uma implementação do plug-in do utilitário de carga que usa o JPA para interagir com o banco de dados. Use as seguintes considerações ao desenvolver um aplicativo que usa um utilitário de carga do JPA.

Plug-ins para o Gerenciamento de Eventos de Ciclo de Vida da Transação

Java

Use o plug-in TransactionCallback para customizar as operações de versão e de comparação de objetos do cache ao usar a estratégia de bloqueio otimista.

É possível fornecer um objeto de retorno de chamada otimista conectável que implementa a interface com.ibm.websphere.objectgrid.plugins.OptimisticCallback. Para os mapas de entidade, um plug-in OptimisticCallback de alto desempenho é automaticamente configurado.

Propósito

Utilize a interface OptimisticCallback para fornecer operações de comparação otimistas para os valores de um mapa. Uma implementação OptimisticCallback é necessária ao utilizar a estratégia de bloqueio otimista. O WebSphere eXtreme Scale fornece uma implementação OptimisticCallback padrão. No entanto, geralmente o aplicativo deve conectar sua própria implementação da interface OptimisticCallback. Consulte o "Estratégias de Bloqueio" na página 473 para obter informações adicionais.

Implementação Padrão

A estrutura do eXtreme Scale fornece uma implementação padrão da interface OptimisticCallback que é usada se o aplicativo não for conectado a um objeto OptimisticCallback fornecido pelo aplicativo, como demonstrado na seção anterior. A implementação padrão sempre retorna o valor especial de NULL_OPTIMISTIC_VERSION como o objeto de versão para o valor e nunca atualiza o objeto de versão. Esta ação transforma a comparação optimistic em uma função no operation. Na maioria dos casos, você não quer que a função no operation ocorra quando você estiver usando a estratégia de bloqueio optimistic. Seus aplicativos devem implementar a interface OptimisticCallback e conectar suas próprias implementações de OptimisticCallback para que a implementação padrão não seja utilizada. No entanto, existe pelo menos um cenário no qual a implementação OptimisticCallback fornecida padrão é útil. Considere a seguinte situação:

- Um utilitário de carga está conectado para o mapa de apoio.
- O utilitário de carga sabe como desempenhar a comparação otimista sem assistência de um plug-in OptimisticCallback.

Como o utilitário de carga pode saber como lidar com a versão otimista sem assistência de um objeto OptimisticCallback? O utilitário de carga conhece o objeto de classe de valor e sabe qual campo de objeto de valor é utilizado como um valor de versão otimista. Por exemplo, suponha que a seguinte interface seja utilizada para o objeto de valor para o mapa employees:

```
public interface Employee
{
    // Sequential sequence number used for optimistic versioning.
    public long getSequenceNumber();
    public void setSequenceNumber(long newSequenceNumber);
    // Other get/set methods for other fields of Employee object.
}
```

Neste caso, o utilitário de carga sabe que pode utilizar o método getSequenceNumber para obter as informações de versão atuais para um objeto de valor Employee. O utilitário de carga incrementa o valor retornado para gerar um novo número de versão antes de atualizar o armazenamento persistente com o novo valor Employee. Para um utilitário de carga do JDBC (Java Database Connectivity), o número de sequência atual na cláusula where de uma instrução update SQL super qualificada é usado, e ele usa o novo número de sequência gerado para configurar a coluna de número de sequência ao novo valor de número de sequência.

Outra possibilidade é que o utilitário de carga faça uso de alguma função fornecida por backend que atualiza automaticamente uma coluna oculta que pode ser utilizada para versões otimistas. Em alguns casos, um procedimento armazenado ou acionador possivelmente pode ser utilizado para ajudar a manter uma coluna que contém informações de controle de versões. Se o utilitário de carga estiver utilizando uma destas técnicas para a manutenção de informações de versões otimistas, então, o aplicativo não precisa fornecer uma implementação do OptimisticCallback. A implementação padrão OptimisticCallback pode ser utilizada porque o utilitário de carga consegue identificar versões otimistas sem nenhuma assistência de um objeto OptimisticCallback.

Implementação Padrão para Entidades

As entidades são armazenadas no ObjectGrid utilizando objetos de tupla. A implementação padrão do OptimisticCallback se comporta da mesma maneira que se comporta com mapas de não-entidade. Entretanto, o campo de versão na entidade é identificado utilizando a anotação @Version ou o atributo version no arquivo XML descritor da entidade.

O atributo version pode ser de um dos seguintes tipos: int, Integer, short, Short, long, Long ou java.sql.Timestamp. Uma entidade deve ter somente um atributo de versão definido. O atributo de versão deve ser configurado somente durante a construção. Depois de a entidade ser persistida, o valor do atributo de versão não deve ser modificado.

Se um atributo de versão não estiver configurado e a estratégia de bloqueio optimistic for usada, então toda a tupla assume implicitamente a versão usando o estado completo da tupla.

No exemplo a seguir, a entidade Employee possui um atributo de versão longa denominado SequenceNumber:

```
@Entity
public class Employee {
private long sequence;
    // Sequential sequence number used for optimistic versioning.
    @Version
    public long getSequenceNumber() {
        return sequence;
    }
    public void setSequenceNumber(long newSequenceNumber) {
```

```
        this.sequence = newSequenceNumber;
    }
    // Other get/set methods for other fields of Employee object.
}
```

Gravando uma Implementação OptimisticCallback

Uma implementação OptimisticCallback precisa implementar a interface OptimisticCallback e seguir as convenções comuns do plug-in ObjectGrid.

A lista a seguir fornece uma descrição ou consideração para cada um dos métodos na interface OptimisticCallback:

NULL_OPTIMISTIC_VERSION

Este valor especial será retornado pelo método getVersionedObjectForValue se a implementação OptimisticCallback padrão for utilizada em vez de uma implementação OptimisticCallback fornecida pelo aplicativo.

Método getVersionedObjectForValue

O método getVersionedObjectForValue pode retornar uma cópia do valor ou pode retornar um atributo do valor que pode ser utilizado para fins de controle de versões. Este método é chamado sempre que um objeto é associado a uma transação. Quando nenhum utilitário de carga é configurado em um mapa de apoio, o mapa de apoio usa este valor no momento da consolidação para executar uma comparação de versão optimistic. A comparação de versão otimista é utilizada pelo mapa de suporte para assegurar que a versão não tenha sido alterada desde que esta transação acessou pela primeira vez a entrada do mapa que foi modificada por esta transação. Se outra transação já tiver modificado a versão desta entrada do mapa, a comparação de versão falhará e o mapa de suporte exibirá uma exceção OptimisticCollisionException para forçar o rollback da transação. Se um Utilitário de Carga estiver conectado, o mapa de suporte não utilizará as informações de controle de versões otimista. Em vez disso, o Utilitário de Carga é responsável por desempenhar a comparação de controle de versões otimista e por atualizar as informações de controle de versões quando necessário. O Utilitário de Carga geralmente obtém o objeto de controle de versões inicial do LogElement transmitido para o método batchUpdate no Utilitário de Carga, que é chamado quando ocorre uma operação de limpeza ou uma transação é confirmada.

O código a seguir mostra a implementação utilizada pelo objeto EmployeeOptimisticCallbackImpl:

```
public Object getVersionedObjectForValue(Object value)
{
    if (value == null)
    {
        return null;
    }
    else
    {
        Employee emp = (Employee) value;
        return new Long( emp.getSequenceNumber() );
    }
}
```

Conforme demonstrado no exemplo anterior, o atributo sequenceNumber é retornado em um objeto java.lang.Long conforme esperado pelo Utilitário de

Carga, que significa que a mesma pessoa que gravou o Utilitário de Carga gravou a implementação de EmployeeOptimisticCallbackImpl ou trabalhou junto com a pessoa que implementou EmployeeOptimisticCallbackImpl. Por exemplo, essas pessoas concordam com o valor que é retornado pelo método getVersionedObjectForValue. Conforme descrito anteriormente, a implementação OptimisticCallback padrão retorna o valor especial NULL_OPTIMISTIC_VERSION como o objeto de versão.

Método updateVersionedObjectForValue

O método updateVersionedObjectForValue method é chamado sempre que uma transação tiver atualizado um valor e um novo objeto de versão for necessário. Se o método getVersionedObjectForValue retornar um atributo do valor, este método geralmente atualizará o valor de atributo com um novo objeto de versão. Se o método getVersionedObjectForValue retornar uma cópia do valor, este método normalmente não será atualizado. O método OptimisticCallback padrão não atualiza pois a implementação padrão de getVersionedObjectForValue sempre retorna o valor especial NULL_OPTIMISTIC_VERSION como o objeto de versão. O seguinte exemplo mostra a implementação usada pelo objeto EmployeeOptimisticCallbackImpl que é usado na seção OptimisticCallback:

```
public void updateVersionedObjectForValue(Object value)
{
    if ( value != null )
    {
        Employee emp = (Employee) value;
        long next = emp.getSequenceNumber() + 1;
        emp.updateSequenceNumber( next );
    }
}
```

Conforme demonstrado no exemplo anterior, o atributo sequenceNumber é incrementado em um para que, na próxima vez o método getVersionedObjectForValue for chamado, o valor java.lang.Long retornado tenha um valor longo que seja o valor do número de sequência original. Mais um, por exemplo, é o próximo valor de versão para esta instância de funcionário. Novamente, este exemplo significa que a mesma pessoa que gravou o Utilitário de Carga gravou a implementação EmployeeOptimisticCallbackImpl ou trabalhou junto com a pessoa que implementou o EmployeeOptimisticCallbackImpl.

Método serializeVersionedValue

Este método grava o valor com versão no fluxo especificado. Dependendo da implementação, o valor com versão pode ser utilizado para identificar colisões de atualização otimistas. Em algumas implementações, o valor com versão é uma cópia do valor original. Outras implementações podem ter um número de sequência ou algum outro objeto para indicar a versão do valor. Como a implementação real é desconhecida, este método é fornecido para executar a serialização apropriada. A implementação padrão faz uma chamada writeObject.

Método inflateVersionedValue

Este método utiliza a versão serializada do valor com versão e retorna o objeto de valor com versão real. Dependendo da implementação, o valor com versão pode ser utilizado para identificar colisões de atualização otimistas. Em algumas implementações, o valor com versão é uma cópia do valor original. Outras implementações podem ter um número de sequência ou algum outro objeto para indicar a versão do valor. Como a implementação real é desconhecida, este método

é fornecido para desempenhar a desserialização apropriada. A implementação padrão chama o método readObject.

Utilizando uma Implementação OptimisticCallback Fornecida pelo Aplicativo

Há duas abordagens para incluir uma implementação OptimisticCallback fornecido pelo aplicativo na configuração de BackingMap: configuração programática e configuração XML.

Conectar Programaticamente em uma Implementação OptimisticCallback

O exemplo a seguir demonstra como um aplicativo pode conectar programaticamente um objeto OptimisticCallback para o mapa de apoio de funcionários na instância grid1 do ObjectGrid:

```
import com.ibm.websphere.objectgrid.ObjectGridManagerFactory;
import com.ibm.websphere.objectgrid.ObjectGridManager;
import com.ibm.websphere.objectgrid.ObjectGrid;
import com.ibm.websphere.objectgrid.BackingMap;
ObjectGridManager ogManager = ObjectGridManagerFactory.getObjectGridManager();
ObjectGrid og = ogManager.createObjectGrid( "grid1" );
BackingMap bm = dg.defineMap("employees");
EmployeeOptimisticCallbackImpl cb = new EmployeeOptimisticCallbackImpl();
bm.setOptimisticCallback( cb );
```

Abordagem de configuração XML para conectar uma implementação OptimisticCallback

O objeto EmployeeOptimisticCallbackImpl no exemplo anterior deve implementar a interface OptimisticCallback. O aplicativo também pode utilizar um arquivo XML para conectar seu objeto OptimisticCallback conforme mostrado no seguinte exemplo:

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">
<objectGrids>
    <objectGrid name="grid1">
        <backingMap name="employees" pluginCollectionRef="employees" lockStrategy="OPTIMISTIC" />
    </objectGrid>
</objectGrids>

<backingMapPluginCollections>
    <backingMapPluginCollection id="employees">
        <bean id="OptimisticCallback" className="com.xyz.EmployeeOptimisticCallbackImpl" />
    </backingMapPluginCollection>
</backingMapPluginCollections>
</objectGridConfig>
```

Introdução aos Slots de Plug-in: Java

Um slot de plug-in é um espaço de armazenamento transacional reservado para os plug-ins que compartilham o contexto transacional. Estes slots fornecem uma forma para os plug-ins do eXtreme Scale se comunicarem um com o outro, compartilhar contexto transacional e assegurar que os recursos transacionais sejam usados correta e consistentemente dentro de uma transação.

Um plug-in pode armazenar o contexto transacional, como a conexão com o banco de dados, a conexão com o JMS (Java Message Service), e assim por diante, em um slot de plug-ins. O contexto transacional armazenado pode ser recuperado por qualquer plug-in que conheça o número do slot do plug-in, o qual serve como chave para recuperar o contexto transacional.

Utilizando Slots de Plug-in

Os slots de plug-in são parte da Interface TxID. Consulte a Documentação da API para obter mais informações sobre a interface.Os slots são entradas em uma matriz ArrayList. Os plug-ins podem reservar uma entrada na matriz ArrayList ao chamar o método ObjectGrid.reserveSlot e indicar que requer um slot em todos os objetos TxID. Após reservar os slots, os plug-ins podem inserir um contexto transacional nos slots de cada objeto TxID e recuperá-lo posteriormente. As operações put e get são coordenadas pelos números de slot que são retornados pelo método ObjectGrid.reserveSlot.

Um plug-in normalmente tem um ciclo de vida. A utilização dos slots de plug-in deve se adequar ao ciclo de vida do plug-in. Normalmente, o plug-in deve reservar slots de plug-in durante o estágio de inicialização e obter os números de cada slot. Durante o tempo de execução normal, o plug-in insere contexto transacional no slot reservado no objeto TxID no ponto apropriado. Normalmente, esse ponto apropriado é o início da transação. O plug-in ou outros plug-ins podem, desse modo, obter o contexto provisório armazenado pelo número de slot do TxID dentro da transação.

O plug-in tipicamente executa uma limpeza por meio da remoção do contexto transacional e dos slots. O fragmento de código a seguir ilustra como utilizar os slots de plug-in em um plug-in TransactionCallback:

```
public class DatabaseTransactionCallback implements TransactionCallback {
    int connectionSlot;
    int autoCommitConnectionSlot;
    int psCacheSlot;
    Properties ivProperties = new Properties();

    public void initialize(ObjectGrid objectGrid) throws TransactionCallbackException {
        // In initialization stage, reserve desired plug-in slots by calling the
        //reserveSlot method of ObjectGrid and
        // passing in the designated slot name, TxID.SLOT_NAME.
        // Note: you have to pass in this TxID.SLOT_NAME that is designated
        // for application.
        try {
            // cache the returned slot numbers
            connectionSlot = objectGrid.reserveSlot(TxID.SLOT_NAME);
            psCacheSlot = objectGrid.reserveSlot(TxID.SLOT_NAME);
            autoCommitConnectionSlot = objectGrid.reserveSlot(TxID.SLOT_NAME);
        } catch (Exception e) {
        }
    }

    public void begin(TxID tx) throws TransactionCallbackException {
        // put transactional contexts into the reserved slots at the
        // beginning of the transaction.
        try {
            Connection conn = null;
            conn = DriverManager.getConnection(ivDriverUrl, ivProperties);
            tx.putSlot(connectionSlot, conn);
            conn = DriverManager.getConnection(ivDriverUrl, ivProperties);
            conn.setAutoCommit(true);
            tx.putSlot(autoCommitConnectionSlot, conn);
            tx.putSlot(psCacheSlot, new HashMap());
        } catch (SQLException e) {
            SQLException ex = getLastSQLException(e);
            throw new TransactionCallbackException("unable to get connection", ex);
        }
    }

    public void commit(TxID id) throws TransactionCallbackException {
        // get the stored transactional contexts and use them
        // then, clean up all transactional resources.
        try {
            Connection conn = (Connection) id.getSlot(connectionSlot);
            conn.commit();
            cleanUpSlots(id);
        } catch (SQLException e) {
            SQLException ex = getLastSQLException(e);
            throw new TransactionCallbackException("commit failure", ex);
        }
    }

    void cleanUpSlots(TxID tx) throws TransactionCallbackException {
        closePreparedStatements((Map) tx.getSlot(psCacheSlot));
```

```
        closeConnection((Connection) tx.getSlot(connectionSlot));
        closeConnection((Connection) tx.getSlot(autoCommitConnectionSlot));
    }

    /**
     * @param map
     */
    private void closePreparedStatements(Map psCache) {
        try {
            Collection statements = psCache.values();
            Iterator iter = statements.iterator();
            while (iter.hasNext()) {
                PreparedStatement stmt = (PreparedStatement) iter.next();
                stmt.close();
            }
        } catch (Throwable e) {
        }

    }

    /**
     * Close connection and swallow any Throwable that occurs.
     *
     * @param connection
     */
    private void closeConnection(Connection connection) {
        try {
            connection.close();
        } catch (Throwable e1) {
        }
    }

    public void rollback(TxID id) throws TransactionCallbackException
        // get the stored transactional contexts and use them
        // then, clean up all transactional resources.
        try {
            Connection conn = (Connection) id.getSlot(connectionSlot);
            conn.rollback();
            cleanUpSlots(id);
        } catch (SQLException e) {
        }
    }

    public boolean isExternalTransactionActive(Session session) {
        return false;
    }

    // Getter methods for the slot numbers, other plug-in can obtain the slot numbers
    // from these getter methods.

    public int getConnectionSlot() {
        return connectionSlot;
    }
    public int getAutoCommitConnectionSlot() {
        return autoCommitConnectionSlot;
    }
    public int getPreparedStatementSlot() {
        return psCacheSlot;
    }
```

O fragmento de código a seguir ilustra como um Utilitário de Carga pode obter o contexto transacional armazenado inserido pelo exemplo de plug-in TransactionCallback anterior:

```
public class DatabaseLoader implements Loader
{
    DatabaseTransactionCallback tcb;
    public void preloadMap(Session session, BackingMap backingMap) throws LoaderException {
        // The preload method is the initialization method of the Loader.
        // Obtain interested plug-in from Session or ObjectGrid instance.
        tcb = (DatabaseTransactionCallback)session.getObjectGrid().getTransactionCallback();
    }
    public List get(TxID txid, List keyList, boolean forUpdate) throws LoaderException
    {
        // get the stored transactional contexts that is put by tcb's begin method.
        Connection conn = (Connection)txid.getSlot(tcb.getConnectionSlot());
        // implement get here
        return null;
    }
    public void batchUpdate(TxID txid, LogSequence sequence) throws LoaderException,
OptimisticCollisionException
    {
        // get the stored transactional contexts that is put by tcb's begin method.
        Connection conn = (Connection)txid.getSlot(tcb.getConnectionSlot());
        // implement batch update here ...
    }
}
```

Gerenciadores de Transações Externas: Java

Normalmente, as transações do eXtreme Scale começam com o método Session.begin e terminam com o método Session.commit. Entretanto, quando um ObjectGrid é integrado, um coordenador de transação externa pode iniciar e terminar transações. Nesse caso, você não precisa chamar os métodos begin ou commit.

Coordenação de Transação Externa

O plug-in TransactionCallback é estendido com o método isExternalTransactionActive(Session session) que associa a sessão do eXtreme Scale com uma transação externa. O cabeçalho do método é o seguinte:

```
public synchronized boolean isExternalTransactionActive(Session session)
```

Por exemplo, o eXtreme Scale pode ser configurado para se integrar com o WebSphere Application Server e WebSphere Extended Deployment.

Além disso, o eXtreme Scale oferece um plug-in integrado chamado WebSphere "Plug-ins para o Gerenciamento de Eventos de Ciclo de Vida da Transação" na página 644, que descreve como construir o plug-in para ambientes do WebSphere Application Server, e também adaptar o plug-in para outras estruturas.

A chave para esta integração simples é a exploração da API ExtendedJTATransaction no WebSphere Application Server Versão 7.1. Use o código de amostra a seguir para associar uma sessão ObjectGrid com um ID de transação do WebSphere Application Server:

```
/**
* This method is required to associate an objectGrid session with a WebSphere
* Application Server transaction ID.
*/
Map/**/ localIdToSession;
public synchronized boolean isExternalTransactionActive(Session session)
{
    // lembre-se de que este localid significa que a sessão é salva posteriormente.
    localIdToSession.put(new Integer(jta.getLocalId()), session);
    return true;
}
```

Recuperar uma Transação Externa

Algumas vezes você pode precisar recuperar um objeto de serviço de transação externa para o plug-in TransactionCallback usar. No servidor do WebSphere Application Server, busque o objeto ExtendedJTATransaction de seu espaço de nomes como mostrado no exemplo a seguir:

```
public J2EETransactionCallback() {
    super();
    localIdToSession = new HashMap();
    String lookupName="java:comp/websphere/ExtendedJTATransaction";
    try
    {
        InitialContext ic = new InitialContext();
        jta = (ExtendedJTATransaction)ic.lookup(lookupName);
        jta.registerSynchronizationCallback(this);
    }
    catch(NotSupportedException e)
    {
        throw new RuntimeException("Cannot register jta callback", e);
    }
```

```
    catch(NamingException e){
        throw new RuntimeException("Cannot get transaction object");
    }
}
```

Para outros produtos, é possível utilizar uma abordagem semelhante para recuperar o objeto de serviço de transações.

Controlar Confirmação por Retorno de Chamada Externo

O plug-in TransactionCallback precisa receber um sinal externo para confirmar ou recuperar a sessão do eXtreme Scale. Para receber este sinal externo, utilize o retorno de chamada do serviço de transações externas. Implemente a interface de retorno de chamada externa e registre-a no serviço de transações externas. Por exemplo, com WebSphere Application Server implemente a interface SynchronizationCallback como mostrado no exemplo a seguir:

```
public class J2EETransactionCallback implements
 com.ibm.websphere.objectgrid.plugins.TransactionCallback, SynchronizationCallback {
   public J2EETransactionCallback() {
      super();
      String lookupName="java:comp/websphere/ExtendedJTATransaction";
      localIdToSession = new HashMap();
      try {
         InitialContext ic = new InitialContext();
         jta = (ExtendedJTATransaction)ic.lookup(lookupName);
         jta.registerSynchronizationCallback(this);
      } catch(NotSupportedException e) {
         throw new RuntimeException("Cannot register jta callback", e);
      }
      catch(NamingException e){
         throw new RuntimeException("Cannot get transaction object");
      }
   }

   public synchronized void afterCompletion(int localId, byte[] arg1,boolean didCommit) {
      Integer lid = new Integer(localId);
      // find the Session for the localId
      Session session = (Session)localIdToSession.get(lid);
      if(session != null) {
          try {
            // if WebSphere Application Server is committed when
            // hardening the transaction to backingMap.
            // We already did a flush in beforeCompletion
            if(didCommit) {
               session.commit();
            } else {
               // otherwise rollback
               session.rollback();
            }
         } catch(NoActiveTransactionException e) {
            // impossible in theory
         } catch(TransactionException e) {
            // given that we already did a flush, this should not fail
         } finally {
            // always clear the session from the mapping map.
            localIdToSession.remove(lid);
         }
      }
   }

   public synchronized void beforeCompletion(int localId, byte[] arg1) {
      Session session = (Session)localIdToSession.get(new Integer(localId));
      if(session != null) {
         try {
            session.flush();
         } catch(TransactionException e) {
            // WebSphere Application Server  does not formally define
            // a way to signal the
            // transaction has failed so do this
            throw new RuntimeException("Cache flush failed", e);
         }
      }
   }
}
```

Use as APIs do eXtreme Scale com o plug-in TransactionCallback

O plug-in TransactionCallback desativa a auto-consolidação no eXtreme Scale. O padrão de uso normal para um eXtreme Scale é o seguinte:

```
Session ogSession = ...;
ObjectMap myMap = ogSession.getMap("MyMap");
ogSession.begin();
MyObject v = myMap.get("key");
v.setAttribute("newValue");
myMap.update("key", v);
ogSession.commit();
```

Quando este plug-in TransactionCallback está em uso, o eXtreme Scale assume que o aplicativo usa o eXtreme Scale quando uma transação gerenciada pelo contêiner está presente. O trecho de código anterior muda o seguinte código neste ambiente:

```
public void myMethod() {
   UserTransaction tx = ...;
   tx.begin();
   Session ogSession = ...;
   ObjectMap myMap = ogSession.getMap("MyMap");
   yObject v = myMap.get("key");
   v.setAttribute("newValue");
   myMap.update("key", v);
   tx.commit();
}
```

O método myMethod é semelhante a um cenário de aplicativo da Web. O aplicativo usa a interface UserTransaction normal para iniciar, consolidar e recuperar transações. O eXtreme Scale automaticam ente inicia e consolida a transação do contêiner. Se o método for um método EJB (Enterprise JavaBeans) que usa o atributo TX_REQUIRES, então remova a referência UserTransaction e as chamadas para iniciar e consolidar transações e o método funciona da mesma forma. Neste caso, o contêiner é responsável por iniciar e encerrar a transação.

Plug-in WebSphereTransactionCallback: Java

Ao usar o plug-in WebSphereTransactionCallback, os aplicativos corporativos que estão em execução em um ambiente do WebSphere Application Server podem gerenciar as transações do ObjectGrid. Esse plug-in foi descontinuado. Use o adaptador de recursos do WebSphere eXtreme Scale em vez disso.

 A interface WebSphereTransactionCallback foi substituída pelo adaptador de recursos do WebSphere eXtreme Scale o que ativa o gerenciamento de transações do Java Transaction API (JTA). É possível instalar esse adaptador de recursos do WebSphere Application Server ou outros servidores de aplicativos Java Platform, Enterprise Edition (Java EE). O plug-in WebSphereTransactionCallback não é uma API JTA relacionada e, portanto, não é designada para retroceder a transação JTA se a confirmação falhar.

Quando você está usando uma sessão do ObjectGrid dentro de um método que está configurado para usar transações gerenciadas por contêiner, o contêiner corporativo automaticamente inicia, consolida ou recupera a transação do ObjectGrid. Ao usar os objetos UserTransaction do Java Transaction API (JTA), a transação ObjectGrid será gerenciada automaticamente pelo objeto UserTransaction.

Para uma discussão detalhada da implementação deste plug-in, consulte “Gerenciadores de Transações Externas” na página 651.

Nota: O ObjectGrid não suporta transações XA, 2-phase. Este plug-in não relaciona a transação do ObjectGrid com o gerenciador de transações. Assim, se o ObjectGrid falhar ao consolidar, todos os outros recursos que são gerenciados pela transação XA não são recuperados.

Conectar Programaticamente no Objeto WebSphereTransactionCallback

É possível ativar o WebSphereTransactionCallback na configuração ObjectGrid com a configuração programática ou XML. O fragmento de código a seguir usa o aplicativo para criar o objeto WebSphereTransactionCallback e o inclui em um ObjectGrid:

```
ObjectGridManager objectGridManager = ObjectGridManagerFactory.getObjectGridManager();
ObjectGrid myGrid = objectGridManager.createObjectGrid("myGrid", false);
WebSphereTransactionCallback wsTxCallback= new WebSphereTransactionCallback ();
myGrid.setTransactionCallback(wsTxCallback);
```

Abordagem de configuração XML para conectar o objeto WebSphereTransactionCallback

A seguinte configuração XML cria o objeto WebSphereTransactionCallback e o inclui em um ObjectGrid. O texto a seguir deve estar no arquivo `myGrid.xml`:

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
    xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="myGrid">
            <bean id="TransactionCallback" className="com.ibm.websphere.objectgrid.plugins.builtins.WebSphereTransactionCallback" />

        </objectGrid>
    </objectGrids>
</objectGridConfig>
```

Programando para Usar a Estrutura do OSGi

Java

Os servidores e clientes do eXtreme Scale podem ser iniciados em um contêiner OSGi para poder incluir e atualizar dinamicamente plug-ins do eXtreme Scale no ambiente de tempo de execução.

Conceitos relacionados:

Java "Visão Geral da Programação do Serialziador" na página 560
É possível usar os plug-ins do DataSerializer para gravar serializadores otimizados para armazenar objetos Java e outros dados no formato binário na grade. O plug-in também fornece métodos que você pode usar para atributos de consulta dentro dos dados binários sem exigir que o objeto de dados inteiro seja expandido.

Java Visão Geral da Serialização
Os dados são sempre expressos, porém não necessariamente armazenados, como objetos Java na grade de dados. O WebSphere eXtreme Scale usa diversos processos Java para serializar os dados, ao converter as instâncias de objetos Java em bytes e retornar para os objetos novamente, conforme necessário, para mover os dados entre os processos do cliente e do servidor.

Java Amostras

Informações relacionadas:

Java Documentação da API do DataSerializer

Construindo Plug-ins Dinâmicos do eXtreme Scale

Java

O WebSphere eXtreme Scale inclui plug-ins ObjectGrid e BackingMap. Estes plug-ins são implementados em Java e são configurados usando o arquivo XML do descritor do ObjectGrid. Para criar um plug-in dinâmico que pode ser dinamicamente atualizado, eles precisam estar cientes dos eventos de ciclo de vida de ObjectGrid e BackingMap porque eles podem precisar concluir algumas ações

durante uma atualização. Aprimorar um pacote configurável de plug-in com métodos de retorno de chamada, listeners de eventos, ou ambos, do ciclo de vida permite que o plug-in conclua essas ações em momentos apropriados.

Antes de Iniciar

Este tópico supõe que você construiu o plug-in apropriado. Para obter informações adicionais sobre como desenvolver plug-ins do eXtreme Scale, consulte o tópico APIs e Plug-ins do Sistema.

Sobre Esta Tarefa

Todos os plug-ins do eXtreme Scale se aplicam a uma instância de BackingMap ou de ObjectGrid. Muitos plug-ins também interagem com outros plug-ins. Por exemplo, um plug-in Loader e TransactionCallback trabalham juntos para interagir corretamente com uma transação do banco de dados e as várias chamadas de banco de dados JDBC. Alguns plug-ins também pode precisar armazenar em cache dados de configuração a partir de outros plug-ins para melhorar o desempenho.

Os plug-ins BackingMapLifecycleListener e ObjectGridLifecycleListener fornecem operações de ciclo de vida para as respectivas instâncias de BackingMap e ObjectGrid. Este processo permite que plug-ins sejam notificados quando o BackingMap ou ObjectGrid pai e seus respectivos plug-ins podem ser alterados. Os plug-ins BackingMap implementam a interface de BackingMapLifecyleListener e os plug-ins ObjectGrid implementam a interface de ObjectGridLifecycleListener. Estes plug-ins são chamados automaticamente quando o ciclo de vida do BackingMap ou ObjectGrid pai é alterado. Para obter mais informações sobre os plug-ins de ciclo de vida, consulte o tópico “Gerenciando Ciclos de Vida de Plug-in” na página 548.

É possível aprimorar os pacotes configuráveis usando os métodos ou os listeners de evento do ciclo de vida nas seguintes tarefas comuns:

- Iniciar e parar recursos, como encadeamentos ou assinantes de sistema de mensagens.
- Especificar que uma notificação ocorra quando os plug-ins equivalentes forem atualizados, permitindo o acesso direto ao plug-in e a detecção de quaisquer mudanças.

Sempre que outro plug-in for acessado diretamente, acesse esse plug-in por meio do contêiner OSGi para assegurar que todas as partes do sistema referenciem o plug-in correto. Se, por exemplo, algum componente no aplicativo referenciar diretamente, ou armazenar em cache, uma instância de um plug-in, ele manterá sua referência para essa versão do plug-in, mesmo depois que o plug-in tiver sido atualizado dinamicamente. Esse comportamento pode causar problemas relacionados ao aplicativo, bem como fugas de memória. Portanto, grave o código que depende dos plug-ins dinâmicos que obtêm sua referência usando semânticas getService() do OSGi. Se o aplicativo precisar armazenar em cache um ou mais plug-ins, ele atenderá eventos de ciclo de vida usando interfaces ObjectGridLifecycleListener e BackingMapLifecycleListener. O aplicativo também deve poder atualizar seu cache quando necessário, de modo thread safe.

Todos os plug-ins do eXtreme Scale usados com o OSGi também devem implementar as respectivas interfaces BackingMapPlugin ou ObjectGridPlugin. Novos plug-ins, tal como a interface MapSerializerPlugin impingem essa prática.

Essas interfaces fornecem ao ambiente de tempo de execução do eXtreme Scale e ao OSGi uma interface consistente para injeção de estado no plug-in e controle de seu ciclo de vida.

Ao usar esta tarefa para especificar que uma notificação ocorre quando os plug-ins equivalentes são atualizados, é possível criar um factory de listener que produz uma instância do listener.

Procedimento

- Atualize a classe de plug-in ObjectGrid para implementar a interface ObjectGridPlugin. Esta interface inclui métodos que permitem que o eXtreme Scale inicialize, configure a instância do ObjectGrid e destrua o plug-in. Consulte o exemplo de código a seguir:

```
package com.mycompany;
import com.ibm.websphere.objectgrid.plugins.ObjectGridPlugin;
...

public class MyTranCallback implements TransactionCallback, ObjectGridPlugin {

    private ObjectGrid og = null;

    private enum State {
        NEW, INITIALIZED, DESTROYED
    }

    private State state = State.NEW;

    public void setObjectGrid(ObjectGrid grid) {
        this.og = grid;
    }

    public ObjectGrid getObjectGrid() {
        return this.og;
    }
    void initialize() {
        // Handle any plug-in initialization here.  This is called by
        // eXtreme Scale, and not the OSGi bean manager.
        state = State.INITIALIZED;
    }
    boolean isInitialized() {
        return state == State.INITIALIZED;
    }

    public void destroy() {
        // Destroy the plug-in and release any resources.  This
        // can be callsed by the OSGi Bean Manager or by eXtreme Scale.
        state = State.DESTROYED;
    }

    public boolean isDestroyed() {
        return state == State.DESTROYED;
    }
}
```

- Atualize a classe de plug-in do ObjectGrid para implementar a interface ObjectGridLifecycleListener. Consulte o exemplo de código a seguir:

```
package com.mycompany;
import com.ibm.websphere.objectgrid.plugins.ObjectGridLifecycleListener;
      import com.ibm.websphere.objectgrid.plugins.ObjectGridLifecycleListener.LifecycleEvent;
      ...

      public class MyTranCallback implements TransactionCallback, ObjectGridPlugin, ObjectGridLifecycleListener{
          public void objectGridStateChanged(LifecycleEvent event) {
              switch(event.getState()) {
              case NEW:
              case DESTROYED:
              case DESTROYING:
              case INITIALIZING:
                  break;
              case INITIALIZED:
                  // Lookup a Loader or MapSerializerPlugin using
                  // OSGi or directly from the ObjectGrid instance.
                  lookupOtherPlugins()
                  break;
              case STARTING:
              case PRELOAD:
                  break;
              case ONLINE:
                  if (event.isWritable()) {
                      startupProcessingForPrimary();
                  } else {
                      startupProcessingForReplica();
                  }
```

```
                break;
            case QUIESCE:
                if (event.isWritable()) {
                    quiesceProcessingForPrimary();
                } else {
                    quiesceProcessingForReplica();
                }
                break;
            case OFFLINE:
                shutdownShardComponents();
                break;
            }
        }
        ...
    }
```

- Atualize um plug-in do BackingMap. Atualize a classe de plug-in do BackingMap para implementar a interface de plug-in do BackingMap. Esta interface inclui métodos que permitem que o eXtreme Scale inicialize, configure a instância do BackingMap e destrua o plug-in. Consulte o exemplo de código a seguir:

```
package com.mycompany;
import com.ibm.websphere.objectgrid.plugins.BackingMapPlugin;
...

public class MyLoader implements Loader, BackingMapPlugin {

    private BackingMap bmap = null;

    private enum State {
        NEW, INITIALIZED, DESTROYED
    }

    private State state = State.NEW;

    public void setBackingMap(BackingMap map) {
        this.bmap = map;
    }

    public BackingMap getBackingMap() {
        return this.bmap;
    }
    void initialize() {
        // Handle any plug-in initialization here.  This is called by
        // eXtreme Scale, and not the OSGi bean manager.
        state = State.INITIALIZED;
    }
    boolean isInitialized() {
        return state == State.INITIALIZED;
    }

    public void destroy() {
        // Destroy the plug-in and release any resources.  This
        // can be callsed by the OSGi Bean Manager or by eXtreme Scale.
        state = State.DESTROYED;
    }

    public boolean isDestroyed() {
        return state == State.DESTROYED;
    }
}
```

- Atualize a classe de plug-in do BackingMap para implementar a interface BackingMapLifecycleListener. Consulte o exemplo de código a seguir:

```
package com.mycompany;

      import com.ibm.websphere.objectgrid.plugins.BackingMapLifecycleListener;
      import com.ibm.websphere.objectgrid.plugins.BackingMapLifecycleListener.LifecycleEvent;
      ...

      public class MyLoader implements Loader, ObjectGridPlugin, ObjectGridLifecycleListener{
          ...
          public void backingMapStateChanged(LifecycleEvent event) {
              switch(event.getState()) {
              case NEW:
              case DESTROYED:
              case DESTROYING:
              case INITIALIZING:
                  break;
              case INITIALIZED:
                  // Lookup a MapSerializerPlugin using
                  // OSGi or directly from the ObjectGrid instance.
                  lookupOtherPlugins()
                  break;
              case STARTING:
              case PRELOAD:
                  break;
              case ONLINE:
                  if (event.isWritable()) {
```

```
                startupProcessingForPrimary();
            } else {
                startupProcessingForReplica();
            }
            break;
        case QUIESCE:
            if (event.isWritable()) {
                quiesceProcessingForPrimary();
            } else {
                quiesceProcessingForReplica();
            }
            break;
        case OFFLINE:
            shutdownShardComponents();
            break;
        }
    }
    ...
}
```

Resultados

Implementando a interface ObjectGridPlugin ou BackingMapPlugin, o eXtreme Scale pode controlar o ciclo de vida de seu plug-in nos momentos certos.

Implementando a interface ObjectGridLifecycleListener ou BackingMapLifecycleListener, o plug-in é automaticamente registrado como um listener dos eventos de ciclo de vida do ObjectGrid ou do BackingMap associados. O evento INITIALIZING é usado para sinalizar que todos os plug-ins do ObjectGrid e do BackingMap foram inicializados e estão disponíveis para consultar e usar. O evento ONLINE é usado para sinalizar que o ObjectGrid está on-line e pronto para iniciar eventos de processamento.

Programação para Integração de JPA

Java

O Java Persistence API (JPA) é uma especificação que permite o mapeamento de objetos Java para bancos de dados relacionais. O JPA contém uma especificação completa de object-relational mapping (ORM) usando anotações de metadados da linguagem Java, descritores XML, ou ambos para definir o mapeamento entre objetos Java e um banco de dados relacional. Inúmeras implementações comerciais e de software livre estão disponíveis.

Para usar o JPA, é necessário ter um provedor JPA suportado, como OpenJPA ou Hibernate, arquivos JAR e um arquivo`META-INF/persistence.xml` no seu caminho da classe.

Tarefas relacionadas:

"Resolução de Problemas de Carregadores" na página 880
Use estas informações para resolver problemas com os carregadores de banco de dados.

Configurando Utilitários de Carga do JPA
Um Utilitário de Carga do Java Persistence API (JPA) é uma implementação de plug-in que utiliza JPA para interagir com o banco de dados.

Carregadores JPA

Java

O Java Persistence API (JPA) é uma especificação que permite o mapeamento de objetos Java para bancos de dados relacionais. O JPA contém uma especificação completa de object-relational mapping (ORM) usando anotações de metadados da

linguagem Java, descritores XML, ou ambos para definir o mapeamento entre objetos Java e um banco de dados relacional. Inúmeras implementações comerciais e de software livre estão disponíveis.

É possível utilizar uma implementação de plug-in de utilitário de carga do Java Persistence API (JPA) com eXtreme Scale para interagir com qualquer banco de dados suportado por seu utilitário de carga escolhido. Para usar o JPA, é necessário ter um provedor JPA suportado, como OpenJPA ou Hibernate, arquivos JAR e um arquivo`META-INF/persistence.xml` no seu caminho da classe.

Os plug-ins JPALoader com.ibm.websphere.objectgrid.jpa.JPALoader e JPAEntityLoader com.ibm.websphere.objectgrid.jpa.JPAEntityLoader são dois plug-ins do utilitário de carga do JPA integrados que são usados para sincronizar os mapas do ObjectGrid com um banco de dados. É necessário ter uma implementação do JPA, como Hibernate ou OpenJPA, para usar este recurso. O banco de dados pode ser qualquer back end que seja suportado pelo provedor JPA escolhido.

É possível usar o plug-in do JPALoader ao armazenar dados usando a API ObjectMap. Use o plug-in do JPAEntityLoader ao armazenar dados usando a API EntityManager.

Arquitetura do Utilitário de Carga do JPA

O Utilitário de Carga do JPA é usado para mapas do eXtreme Scale que armazenam objetos Java antigos simples (POJO).

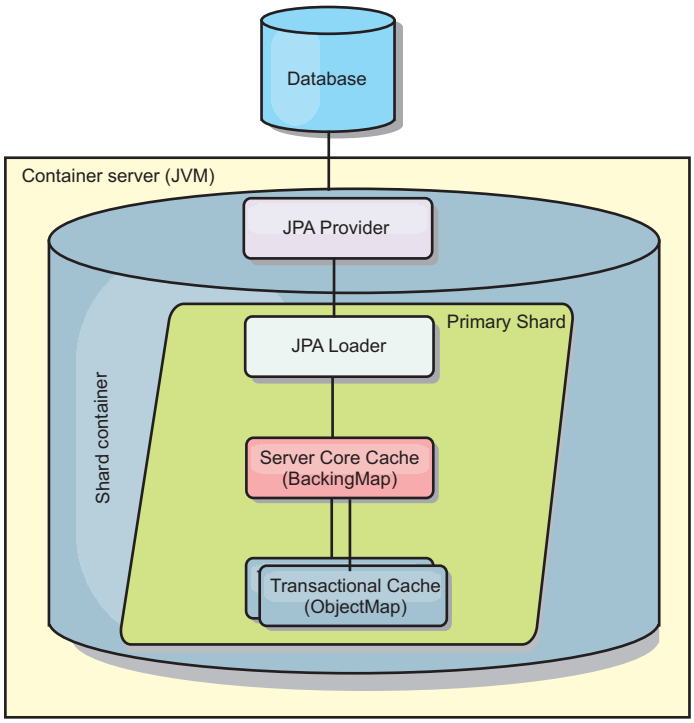


Figura 42. Arquitetura do Utilitário de Carga do JPA

Quando um método ObjectMap.get(Object key) é chamado, o eXtreme Scale executa as primeiras verificações se a entrada está contida na camada do ObjectMap. Se não, o tempo de execução delega a solicitação ao Utilitário de Carga

do JPA. Sob solicitação de carregamento da chave, o JPALoader chama o método EntityManager.find(Object key) do JPA para localizar os dados de uma camada do JPA. Se os dados estiverem contidos no gerenciador de entidades JPA, ele serão retornados; caso contrário, o provedor JPA interage com o banco de dados para obter o valor.

Quando uma atualização para o ObjectMap ocorre, por exemplo, usando o método ObjectMap.update(Objectkey, Object value), o tempo de execução do eXtreme Scale cria um LogElement para esta atualização e a envia para o JPALoader. O JPALoader chama o método EntityManager.merge(Object value) do JPA para atualizar o valor no banco de dados.

Para o JPAEntityLoader, as mesmas quatro camadas estão envolvidas. Porém, como o plug-in JPAEntityLoader é usado para mapas que armazenam entidades do eXtreme Scale, as relações entre as entidades poderiam complicar o cenário de uso. Uma entidade do eXtreme Scale é diferenciada de uma entidade do JPA. Para obter mais detalhes, consulte o "Plug-in JPAEntityLoader" na página 631.Para obter mais informações, consulte o "Plug-in JPAEntityLoader" na página 631.Para obter mais informações, consulte o plug-in JPAEntityLoader no *Guia de Programação*.

Métodos

Utilitários de Carga Fornecem Três Métodos Principais:

1. get: Retorna uma lista de valores que corresponde à lista de chaves que são passadas por meio da recuperação de dados usando o JPA. O método usa o JPA para localizar as entidades no banco de dados. Para o plug-inJPALoader, a lista retornada contém uma lista de entidades JPA diretamente a partir da operação find. Para o plug-in JPAEntityLoader, a lista retornada contém tuplas do valor da entidade de eXtreme Scale convertidas de entidades do JPA.
2. batchUpdate: grava os dados dos mapas do ObjectGrid para o banco de dados. Dependendo dos diferentes tipos de operação (inserir, atualizar ou excluir), o utilitário de carga usa as operações de persistir, mesclar ou remover para atualizar os dados para o banco de dados. Para o JPALoader, os objetos no mapa são utilizados diretamente como entidades JPA. Para o JPAEntityLoader, as tuplas de entidade no mapa são convertidas nos objetos que são utilizados como entidades JPA.
3. preloadMap: Pré-carrega o mapa usando o método do utilitário de carga do ClientLoader.load. Para mapas particionados, o método preloadMap é chamado apenas em uma partição. A partição é especificada na propriedade preloadPartition da classe JPALoader ou JPAEntityLoader. Se o valor de preloadPartition for configurado para menor que zero ou maior que (*total_number_of_partitions* - 1), o pré-carregamento será desativado.

Ambos os plug-ins JPALoader e JPAEntityLoader funcionam com a classe JPATxCallback para coordenar as transações do eXtreme Scale e as transações do JPA. O JPATxCallback precisa ser configurado na instância do ObjectGrid para utilizar estes dois utilitários de carga.

Configuração e Programação

Se você estiver usando os carregadores JPA em um ambiente multimestre, consulte o "Considerações Sobre o Carregador em uma Topologia Multimestre" na página 289. Para obter mais informações sobre como configurar os carregadores do JPA, consulte Configurando Utilitários de Carga do JPA. Para obter mais informações sobre como programar os carregadores JPA, consulte o "Considerações sobre a

Programação do Utilitário de Carga do JPA" na página 628.

Desenvolvendo Carregadores JPA Baseados em Cliente

Java

É possível implementar o pré-carregamento e o recarregamento de dados no seu aplicativo usando o utilitário Java Persistence API (JPA). Este recurso pode simplificar o carregamento dos mapas quando as consultas ao banco de dados não puderem ser particionadas.

Antes de Iniciar

- Um provedor de JPA deve ser usado com um banco de dados suportado.
- Antes de pré-carregar ou de recarregar os mapas, você deve configurar o estado de disponibilidade de um ObjectGrid para `PRELOAD`. É possível configurar o estado de disponibilidade com o método setObjectGridState da interface StateManager. A interface StateManager impede que outros clientes acessem o ObjectGrid quando ainda não estiver on-line. Depois de pré-carregar ou de recarregar o mapa, o estado pode ser configurado de volta para ONLINE.
- Quando estiver pré-carregando mapas diferentes em um ObjectGrid, configure o estado ObjectGrid para `PRELOAD` uma vez e configure o valor de volta para `ONLINE` depois que todos os mapas concluírem o carregamento dos dados. Esta coordenação pode ser feita pela interface ClientLoadCallback. Configure o estado ObjectGrid para `PRELOAD` após a primeira notificação preStart a partir da instância ObjectGrid e configure-a de volta para `ONLINE` após a última notificação postFinish.
- Se for necessário pré-carregar mapas de diferentes Java Virtual Machines, será necessário coordenar entre várias Java Virtual Machines. Configure o estado de ObjectGrid para `PRELOAD` uma vez antes de o primeiro mapa ser pré-carregado em qualquer uma das Java Virtual Machines e configure o valor de volta para `ONLINE` depois que todos os mapas concluírem o carregamento de dados em todas as Java Virtual Machines. Para obter informações adicionais, consulte Gerenciando a Disponibilidade do ObjectGrid.

Sobre Esta Tarefa

Quando executar uma operação de pré-carregamento ou de recarregamento no mapa, as seguintes ações ocorrerão:

1. A ação inicial a ser executada depende de se uma operação de pré-carregamento ou de recarregamento está sendo executada.
   - **Operação de pré-carregamento:** O mapa a ser pré-carregado é limpo. Para um mapa de entidade, se qualquer relação for configurada como remoção em cascata, quaisquer mapas relacionados são limpos.
   - **Operação de recarregamento:** A consulta fornecida é executada no mapa e os resultados são invalidados. Para um mapa de entidade, se qualquer relação for configurada com a opção **`CascadeType.INVALIDATE`**, as entidades relacionadas também serão invalidadas a partir dos seus mapas.
2. Execute a consulta ao JPA para as entidades em um lote.
3. Para cada lote, uma lista de chaves e uma lista de valores para cada partição são construídas.
4. Para cada partição, o agente da grade de dados é chamado para inserir ou atualizar os dados no lado do servidor diretamente se ele for um cliente do eXtreme Scale. Se a grade de dados for uma instância local, os dados nos mapas serão inseridos ou atualizados diretamente.

Conceitos relacionados:

Java "Visão Geral do Utilitário de Pré-Carregamento JPA Baseado em Cliente"
O utilitário de pré-carregamento Java Persistence API (JPA) baseado em cliente carrega dados nos mapas de apoio do eXtreme Scale usando uma conexão de cliente para o ObjectGrid.

Referências relacionadas:

Java "Exemplo: Pré-carregando um Mapa com a Interface ClientLoader" na página 664
É possível pré-carregar um mapa para preencher os dados do mapa antes que os clientes comecem a acessar o mapa.

Java "Exemplo: Recarregando um Mapa com a Interface ClientLoader" na página 665
Recarregar um mapa é o mesmo que pré-carregar um mapa, exceto que o argumento **isPreload** é configurado para false no método ClientLoader.load.

Java "Exemplo: Chamando um Carregador do Cliente" na página 666
É possível usar o método de pré-carregamento na interface Loader para chamar um carregador do cliente.

Informações relacionadas:

Java Interface ClientLoader

Java Interface StateManager

Visão Geral do Utilitário de Pré-Carregamento JPA Baseado em Cliente:

Java

O utilitário de pré-carregamento Java Persistence API (JPA) baseado em cliente carrega dados nos mapas de apoio do eXtreme Scale usando uma conexão de cliente para o ObjectGrid.

Este recurso pode simplificar o carregamento dos mapas quando as consultas ao banco de dados não puderem ser particionadas. Um carregador, como um Carregador JPA também pode ser usado e é ideal quando os dados podem ser carregados em paralelo.

O utilitário de pré-carregamento JPZ baseado em cliente pode usar as implementações de OpenJPA ou Hibernate para carregar o ObjectGrid de um banco de dados. Porque oWebSphere eXtreme Scale não interage diretamente com o banco de dados ou o Java Database Connectivity (JDBC), qualquer banco de dados que o OpenJPA ou o Hibernate suporta pode ser usado para carregar o ObjectGrid.

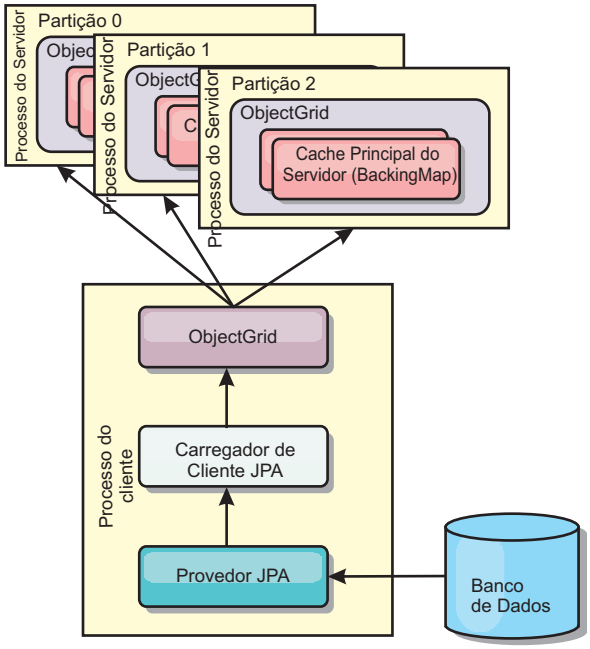


Figura 43. Utilitário de Carga do Cliente que usa Implementação JPA para Carregar o ObjectGrid

Normalmente, um aplicativo de usuário fornece um nome de unidade de persistência, um nome de classe de entidade e uma consulta JPA para o utilitário de carga do cliente. O utilitário de carga do cliente recupera o gerenciador de entidades JPA baseado no nome da unidade de persistência, utiliza o gerenciador de entidades para consultar dados do banco de dados com a classe de entidade fornecida e a consulta JPA e, finalmente, carrega os dados nos mapas distribuídos do ObjectGrid. Quando relações de múltiplos níveis estão envolvidas na consulta, é possível usar uma cadeia de consulta customizada para otimizar o desempenho. Opcionalmente, uma mapa de propriedade de persistência poderia ser fornecido para substituir as propriedades de persistência configuradas.

Um utilitário de carga do cliente pode carregar dados em dois modos diferentes, como exibidos na tabela a seguir:

Tabela 23. Modos do Utilitário de Carga do Cliente

Modo	Descrição
Pré-carregar	Limpa e carrega todas as entradas no mapa de apoio. Se o mapa for um mapa de entidade, quaisquer mapas de entidade relacionados também serão limpos se a opção CascadeType.REMOVE do ObjectGrid estiver ativada.
Recarregar	A consulta JPA é executada junto ao ObjectGrid para invalidar todas as entidades no mapa que correspondem à consulta. Se o mapa for um mapa de entidade, quaisquer mapas de entidade relacionados também serão limpos se a opção CascadeType.INVALIDATE do ObjectGrid estiver ativada.

Em qualquer um dos casos, uma consulta JPA é utilizada para selecionar e carregar as entidades desejadas a partir do banco de dados e armazená-las nos mapas do ObjectGrid. Se o mapa do ObjectGrid for um mapa de não-entidade, as entidades JPA serão separadas e armazenadas diretamente. Se o mapa do ObjectGrid for um mapa de entidade, as entidades JPA serão armazenadas como tuplas de entidade do ObjectGrid. É possível fornecer uma consulta JPA ou utilizar a consulta padrão `select o from EntityName o`.

Para obter mais informações sobre como configurar o utilitário de pré-carregamento do JPA baseado em cliente, consulte o "Desenvolvendo Carregadores JPA Baseados em Cliente" na página 661

Tarefas relacionadas:

Java "Desenvolvendo Carregadores JPA Baseados em Cliente" na página 661
É possível implementar o pré-carregamento e o recarregamento de dados no seu aplicativo usando o utilitário Java Persistence API (JPA). Este recurso pode simplificar o carregamento dos mapas quando as consultas ao banco de dados não puderem ser particionadas.

Referências relacionadas:

Java "Exemplo: Pré-carregando um Mapa com a Interface ClientLoader"
É possível pré-carregar um mapa para preencher os dados do mapa antes que os clientes comecem a acessar o mapa.

Java "Exemplo: Recarregando um Mapa com a Interface ClientLoader" na página 665
Recarregar um mapa é o mesmo que pré-carregar um mapa, exceto que o argumento **`isPreload`** é configurado para false no método ClientLoader.load.

Java "Exemplo: Chamando um Carregador do Cliente" na página 666
É possível usar o método de pré-carregamento na interface Loader para chamar um carregador do cliente.

Informações relacionadas:

Java Interface ClientLoader

Java Interface StateManager

Exemplo: Pré-carregando um Mapa com a Interface ClientLoader: Java

É possível pré-carregar um mapa para preencher os dados do mapa antes que os clientes comecem a acessar o mapa.

Exemplo de Pré-Carregamento Baseado no Cliente

O seguinte trecho de código de amostra mostra um carregamento de cliente simples. Neste exemplo, o mapa CUSTOMER é configurado como um mapa de entidade. A classe de entidade Customer, que é configurada no arquivo descritor XML de metadados da entidade ObjectGrid, possui uma relação de um para muitos com as entidades Order. A entidade Customer possui a opção CascadeType.ALL ativada na relação com a entidade Order. Antes que o método ClientLoader.load seja chamado, o estado ObjectGrid é configurado para PRELOAD. O parâmetro **`isPreload`** no método de carregamento é configurado para `true`.

```
// Get the StateManager
StateManager stateMgr = StateManagerFactory.getStateManager();

// Set ObjectGrid state to PRELOAD before calling ClientLoader.loader
stateMgr.setObjectGridState(AvailabilityState.PRELOAD, objectGrid);
```

```
ClientLoader c = ClientLoaderFactory.getClientLoader();

// Load the data
c.load(objectGrid, "CUSTOMER", "customerPU", null,
    null, null, null, true, null);

// Set ObjectGrid state back to ONLINE
stateMgr.setObjectGridState(AvailabilityState.ONLINE, objectGrid);
```

Conceitos relacionados:

Java "Visão Geral do Utilitário de Pré-Carregamento JPA Baseado em Cliente" na página 662
O utilitário de pré-carregamento Java Persistence API (JPA) baseado em cliente carrega dados nos mapas de apoio do eXtreme Scale usando uma conexão de cliente para o ObjectGrid.

Tarefas relacionadas:

Java "Desenvolvendo Carregadores JPA Baseados em Cliente" na página 661
É possível implementar o pré-carregamento e o recarregamento de dados no seu aplicativo usando o utilitário Java Persistence API (JPA). Este recurso pode simplificar o carregamento dos mapas quando as consultas ao banco de dados não puderem ser particionadas.

Informações relacionadas:

Java Interface ClientLoader

Java Interface StateManager

Exemplo: Recarregando um Mapa com a Interface ClientLoader: Java

Recarregar um mapa é o mesmo que pré-carregar um mapa, exceto que o argumento **isPreload** é configurado para false no método ClientLoader.load.

Exemplo de Recarregamento Baseado no Cliente

A seguinte amostra ilustra como recarregar mapas. Comparado com a amostra de pré-carregamento, a diferença principal é que o loadSql e os parâmetros são fornecidos. Esta amostra recarrega apenas os dados do Cliente com um ID entre 1000 e 2000. O parâmetro **isPreload** no método de carregamento é configurado para false.

```
// Get the StateManager
StateManager stateMgr = StateManagerFactory.getStateManager();

// Set ObjectGrid state to PRELOAD before calling ClientLoader.loader
stateMgr.setObjectGridState(AvailabilityState.PRELOAD, objectGrid);

ClientLoader c = ClientLoaderFactory.getClientLoader();

// Load the data
String loadSql = "select c from CUSTOMER c
    where c.custId >= :startCustId and c.custId < :endCustId ";
Map<String, Long> params = new HashMap<String, Long>();
params.put("startCustId", 1000L);
params.put("endCustId", 2000L);

c.load(objectGrid, "CUSTOMER", "customerPU", null, null,
    loadSql, params, false, null);

// Set ObjectGrid state back to ONLINE
stateMgr.setObjectGridState(AvailabilityState.ONLINE, objectGrid);
```

Lembre-se: Esta sequência de consulta observa as duas sintaxes de consulta JPA e a sintaxe de consulta da entidade eXtreme Scale . Essa sequência de consulta é importante porque ela é executada duas vezes: para invalidar as entidades ObjectGrid correspondidas e para carregar as entidades do JPA correspondidas.

Conceitos relacionados:

Java "Visão Geral do Utilitário de Pré-Carregamento JPA Baseado em Cliente" na página 662
O utilitário de pré-carregamento Java Persistence API (JPA) baseado em cliente carrega dados nos mapas de apoio do eXtreme Scale usando uma conexão de cliente para o ObjectGrid.

Tarefas relacionadas:

Java "Desenvolvendo Carregadores JPA Baseados em Cliente" na página 661
É possível implementar o pré-carregamento e o recarregamento de dados no seu aplicativo usando o utilitário Java Persistence API (JPA). Este recurso pode simplificar o carregamento dos mapas quando as consultas ao banco de dados não puderem ser particionadas.

Informações relacionadas:

Java Interface ClientLoader

Java Interface StateManager

Exemplo: Chamando um Carregador do Cliente: Java

É possível usar o método de pré-carregamento na interface Loader para chamar um carregador do cliente.

Use o método de pré-carregamento na interface Loader para chamar um carregador do cliente:

```
void preloadMap(Session session, BackingMap backingMap) throws LoaderException;
```

Este método sinaliza ao utilitário de carga para pré-carregar os dados no mapa. Uma implementação do utilitário de carga pode utilizar um utilitário de carga do cliente para pré-carregar os dados em todas as suas partições. Por exemplo, o utilitário de carga do JPA usa o utilitário de carga do cliente para pré-carregar os dados no mapa. Consulte "Visão Geral do Utilitário de Pré-Carregamento JPA Baseado em Cliente" na página 662 para obter informações adicionais.

Exemplo: Chamando um Carregador de Cliente com o Método preloadMap

A seguir há um exemplo de como pré-carregar o mapa usando o utilitário de carga do cliente no método preloadMap. O exemplo primeiro verifica se o número da partição atual é o mesmo que o da partição pré-carregada. Se o número da partição não for igual ao da partição pré-carregada, nenhuma ação ocorrerá. Se os números da partição corresponderem, o utilitário de carga do cliente será chamado para carregar os dados nos mapas. Você deve chamar o carregador do cliente em uma, e somente uma, partição.

```
void preloadMap (Session session, BackingMap backingMap) throws LoaderException {

....
 ObjectGrid objectGrid = session.getObjectGrid();
 int partitionId = backingMap.getPartitionId();
 int numPartitions = backingMap.getPartitionManager().getNumOfPartitions();

 // Only call client loader data in one partition
 if (partitionId == preloadPartition) {
```

```
     ClientLoader c = ClientLoaderFactory.getClientLoader();
    // Call the client loader to load the data
    try {
        c.load(objectGrid, "CUSTOMER", "customerPU",
     null, entityClass, null, null, true, null);
    } catch (ObjectGridException e) {
        LoaderException le = new LoaderException("Exception caught in ObjectMap " + ogName + "." +
        le.initCause(e);
        throw le;
    }
 }
}
```

Lembre-se: Configure o atributo de backingMap "preloadMode" para `true`, para que o método de pré-carregamento seja executado de forma assíncrona. Caso contrário, o método de pré-carregamento impedirá que a instância de ObjectGrid seja ativada.

Conceitos relacionados:

Java "Visão Geral do Utilitário de Pré-Carregamento JPA Baseado em Cliente" na página 662
O utilitário de pré-carregamento Java Persistence API (JPA) baseado em cliente carrega dados nos mapas de apoio do eXtreme Scale usando uma conexão de cliente para o ObjectGrid.

Tarefas relacionadas:

Java "Desenvolvendo Carregadores JPA Baseados em Cliente" na página 661
É possível implementar o pré-carregamento e o recarregamento de dados no seu aplicativo usando o utilitário Java Persistence API (JPA). Este recurso pode simplificar o carregamento dos mapas quando as consultas ao banco de dados não puderem ser particionadas.

Informações relacionadas:

Java Interface ClientLoader

Java Interface StateManager

Exemplo: Criando um Carregador JPA Baseado em Cliente Customizado:

Java

O método ClientLoader.load na interface Loader fornece uma função de carregamento do cliente que atende à maioria dos cenários. No entanto, se desejar carregar os dados sem o método ClientLoader.load, poderá implementar seu próprio utilitário de pré-carregamento.

Modelo de Carregador Customizado

Use o seguinte modelo para desenvolver seu carregador:

```
// Get the StateManager
StateManager stateMgr = StateManagerFactory.getStateManager();

// Set ObjectGrid state to PRELOAD before calling ClientLoader.loader
stateMgr.setObjectGridState(AvailabilityState.PRELOAD, objectGrid);


// Load the data
...<your preload utility implementation>...

// Set ObjectGrid state back to ONLINE
stateMgr.setObjectGridState(AvailabilityState.ONLINE, objectGrid);
```

Desenvolvendo um Carregador JPA Baseado em Cliente com um Agente DataGrid: Java

Quando estiver carregando os dados no lado do cliente, usar um agente DataGrid poderá aumentar o desempenho. Ao usar o agente DataGrid, todas as leituras e gravações de dados ocorrerão no processo do servidor. Também é possível projetar seu aplicativo para certificar-se de que os agentes DataGrid em várias partições sejam executados em paralelo para aumentar ainda mais o desempenho.

Sobre Esta Tarefa

Para obter mais informações sobre o agente DataGrid, consulte "APIs do DataGrid e Particionamento" na página 509.

Depois de criar a implementação de pré-carregamento de dados, poderá criar um Utilitário de Carga genérico para concluir as seguintes tarefas:

- Consultar os dados do banco de dados nos lotes.
- Criar uma lista de chaves e uma lista de valores para cada partição.
- Para cada partição, chame o método agentMgr.callReduceAgent(agent, aKey) para executar o agente no servidor em um encadeamento. Ao executar um encadeamento, poderá executar os agentes simultaneamente em várias partições.

Exemplo

O fragmento de código a seguir é um exemplo de como carregar usando um agente do DataGrid:

```
import java.io.Externalizable;
import java.io.IOException;
import java.io.ObjectInput;
import java.io.ObjectOutput;
import java.util.ArrayList;
import java.util.Collection;
import java.util.Iterator;
import java.util.List;

import com.ibm.websphere.objectgrid.NoActiveTransactionException;
import com.ibm.websphere.objectgrid.ObjectGridException;
import com.ibm.websphere.objectgrid.ObjectGridRuntimeException;
import com.ibm.websphere.objectgrid.ObjectMap;
import com.ibm.websphere.objectgrid.Session;
import com.ibm.websphere.objectgrid.TransactionException;
import com.ibm.websphere.objectgrid.datagrid.ReduceGridAgent;
import com.ibm.websphere.objectgrid.em.EntityManager;

public class InsertAgent implements ReduceGridAgent, Externalizable {

    private static final long serialVersionUID = 6568906743945108310L;

    private List keys = null;

    private List vals = null;

    protected boolean isEntityMap;

    public InsertAgent() {
    }

    public InsertAgent(boolean entityMap) {
        isEntityMap = entityMap;
    }
```

```
public Object reduce(Session sess, ObjectMap map) {
    throw new UnsupportedOperationException(
        "ReduceGridAgent.reduce(Session, ObjectMap)");
}

public Object reduce(Session sess, ObjectMap map, Collection arg2) {
    Session s = null;
    try {
        s = sess.getObjectGrid().getSession();
        ObjectMap m = s.getMap(map.getName());
        s.beginNoWriteThrough();
        Object ret = process(s, m);
        s.commit();
        return ret;
    } catch (ObjectGridRuntimeException e) {
        if (s.isTransactionActive()) {
            try {
                s.rollback();
            } catch (TransactionException e1) {
            } catch (NoActiveTransactionException e1) {
            }
        }
        throw e;
    } catch (Throwable t) {
        if (s.isTransactionActive()) {
            try {
                s.rollback();
            } catch (TransactionException e1) {
            } catch (NoActiveTransactionException e1) {
            }
        }
        throw new ObjectGridRuntimeException(t);
    }

}

public Object process(Session s, ObjectMap m) {
    try {

        if (!isEntityMap) {
            // In the POJO case, it is very straightforward,
            // we can just put everything in the
            // map using insert
            insert(m);
        } else {
            // 2. Entity case.
            // In the Entity case, we can persist the entities
            EntityManager em = s.getEntityManager();
            persistEntities(em);

        }
        return Boolean.TRUE;
    } catch (ObjectGridRuntimeException e) {
        throw e;
    } catch (ObjectGridException e) {
        throw new ObjectGridRuntimeException(e);
    } catch (Throwable t) {
        throw new ObjectGridRuntimeException(t);
    }

}

/**
 * Basically this is fresh load.
 * @param s
 * @param m
```

```
     * @throws ObjectGridException
     */
    protected void insert(ObjectMap m) throws ObjectGridException {

        int size = keys.size();

        for (int i = 0; i < size; i++) {
            m.insert(keys.get(i), vals.get(i));
        }

    }


    protected void persistEntities(EntityManager em) {
        Iterator<Object> iter = vals.iterator();

        while (iter.hasNext()) {
            Object value = iter.next();
            em.persist(value);
        }
    }

    public Object reduceResults(Collection arg0) {
        return arg0;
    }

    public void readExternal(ObjectInput in)
      throws IOException, ClassNotFoundException {
        int v = in.readByte();
        isEntityMap = in.readBoolean();
        vals = readList(in);
        if (!isEntityMap) {
            keys = readList(in);
        }
    }

    public void writeExternal(ObjectOutput out) throws IOException {
        out.write(1);
        out.writeBoolean(isEntityMap);

        writeList(out, vals);
        if (!isEntityMap) {
            writeList(out, keys);
        }

    }

    public void setData(List ks, List vs) {
        vals = vs;
        if (!isEntityMap) {
            keys = ks;
        }
    }

    /**
     * @return Returns the isEntityMap.
     */
    public boolean isEntityMap() {
        return isEntityMap;
    }

    static public void writeList(ObjectOutput oo, Collection l)
      throws IOException {
        int size = l == null ? -1 : l.size();
        oo.writeInt(size);
        if (size > 0) {
            Iterator iter = l.iterator();
```

```
            while (iter.hasNext()) {
                Object o = iter.next();
                oo.writeObject(o);
            }
        }
    }

    public static List readList(ObjectInput oi)
      throws IOException, ClassNotFoundException {
        int size = oi.readInt();
        if (size == -1) {
            return null;
        }


        ArrayList list = new ArrayList(size);
        for (int i = 0; i < size; ++i) {
            Object o = oi.readObject();
            list.add(o);
        }
        return list;
    }
}
```

Exemplo: Usando o Plug-in Hibernate para Pré-Carregar Dados no Cache do ObjectGrid

Java

É possível usar o método preload da classe ObjectGridHibernateCacheProvider para pré-carregar dados no cache do ObjectGrid para uma classe de entidade.

Exemplo: Usando a classe EntityManagerFactory

```
EntityManagerFactory emf = Persistence.createEntityManagerFactory("testPU");
ObjectGridHibernateCacheProvider.preload("objectGridName", emf, TargetEntity.class, 100, 100);
```

Importante: Por padrão, as entidades não fazem parte do segundo nível de cache. No classes de Entidade que precisam de armazenamento em cache, inclua a anotação @cache. Este é um exemplo:

```
import org.hibernate.annotations.Cache;
import org.hibernate.annotations.CacheConcurrencyStrategy;
@Entity
@Cache(usage=CacheConcurrencyStrategy.TRANSACTIONAL)
public class HibernateCacheTest { ... }
```

É possível substituir esse padrão ao configurar o elemento modo de cache compartilhado no arquivo `persistence.xml` ou usando a propriedade javax.persistence.sharedCache.mode.

Exemplo: Usando a classe SessionFactory

```
org.hibernate.cfg.Configuration cfg = new Configuration();
// use o método addResource, addClass e setProperty da Configuração para preparar a
// configuração necessária para criar o SessionFactor
SessionFactory sessionFactory= cfg.buildSessionFactory();
ObjectGridHibernateCacheProvider.preload("objectGridName", sessionFactory, TargetEntity.class, 100, 100);
```

Nota:

1. Em um sistema distribuído, este mecanismo de pré-carregamento somente pode ser chamado de uma Java virtual machine. O mecanismo de pré-carregamento não pode executar simultaneamente a partir de várias Java Virtual Machines.
2. Antes de executar o pré-carregamento, você deve inicializar o cache do eXtreme Scale ao criar o EntityManager usando o EntityManagerFactory para que todos os BackingMaps correspondentes sejam criados, caso contrário, o

pré-carregamento forçará o cache a ser inicializado com somente um BackingMap padrão para suportar todas as entidades. Isto significa que um único BackingMap é compartilhado por todas as entidades.

Iniciando o Atualizador Baseado em Tempo do JPA

Java

Ao iniciar um atualizador baseado em tempo do Java Persistence API (JPA), os mapas do ObjectGrid são atualizados com as últimas alterações no banco de dados.

Antes de Iniciar

Configurar o atualizador baseado em tempo. Consulte o Configurando um Atualizador de Dados Baseado em Tempo do JPA.

Sobre Esta Tarefa

Para obter mais informações sobre como o atualizador de dados baseado em tempo do Java Persistence API (JPA) trabalha, consulte "Atualizador de Dados Baseado em Tempo JPA" na página 675.

Procedimento

- Inicie um atualizador de banco de dados baseado em tempo.
  - **Automaticamente para o eXtreme Scale distribuído:**

    Se você criar uma configuração do timeBasedDBUpdate para o mapa de apoio, o atualizador do banco de dados baseado em tempo será iniciado automaticamente quando um shard primário do ObjectGrid distribuído for ativado. Para um ObjectGrid com várias partições, o atualizador do banco de dados baseado em tempo será iniciado apenas na partição 0.
  - **Automaticamente para o eXtreme Scale local:**

    Se você criar uma configuração do timeBasedDBUpdate para o mapa de apoio, o atualizador do banco de dados baseado em tempo será iniciado automaticamente quando o mapa local for ativado.
  - **Manualmente:**

    Também é possível iniciar ou parar manualmente um atualizador de banco de dados baseado em tempo utilizando a API do TimeBasedDBUpdater.

    ```
    public synchronized void startDBUpdate(ObjectGrid objectGrid, String mapName,
     String punitName, Class entityClass, String timestampField, DBUpdateMode mode) {
    ```

    1. **ObjectGrid**: a instância do ObjectGrid (local ou cliente).
    2. **mapName**: o nome do mapa de apoio para o qual o atualizador de banco de dados baseado em tempo é iniciado.
    3. **punitName**: O nome da unidade de persistência JPA para criar um factory do gerenciador de entidade JPA; o valor padrão é o nome da primeira unidade de pesistência definida no arquivo `persistence.xml`.
    4. **entityClass**: O nome da classe de entidade usado para interagir com o provedor Java Persistence API (JPA); o nome da classe de entidade é usado para obter as entidades do JPA usando as consultas de entidade.
    5. **timestampField**: Um campo de registro de data e hora da classe de entidade para identificar a hora ou a sequência quando um registro back end de banco de dados foi atualizado ou inserido pela última vez.
    6. **mode**: O modo de atualização de banco de dados baseado em tempo; um tipo INVALIDATE_ONLY faz com que ele invalide as entradas no mapa do ObjectGrid se os registros correspondentes no banco de dados foram

atualizados; um tipo UPDATE_ONLY indica para atualizar as entradas existentes no mapa do ObjectGrid com os valores mais recentes do banco de dados; entretanto, todos os registros recentemente inseridos no banco de dados são ignorados; um tipo INSERT_UPDATE indica para atualizar as entradas existentes no mapa do ObjectGrid com os valores mais recentes a partir do banco de dados; além disso, todos os registros recentemente inseridos no banco de dados são inseridos no mapa do ObjectGrid.

Se você desejar parar o atualizador de banco de dados baseado em tempo, poderá chamar o seguinte método para parar o atualizador:

```
public synchronized void stopDBUpdate(ObjectGrid objectGrid, String mapName)
```

Os parâmetros ObjectGrid e mapName devem ser os mesmos que aqueles transmitidos no método startDBUpdate.

- Crie o campo do registro de data e hora no seu banco de dados.
  - **DB2**

    Como parte do recurso de bloqueio otimista, o DB2 9.5 fornece um recurso de registro de data e hora de alteração de linha. É possível definir uma coluna ROWCHGTS utilizando o formato ROW CHANGE TIMESTAMP, conforme a seguir:

    ```
    ROWCHGTS TIMESTAMP NOT NULL
         GENERATED ALWAYS
         FOR EACH ROW ON UPDATE AS
         ROW CHANGE TIMESTAMP
    ```

    Em seguida, é possível indicar o campo de entidade que corresponde à esta coluna como o campo do registro de data e hora pela anotação ou configuração. Este é um exemplo:

    ```
    @Entity(name = "USER_DB2")
    @Table(name = "USER1")
    public class User_DB2 implements Serializable {

        private static final long serialVersionUID = 1L;

        public User_DB2() {
        }

        public User_DB2(int id, String firstName, String lastName) {
            this.id = id;
            this.firstName = firstName;
            this.lastName = lastName;
        }

        @Id
        @Column(name = "ID")
        public int id;

        @Column(name = "FIRSTNAME")
        public String firstName;

        @Column(name = "LASTNAME")
        public String lastName;

        @com.ibm.websphere.objectgrid.jpa.dbupdate.annotation.Timestamp
        @Column(name = "ROWCHGTS", updatable = false, insertable = false)
        public Timestamp rowChgTs;
    }
    ```

  - **Oracle**

    No Oracle, há uma semicoluna `ora_rowscn` para o número de alteração do sistema do registro. É possível utilizar esta coluna para o mesmo propósito.

Um exemplo da entidade que usa o campo ora_rowscn como o campo do registro de data e hora de atualização de banco de dados baseado em tempo é o seguinte:

```
@Entity(name = "USER_ORA")
@Table(name = "USER1")
public class User_ORA implements Serializable  {

    private static final long serialVersionUID = 1L;

    public User_ORA() {
    }

    public User_ORA(int id, String firstName, String lastName) {
        this.id = id;
        this.firstName = firstName;
        this.lastName = lastName;
    }

    @Id
    @Column(name = "ID")
    public int id;

    @Column(name = "FIRSTNAME")
    public String firstName;

    @Column(name = "LASTNAME")
    public String lastName;

    @com.ibm.websphere.objectgrid.jpa.dbupdate.annotation.Timestamp
    @Column(name = "ora_rowscn", updatable = false, insertable = false)
    public long rowChgTs;
}
```

– **Outros Bancos de Dados**

Para outros tipos de bancos de dados, é possível criar uma coluna da tabela para controlar as alterações. Os valores da coluna precisam ser gerenciados manualmente pelo aplicativo que atualiza a tabela.

Tome o banco de dados Apache Derby como exemplo: É possível criar uma coluna "ROWCHGTS" para controlar os números de alteração. Além disso, um número de alteração mais recente é controlado para esta tabela. Sempre que um registro for inserido ou atualizado, o número de alteração mais recente para a tabela é aumentado e o valor da coluna ROWCHGTS para o registro é atualizado com o número aumentado.

```
@Entity(name = "USER_DER")
@Table(name = "USER1")
public class User_DER implements Serializable {

    private static final long serialVersionUID = 1L;

    public User_DER() {
    }

    public User_DER(int id, String firstName, String lastName) {
        this.id = id;
        this.firstName = firstName;
        this.lastName = lastName;
    }

    @Id
    @Column(name = "ID")
    public int id;

    @Column(name = "FIRSTNAME")
    public String firstName;
```

```
    @Column(name = "LASTNAME")
    public String lastName;

    @com.ibm.websphere.objectgrid.jpa.dbupdate.annotation.Timestamp
    @Column(name = "ROWCHGTS", updatable = true, insertable = true)
    public long rowChgTs;
}
```

Atualizador de Dados Baseado em Tempo JPA: Java

Um atualizador de banco de dados baseado em tempo do Java Persistence API (JPA) atualiza os mapas do ObjectGrid com as últimas alterações no banco de dados.

Quando são feitas alterações diretamente em um banco de dados que está sendo confrontado pelo WebSphere eXtreme Scale, essas alterações não são refletidas simultaneamente na grade do eXtreme Scale. Para implementar corretamente o eXtreme Scale como um espaço de processamento de banco de dados de memória, lembre-se de que sua grade pode sair de sincronia com o banco de dados. O atualizar de banco de dados baseado em tempo usa o recurso System Change Number (SCN) no Oracle 10g e a indicação de data e hora da alteração da linha no DB2 9.5 para monitorar as alterações no banco de dados para invalidação e atualização. O atualizador também permite que os aplicativos tenham um campo definido pelo usuário para o mesmo propósito.

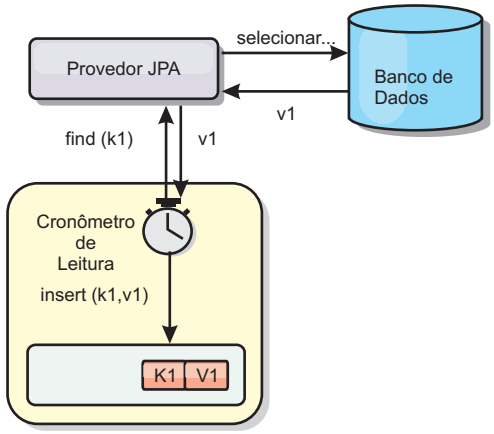


Figura 44. Atualização Periódica

O atualizador de banco de dados baseado em tempo consulta periodicamente o banco de dados usando as interfaces do JPA para obter as entidades do JPA que representam os registros recentemente inseridos e atualizados no banco de dados. Para atualizar periodicamente os registros, cada registro no banco de dados deve ter um registro de data e hora para identificar o tempo ou a sequência em que o registro foi atualizado ou inserido pela última vez. O registro de data e hora não precisa estar no formato do registro de data e hora. O valor do registro de data e hora pode estar em um formato inteiro ou longo, se ele gerar um valor exclusivo e cada vez maior.

Vários bancos de dados comerciais fornecem este recurso.

Por exemplo, no DB2 9.5, é possível definir uma coluna usando o formato ROW CHANGE TIMESTAMP como a seguir:

```
ROWCHGTS TIMESTAMP NOT NULL
      GENERATED ALWAYS
      FOR EACH ROW ON UPDATE AS
      ROW CHANGE TIMESTAMP
```

No Oracle, é possível utilizar a pseudo-coluna **ora_rowscn**, que representa o número de alteração de sistema do registro.

O atualizador do banco de dados baseado em tempo atualiza os mapas do ObjectGrid de três diferentes maneiras:

1. INVALIDATE_ONLY. Invalidar as entradas no mapa ObjectGrid se os registros correspondentes no banco de dados foram alterados.
2. UPDATE_ONLY. Atualizar as entradas no mapa do ObjectGrid se os registros correspondentes no banco de dados foram alterados. Entretanto, todos os registros recentemente inseridos no banco de dados são ignorados.
3. INSERT_UPDATE. Atualizar as entradas existentes no mapa do ObjectGrid com os valores mais recentes do banco de dados. Além disso, todos os registros recentemente inseridos no banco de dados são inseridos no mapa do ObjectGrid.

Para obter informações adicionais sobre como configurar o atualizador de dados baseado em tempo JPA, consulte o Configurando um Atualizador de Dados Baseado em Tempo do JPA.

Desenvolvendo Aplicativos com a Estrutura Spring

Java

Aprenda como integrar seus aplicativos eXtreme Scale com o Spring Framework popular.

Conceitos relacionados:

Java "Visão Geral da Estrutura Spring" na página 330
O Spring é uma estrutura para desenvolvimento de aplicativos Java. O WebSphere eXtreme Scale fornece suporte para permitir que o Spring gerencie as transações e configure clientes e servidores que compõem a grade de dados em memória implementada.

Java "Beans de Extensão Spring e Suporte a Espaço de Nomes" na página 684
O WebSphere eXtreme Scale fornece um recurso para declarar Plain Old Java Objects (POJOs) para uso como pontos de extensão no arquivo `objectgrid.xml`, além de uma maneira de nomear os beans e especificar o nome da classe. Normalmente, as instâncias da classe especificada são criadas, e tais objetos são usados como plug-ins. Agora, o eXtreme Scale pode delegar que Spring obtenha instâncias destes objetos plug-in. Se um aplicativo utiliza o Spring, então, normalmente, tais POJOs possuem um requisito de serem conectados ao resto do aplicativo.

Referências relacionadas:

Java "Beans de Extensão Gerenciados pelo Spring" na página 682
É possível declarar que os POJOs sejam usados como pontos de extensão no arquivo `objectgrid.xml`. Se você nomear os beans e, em seguida, especificar o nome de classe, o eXtreme Scale normalmente cria instâncias da classe especificada e usa essas instâncias como o plug-in. O WebSphere eXtreme Scale pode delegar para que o Spring aja como o bean factory para obter instâncias desses objetos de plug-in.

Java Arquivo XML descritor do Spring
Use um arquivo XML descritor do Spring para configurar e integrar o eXtreme Scale com o Spring.

Java Arquivo `objectgrid.xsd` Spring
Use o arquivo `objectgrid.xsd` Spring para integrar o eXtreme Scale ao Spring para gerenciar as transações do eXtreme Scale e configurar os clientes e servidores.

Visão Geral da Estrutura Spring

Java

O Spring é uma estrutura para desenvolvimento de aplicativos Java. O WebSphere eXtreme Scale fornece suporte para permitir que o Spring gerencie as transações e configure clientes e servidores que compõem a grade de dados em memória implementada.

Provedor de Cache Spring

O Spring Framework Versão 3.1 introduziu uma nova abstração de cache. Com essa nova abstração, é possível incluir de modo transparente o armazenamento em cache em um aplicativo Spring existente. É possível usar o WebSphere eXtreme Scale como o provedor de cache para a abstração de cache. Para obter informações adicionais, consulte Configurando um Provedor de Cache Spring.

Transações Nativas Gerenciadas do Spring

O Spring fornece transações gerenciadas por contêiner que são similares a um servidor de aplicativos do Java Platform, Enterprise Edition. Porém, o mecanismo do Spring pode usar diferentes implementações. O WebSphere eXtreme Scale fornece a integração do gerenciador de transações que permite ao Spring para gerenciar os ciclos de vida da transação do ObjectGrid. Para obter informações

adicionais, consulte “Gerenciando Transações com o Spring” na página 679.

Beans de Extensão Gerenciados do Spring e Suporte a Espaço de Nomes

Além disso, o eXtreme Scale se integra ao Spring para permitir que os beans de estilo do Spring definidos para pontos de extensão ou plug-ins. Este recurso fornece configurações mais sofisticadas e mais flexíveis para configuração dos pontos de extensão.

Além dos beans de extensão gerenciados do Spring, o eXtreme Scale fornece um espaço de nomes Spring chamado "objectgrid". Beans e implementações integradas são predefinidos neste espaço de nomes, o que facilita aos usuários configurar o eXtreme Scale. Consulte “Beans de Extensão Spring e Suporte a Espaço de Nomes” na página 684 para obter mais detalhes sobre esses tópicos e uma amostra de como iniciar um servidor de contêiner do eXtreme Scale usando configurações Spring.

Suporte ao Escopo Shard

Com a configuração do Spring estilo tradicional, um bean ObjectGrid pode se do tipo singleton ou prototype. O ObjectGrid também suporta um novo escopo chamado de escopo "shard". Se um bean for definido como escopo shard, então somente um bean será criado por shard. Todas as solicitações de beans com um ID ou IDs correspondentes a essa definição de bean no mesmo shard resulta nessa instância de bean específica sendo retornada pelo contêiner Spring.

O exemplo a seguir mostra que um bean com.ibm.ws.objectgrid.jpa.plugins.JPAPropFactoryImpl é definido com o escopo configurado para shard. Portanto, apenas uma instância da classe JPAPropFactoryImpl é criada por shard.

```
<bean id="jpaPropFactory" class="com.ibm.ws.objectgrid.jpa.plugins.JPAPropFactoryImpl" scope="shard" />
```

Fluxo da Web do Spring

O Fluxo da Web do Spring armazena seu estado de sessão em uma sessão HTTP por padrão. Se um aplicativo da web usar o eXtreme Scale para gerenciamento de sessões, o Spring armazenará automaticamente o estado com o eXtreme Scale. Além disso, a tolerância a falhas é ativada da mesma forma que a sessão.

Para obter mais informações, consulte Gerenciando de Sessões HTTP.

compactando

As extensões Spring do eXtreme Scale estão no arquivo `ogspring.jar`. Este arquivo Java archive (JAR) deve estar no caminho de classe para o suporte ao Spring funcionar. Se um aplicativo Java EE que estiver em execução em um WebSphere Application Server Network Deployment aumentado pelo WebSphere Extended Deployment, coloque o arquivo `spring.jar` e seus arquivos associados nos módulos EAR (enterprise archive). Você também deve colocar o arquivo `ogspring.jar` no mesmo local.

Tarefas relacionadas:

Java "Desenvolvendo Aplicativos com a Estrutura Spring" na página 676
Aprenda como integrar seus aplicativos eXtreme Scale com o Spring Framework popular.

Java "Iniciando um Servidor de Contêiner com o Spring" na página 687
É possível iniciar um servidor de contêiner usando beans de extensão gerenciados pelo Spring e o suporte ao namespace.

Java "Gerenciando Transações com o Spring"
O Spring é uma estrutura popular para desenvolvimento de aplicativos Java. O WebSphere eXtreme Scale fornece suporte para permitir que o Spring gerencie transações do eXtreme Scale e configure clientes e servidores eXtreme Scale.

Referências relacionadas:

Java "Beans de Extensão Gerenciados pelo Spring" na página 682
É possível declarar que os POJOs sejam usados como pontos de extensão no arquivo `objectgrid.xml`. Se você nomear os beans e, em seguida, especificar o nome de classe, o eXtreme Scale normalmente cria instâncias da classe especificada e usa essas instâncias como o plug-in. O WebSphere eXtreme Scale pode delegar para que o Spring aja como o bean factory para obter instâncias desses objetos de plug-in.

Java Arquivo XML descritor do Spring
Use um arquivo XML descritor do Spring para configurar e integrar o eXtreme Scale com o Spring.

Java Arquivo `objectgrid.xsd` Spring
Use o arquivo `objectgrid.xsd` Spring para integrar o eXtreme Scale ao Spring para gerenciar as transações do eXtreme Scale e configurar os clientes e servidores.

Gerenciando Transações com o Spring

Java

O Spring é uma estrutura popular para desenvolvimento de aplicativos Java. O WebSphere eXtreme Scale fornece suporte para permitir que o Spring gerencie transações do eXtreme Scale e configure clientes e servidores eXtreme Scale.

Sobre Esta Tarefa

A Estrutura Spring é altamente integrable com o eXtreme Scale, conforme discutido nas seções a seguir.

Procedimento

- **Transações nativas:** O Spring fornece transações gerenciadas por contêiner junto com o estilo de um servidor de aplicativos Java Platform, Enterprise Edition, mas com a vantagem de que o mecanismo Springs pode ter implementações diferentes conectadas. Este tópico descreve um gerenciador eXtreme Scale Platform Transaction que pode ser utilizado com o Spring. Isso permite que os programadores anotem os Plain Old Java Objects (POJOs), façam com que o Spring adquira automaticamente Sessões a partir do eXtreme Scale e comecem, confirmem, recuperem, suspendam e continuem as transações do eXtreme Scale. As transações do Spring são descritas mais completamente no Capítulo 10 da documentação oficial de referência do Spring. O seguinte explica como criar um gerenciador de transações do eXtreme Scale e usá-lo com os POJOs anotados. Ele também explica como utilizar esta abordagem com o eXtreme Scale cliente ou local, bem como com um aplicativo do estilo Data Grid.

- **Gerenciador de Transação:** Para trabalhar com Spring, eXtreme Scale fornece uma implementação de um Spring PlatformTransactionManager. Este gerenciador pode fornecer sessões gerenciadas do eXtreme Scale para POJOs gerenciados pelo Spring. Através do uso das anotações, o Spring gerencia essas sessões para os POJOs em termos de ciclo de vida da transação. O seguinte snippet XML mostra como criar um Gerenciador de transações:

```
<aop:aspectj-autoproxy/>
 <tx:annotation-driven transaction-manager="transactionManager"/>

 <bean id="ObjectGridManager"
    class="com.ibm.websphere.objectgrid.ObjectGridManagerFactory"
    factory-method="getObjectGridManager"/>

 <bean id="ObjectGrid"
    factory-bean="ObjectGridManager"
    factory-method="createObjectGrid"/>

 <bean id="transactionManager"
    class="com.ibm.websphere.objectgrid.spring.ObjectGridSpringFactory"
    factory-method="getLocalPlatformTransactionManager"/>
 </bean>

 <bean id="Service" class="com.ibm.websphere.objectgrid.spring.test.TestService">
  <property name="txManager" ref+"transactionManager"/>
 </bean>
```

  Isto mostra o bean transactionManager que está sendo declarado e vinculado ao bean Service que utilizará transações Spring. Demonstraremos isto utilizando anotações e este é o motivo ara a cláusula tx:annotation no início.
- **Obtendo uma sessão do ObjectGrid:** Um POJO que possui métodos gerenciados pelo Spring agora podem obter a sessão do ObjectGrid para a transação atual utilizando

  ```
  Session s = txManager.getSession();
  ```

  Isto retorna a sessão para o POJO utilizar. Beans participando na mesma transação receberão a mesma sessão quando eles chamam este método. O Spring identificará automaticamente o início para o objeto Session e também chamará automaticamente o commit ou rollback, quando necessário. Também é possível obter um EntityManager do ObjectGrid simplesmente chamando getEntityManager do objeto Session.
- **Configurando a instância do ObjectGrid para um encadeamento:** Uma única Java Virtual Machine (JVM) pode hospedar várias instâncias do ObjectGrid. Cada shard primário colocado em uma JVM possui sua própria instância do ObjectGrid. Uma JVM atuando como um cliente para um ObjectGrid remoto utiliza uma instância do ObjectGrid retornada do ClientClusterContext do método de conexão para interagir com tal Grade. Antes de chamar um método em um POJO utilizando transações Spring para o ObjectGrid, o encadeamento deve ser primed com a instância do ObjectGrid a utilizar. A instância do TransactionManager possui um método permitindo que uma instância específica do ObjectGrid seja especificada. Depois de especificada, todas as chamadas subsequentes do txManager.getSession retornarão Sessões para essa instância de ObjectGrid.

  O exemplo a seguir mostra um principal de amostra para exercitar este recurso:

```
ClassPathXmlApplicationContext ctx = new ClassPathXmlApplicationContext(new String[]
           {"applicationContext.xml"});
    SpringLocalTxManager txManager = (SpringLocalTxManager)ctx.getBean("transactionManager");
    txManager.setObjectGridForThread(og);

    ITestService s = (ITestService)ctx.getBean("Service");
    s.initialize();
    assertEquals(s.query(), "Billy");
    s.update("Bobby");
    assertEquals(s.query(), "Bobby");
    System.out.println("Requires new test");
    s.testRequiresNew(s);
    assertEquals(s.query(), "1");
```

Aqui, utilizamos um Spring ApplicationContext. O ApplicationContext é utilizado para obter uma referência para o txManager e especificar um ObjectGrid a utilizar neste encadeamento. O código então obtém uma referência para o serviço e chama métodos nele. Cada chamada de método neste nível faz com que o Spring crie um objeto Session e faz chamadas begin/commit em torno da chamada de método. Quaisquer exceções causarão um retrocesso.

- **Interface SpringLocalTxManager:** A interface SpringLocalTxManager é implementada pelo ObjectGrid Platform Transaction Manager e possui todas as interfaces públicas. Os métodos nesta interface são utilizados para selecionar a instância do ObjectGrid para utilizar em um encadeamento e obter um objeto Session para o encadeamento. Quaisquer POJOs que utilizam transações locais do ObjectGrid devem ser injetados com uma referência para esta instância do gerenciador e apenas uma única instância deve ser criada, ou seja, seu escopo deve ser um singleton. Esta instância é criada utilizando um método estático no ObjectGridSpringFactory. getLocalPlatformTransactionManager().

  Restrição: O WebSphere eXtreme Scale não suporta o JTA ou two-phase commit por vários motivos, principalmente devido à escalabilidade. Assim, exceto em um último participante single-phase, o ObjectGrid não interage em transações globais do tipo XA ou JTA. Este gerenciador de plataformas é destinado a tornar o uso de transações locais do ObjectGrid o mais fácil possível para os desenvolvedores do Spring.

Conceitos relacionados:

Java "Visão Geral da Estrutura Spring" na página 330
O Spring é uma estrutura para desenvolvimento de aplicativos Java. O WebSphere eXtreme Scale fornece suporte para permitir que o Spring gerencie as transações e configure clientes e servidores que compõem a grade de dados em memória implementada.

Java "Beans de Extensão Spring e Suporte a Espaço de Nomes" na página 684
O WebSphere eXtreme Scale fornece um recurso para declarar Plain Old Java Objects (POJOs) para uso como pontos de extensão no arquivo `objectgrid.xml`, além de uma maneira de nomear os beans e especificar o nome da classe. Normalmente, as instâncias da classe especificada são criadas, e tais objetos são usados como plug-ins. Agora, o eXtreme Scale pode delegar que Spring obtenha instâncias destes objetos plug-in. Se um aplicativo utiliza o Spring, então, normalmente, tais POJOs possuem um requisito de serem conectados ao resto do aplicativo.

Referências relacionadas:

Java "Beans de Extensão Gerenciados pelo Spring"
É possível declarar que os POJOs sejam usados como pontos de extensão no arquivo `objectgrid.xml`. Se você nomear os beans e, em seguida, especificar o nome de classe, o eXtreme Scale normalmente cria instâncias da classe especificada e usa essas instâncias como o plug-in. O WebSphere eXtreme Scale pode delegar para que o Spring aja como o bean factory para obter instâncias desses objetos de plug-in.

Java Arquivo XML descritor do Spring
Use um arquivo XML descritor do Spring para configurar e integrar o eXtreme Scale com o Spring.

Java Arquivo `objectgrid.xsd` Spring
Use o arquivo `objectgrid.xsd` Spring para integrar o eXtreme Scale ao Spring para gerenciar as transações do eXtreme Scale e configurar os clientes e servidores.

Beans de Extensão Gerenciados pelo Spring

Java

É possível declarar que os POJOs sejam usados como pontos de extensão no arquivo `objectgrid.xml`. Se você nomear os beans e, em seguida, especificar o nome de classe, o eXtreme Scale normalmente cria instâncias da classe especificada e usa essas instâncias como o plug-in. O WebSphere eXtreme Scale pode delegar para que o Spring aja como o bean factory para obter instâncias desses objetos de plug-in.

Se um aplicativo usar o Spring, os POJOs precisarão estar acessíveis ao restante do aplicativo.

Um aplicativo pode registrar uma instância do Spring Bean Factory a ser usada para um ObjectGrid especificado por nome. O aplicativo cria uma instância de um contexto de aplicativo BeanFactorty ou Spring e, em seguida, registra-a com o ObjectGrid usando o seguinte método estático:

```
void registerSpringBeanFactoryAdapter(String objectGridName, Object springBeanFactory)
```

O método anterior se aplica quando o eXtreme Scale localiza um bean de extensão cujo className inicia com o prefixo {spring}. Tal uma extensão de bean, que pode ser um ObjectTransformer, Loader, TransactionCallback, e assim por diante, o

restante do nome é usado como um nome Spring Bean. Em seguida, a instância de bean é obtida usando o Spring Bean Factory.

O ambiente de implementação do eXtreme Scale também pode criar um Spring Bean Factory a partir de um arquivo de configuração XML do Spring padrão. Se nenhum bean factory foi registrado para um determinado ObjectGrid, sua implementação procurará pelo arquivo XML chamado "/<ObjectGridName>_spring.xml". Por exemplo, se sua grade de dados for denominada GRID, o arquivo XML será chamado "/GRID_spring.xml' e aparecerá no caminho de classe no pacote raiz. O ObjectGrid constrói um ApplicationContext usando o arquivo "/<ObjectGridName>_spring.xml e constrói beans a partir do bean factory.

A seguir há um exemplo de nome de classe:

```
"{spring}MyLoaderBean"
```

Usar o nome da classe anterior permite que o eXtreme Scale use o Spring para procurar um bean denominado "MyLoaderBean". É possível especificar POJOs gerenciados pelo Spring em qualquer ponto de extensão se o bean factory foi registrado. As extensões Spring estão no arquivo ogspring.jar. Esse arquivo JAR deve estar no caminho de classe para o suporte ao Spring. Se um aplicativo J2EE executado no WebSphere Application Server Network Deployment foi aumentado com o WebSphere Extended Deployment, você deverá colocar o aplicativo, o arquivo spring.jar e seus arquivos associados nos módulos EAR. O ogspring.jar também deve ser colocado no mesmo local.

Conceitos relacionados:

Java "Visão Geral da Estrutura Spring" na página 330
O Spring é uma estrutura para desenvolvimento de aplicativos Java. O WebSphere eXtreme Scale fornece suporte para permitir que o Spring gerencie as transações e configure clientes e servidores que compõem a grade de dados em memória implementada.

Java "Beans de Extensão Spring e Suporte a Espaço de Nomes"
O WebSphere eXtreme Scale fornece um recurso para declarar Plain Old Java Objects (POJOs) para uso como pontos de extensão no arquivo `objectgrid.xml`, além de uma maneira de nomear os beans e especificar o nome da classe. Normalmente, as instâncias da classe especificada são criadas, e tais objetos são usados como plug-ins. Agora, o eXtreme Scale pode delegar que Spring obtenha instâncias destes objetos plug-in. Se um aplicativo utiliza o Spring, então, normalmente, tais POJOs possuem um requisito de serem conectados ao resto do aplicativo.

Tarefas relacionadas:

Java "Desenvolvendo Aplicativos com a Estrutura Spring" na página 676
Aprenda como integrar seus aplicativos eXtreme Scale com o Spring Framework popular.

Java "Iniciando um Servidor de Contêiner com o Spring" na página 687
É possível iniciar um servidor de contêiner usando beans de extensão gerenciados pelo Spring e o suporte ao namespace.

Java "Gerenciando Transações com o Spring" na página 679
O Spring é uma estrutura popular para desenvolvimento de aplicativos Java. O WebSphere eXtreme Scale fornece suporte para permitir que o Spring gerencie transações do eXtreme Scale e configure clientes e servidores eXtreme Scale.

Beans de Extensão Spring e Suporte a Espaço de Nomes

Java

O WebSphere eXtreme Scale fornece um recurso para declarar Plain Old Java Objects (POJOs) para uso como pontos de extensão no arquivo `objectgrid.xml`, além de uma maneira de nomear os beans e especificar o nome da classe. Normalmente, as instâncias da classe especificada são criadas, e tais objetos são usados como plug-ins. Agora, o eXtreme Scale pode delegar que Spring obtenha instâncias destes objetos plug-in. Se um aplicativo utiliza o Spring, então, normalmente, tais POJOs possuem um requisito de serem conectados ao resto do aplicativo.

Em alguns cenários, você deve usar o Spring para configurar um plug-in, como no exemplo a seguir:

```
<objectGrid name="Grid">
    <bean id="TransactionCallback" className="com.ibm.websphere.objectgrid.jpa.JPATxCallback">
        <property name="persistenceUnitName" type="java.lang.String"  value="employeePU" />
    </bean>
    ...
</objectGrid>
```

A implementação de TransactionCallback integrada, a classe com.ibm.websphere.objectgrid.jpa.JPATxCallback, é configurada como a classe TransactionCallback. Esta classe é configurada com a propriedade **`persistenceUnitName`**, conforme mostrado no exemplo anterior. A classe JPATxCallback também tem o atributo JPAPropertyFactory, que é do tipo java.lang.Object. A configuração XML do ObjectGrid não pode suportar este tipo de configuração.

A integração Spring do eXtreme Scale soluciona este problema delegando a criação do bean à estrutura do Spring. A configuração revisada é a seguinte:

```
<objectGrid name="Grid">
    <bean id="TransactionCallback" className="{spring}jpaTxCallback"/>
    ...
</objectGrid>
```

O arquivo Spring para o objeto "Grid" contém as seguintes informações:

```
<bean id="jpaTxCallback" class="com.ibm.websphere.objectgrid.jpa.JPATxCallback" scope="shard">
    <property name="persistenceUnitName" value="employeeEMPU"/>
    <property name="JPAPropertyFactory" ref ="jpaPropFactory"/>
</bean>

<bean id="jpaPropFactory" class="com.ibm.ws.objectgrid.jpa.plugins.
JPAPropFactoryImpl" scope="shard">
</bean>
```

Aqui, o TransactionCallback está especificado como `{spring}jpaTxCallback`, e os beans jpaTxCallback e jpaPropFactory estão configurados no arquivo Spring como mostrado no exemplo anterior. A configuração Spring torna possível a configuração de um bean JPAPropertyFactory como um parâmetro do objeto JPATxCallback.

Bean factory Spring padrão

Quando o eXtreme Scale encontra um plug-in ou um bean de extensão (como um ObjectTransformer, utilitário de carga, TransactionCallback e assim por diante) com um valor className que inicia com o prefixo `{spring}`, o eXtreme Scale usará o restante do nome como um nome Spring Bean e obterá a instância do bean usando o Spring Bean Factory.

Pelo padrão, se nenhum bean factory tiver sido registrado para um determinado ObjectGrid, então ele tenta localizar um arquivo `ObjectGridName_spring.xml`. Por exemplo, se sua grade de dados for chamada como "Grid", então o arquivo XML será chamado como `/Grid_spring.xml`. Este arquivo deve estar no caminho da classe ou em um diretório `META-INF` que está no caminho da classe. Se este arquivo for encontrado, então o eXtreme Scale construi um ApplicationContext usando tal arquivo e construi beans a partir desse bean factory.

Bean factory Spring customizado

O WebSphere eXtreme Scale também fornece uma API ObjectGridSpringFactory para registrar uma instância do Spring Bean Factory para usar para um ObjectGrid específico nomeado. Esta API registra uma instância de BeanFactory com eXtreme Scale ussando o método estático a seguir:

```
void registerSpringBeanFactoryAdapter(String objectGridName, Object
springBeanFactory)
```

Suporte a Espaço de Nomes

Desde a versão 2.0, o Spring possui um mecanismo para extensão baseado em esquema para o formato XML do Spring básico para definição e configuração de beans. O ObjectGrid usa este novo recurso para definir e configurar beans ObjectGrid. Com a extensão de esquema XML do Spring, algumas das implementações integradas dos plug-ins do eXtreme Scale e alguns beans do ObjectGrid são predefinidos no espaço de nomes "objectgrid". Ao escrever os arquivos de configuração Spring, não é necessário especificar o nome completo de classe das implementações integradas. Em vez disso, é possível referenciar os beans predefinidos.

Além disso, com os atributos dos beans definidos no esquema XML, é menos provável que você forneça um nome de atributo errado. A validação XML baseada no esquema XML pode capturar estes tipos de erros anteriormente no ciclo de desenvolvimento.

Estes beans definidos nas extensões de esquema XML são:

- transactionManager
- registro
- servidor
- catálogo
- catalogServerProperties
- contêiner
- JPALoader
- JPATxCallback
- JPAEntityLoader
- LRUEvictor
- LFUEvictor
- HashIndex

Estes beans são definidos no esquema XML objectgrid.xsd. Este arquivo XSD é enviado como arquivo `com/ibm/ws/objectgrid/spring/namespace/objectgrid.xsd` no arquivo `ogspring.jar`. Para obter descrições detalhadas do arquivo XSD e dos beans definidos no arquivo XSD, consulte o Arquivo XML descritor do Spring.

Use o exemplo JPATxCallback da seção anterior. Na seção anterior, o bean JPATxCallback é configurado como o seguinte:

```
<bean id="jpaTxCallback" class="com.ibm.websphere.objectgrid.jpa.JPATxCallback" scope="shard">
    <property name="persistenceUnitName" value="employeeEMPU"/>
    <property name="JPAPropertyFactory" ref ="jpaPropFactory"/>
</bean>

<bean id="jpaPropFactory" class="com.ibm.ws.objectgrid.jpa.plugins.JPAPropFactoryImpl" scope="shard">
</bean>
```

Usando este recurso de espaço de nomes, a configuração XML do Spring pode ser escrita da seguinte forma:

```
<objectgrid:JPATxCallback id="jpaTxCallback" persistenceUnitName="employeeEMPU"
 jpaPropertyFactory="jpaPropFactory" />

<bean id="jpaPropFactory" class="com.ibm.ws.objectgrid.jpa.plugins.JPAPropFactoryImpl"
 scope="shard">
</bean>
```

Observe que, em vez de especificar a classe com.ibm.websphere.objectgrid.jpa.JPATxCallback como no exemplo anterior, o bean objectgrid:JPATxCallback pré-definido foi usado diretamente. Como pode ser visto, esta configuração é menos detalhada e mais amigável para verificação de erro.

Para obter uma descrição de como trabalhar com beans Spring, consulte o “Iniciando um Servidor de Contêiner com o Spring” na página 687.

Tarefas relacionadas:

Java "Desenvolvendo Aplicativos com a Estrutura Spring" na página 676
Aprenda como integrar seus aplicativos eXtreme Scale com o Spring Framework popular.

Java "Iniciando um Servidor de Contêiner com o Spring"
É possível iniciar um servidor de contêiner usando beans de extensão gerenciados pelo Spring e o suporte ao namespace.

Java "Gerenciando Transações com o Spring" na página 679
O Spring é uma estrutura popular para desenvolvimento de aplicativos Java. O WebSphere eXtreme Scale fornece suporte para permitir que o Spring gerencie transações do eXtreme Scale e configure clientes e servidores eXtreme Scale.

Referências relacionadas:

Java "Beans de Extensão Gerenciados pelo Spring" na página 682
É possível declarar que os POJOs sejam usados como pontos de extensão no arquivo `objectgrid.xml`. Se você nomear os beans e, em seguida, especificar o nome de classe, o eXtreme Scale normalmente cria instâncias da classe especificada e usa essas instâncias como o plug-in. O WebSphere eXtreme Scale pode delegar para que o Spring aja como o bean factory para obter instâncias desses objetos de plug-in.

Java Arquivo XML descritor do Spring
Use um arquivo XML descritor do Spring para configurar e integrar o eXtreme Scale com o Spring.

Java Arquivo `objectgrid.xsd` Spring
Use o arquivo `objectgrid.xsd` Spring para integrar o eXtreme Scale ao Spring para gerenciar as transações do eXtreme Scale e configurar os clientes e servidores.

Iniciando um Servidor de Contêiner com o Spring

Java

É possível iniciar um servidor de contêiner usando beans de extensão gerenciados pelo Spring e o suporte ao namespace.

Sobre Esta Tarefa

Com vários arquivos XML configurados para Spring, é possível iniciar os servidores de contêiner eXtreme Scale básicos.

Procedimento

1. **Arquivo XML do ObjectGrid**

   Primeiramente, defina um arquivo XML do ObjectGrid muito simples que contenha um "Grid" do ObjectGrid e uma mapa "Test". O ObjectGrid possui um plug-in ObjectGridEventListener chamado "partitionListener", e o mapa "Test" possui um Evictor conectado chamado "testLRUEvictor". Observe que ambos os plug-ins ObjectGridEventListener e Evictor são configurados usando Spring pois seus nomes contêm "{spring}".

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="Grid">
     <bean id="ObjectGridEventListener" className="{spring}partitionListener" />
           <backingMap name="Test" pluginCollectionRef="test" />
```

```
        </objectGrid>
    </objectGrids>

    <backingMapPluginCollections>
        <backingMapPluginCollection id="test">
            <bean id="Evictor" className="{spring}testLRUEvictor"/>
        </backingMapPluginCollection>
    </backingMapPluginCollections>
</objectGridConfig>
```

2. **Arquivo XML de implementação do ObjectGrid:**

   Agora, crie um arquivo XML de implementação simples do ObjectGrid da forma a seguir. Ele particiona o ObjectGrid em 5 partições, e nenhuma réplica é necessária.

```
<?xml version="1.0" encoding="UTF-8"?>
<deploymentPolicy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/deploymentPolicy ../deploymentPolicy.xsd"
 xmlns="http://ibm.com/ws/objectgrid/deploymentPolicy">
    <objectgridDeployment objectgridName="Grid">
        <mapSet name="mapSet" numInitialContainers="1" numberOfPartitions="5" minSyncReplicas="0"

maxSyncReplicas="1" >"1" maxAsyncReplicas="0">
            <map ref="Test"/>
        </mapSet>
    </objectgridDeployment>
</deploymentPolicy>
```

3. **Arquivo XML Spring do ObjectGrid**

   Agora serão usados tanto beans de extensão gerenciado Spring do ObjectGrid e recursos de suporte a espaço de nomes para configurar os beans ObjectGrid. O nome do arquivo XML Spring é `Grid_spring.xml`. Observe que estão incluídos dois esquemas no arquivo XML: `spring-beans-2.0.xsd` é para uso dos beans gerenciados do Spring, e `objectgrid.xsd` é para uso dos beans predefinidos no namespace do objectgrid.

```
<beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xmlns:aop="http://www.springframework.org/schema/aop"
       xmlns:tx="http://www.springframework.org/schema/tx"
       xmlns:objectgrid="http://www.ibm.com/schema/objectgrid"
       xsi:schemaLocation="
       http://www.ibm.com/schema/objectgrid
   http://www.ibm.com/schema/objectgrid/objectgrid.xsd
       http://www.springframework.org/schema/beans
   http://www.springframework.org/schema/beans/spring-beans-2.0.xsd">

    <objectgrid:register id="ogregister" gridname="Grid"/>

    <objectgrid:server id="server" isCatalog="true" name="server">
        <objectgrid:catalog host="localhost" port="2809"/>
    </objectgrid:server>

    <objectgrid:container id="container"
   objectgridxml="com/ibm/ws/objectgrid/test/springshard/objectgrid.xml"
       deploymentxml="com/ibm/ws/objectgrid/test/springshard/deployment.xml"
   server="server"/>

    <objectgrid:LRUEvictor id="testLRUEvictor" numberOfLRUQueues="31"/>

    <bean id="partitionListener"
   class="com.ibm.websphere.objectgrid.springshard.ShardListener" scope="shard"/>
</beans>
```

   Havia seis beans definidos neste arquivo XML do Spring:

   a. *objectgrid:register*: Isto registra o bean factory padrão para o "Grid" do ObjectGrid.

b. *objectgrid:server*: Isto define um servidor do ObjectGrid com o nome "server". Este servidor também fornece o serviço de catálogo desde que ele possua um bean objectgrid:catalog aninhado nele.

c. *objectgrid:catalog*: Isto define um terminal de serviço de catálogo ObjectGrid, que está configurado como "localhost:2809".

d. *objectgrid:container*: Isto define um contêiner ObjectGrid com o arquivo XML objectgrid especificado e o arquivo XML de implementação como discutido anteriormente. A propriedade de servidor especifica em qual servidor este contêiner está hospedado.

e. *objectgrid:LRUEvictor*: Isto define um LRUEvictor com a quantidade de filas LRU para usar configurada como 31.

f. *bean partitionListener*: Isto define um plug-in ShardListener. É necessário fornecer uma implementação para este plug-in, caso contrário, ele não poderá usar os beans predefinidos. Além disso, esse escopo do bean é configurado como "shard", o que significa que existe apenas uma instância desse ShardListener por shard ObjectGrid.

4. **Iniciando o servidor:**

   O fragmento a seguir inicia o servidor ObjectGrid, que hospeda tanto o serviço de contêiner e o serviço de catálogo. Como podemos ver, o único método que precisamos chamar para iniciar o servidor é para obter um "contêiner" de bean do bean factory. Isto simplifica a complexidade de programação pela movimentação da maioria da lógica na configuração do Spring.

```
public class ShardServer extends TestCase
{
    Container container;
    org.springframework.beans.factory.BeanFactory bf;

    public void startServer(String cep)
    {
        try
        {
            bf = new org.springframework.context.support.ClassPathXmlApplicationContext(
                "/com/ibm/ws/objectgrid/test/springshard/Grid_spring.xml", ShardServer.class);
            container = (Container)bf.getBean("container");
        }
        catch(Exception e)
        {
            throw new ObjectGridRuntimeException("Cannot start OG container", e);
        }
    }

    public void stopServer()
    {
        if(container != null)
            container.teardown();
    }
}
```

Conceitos relacionados:

Java "Visão Geral da Estrutura Spring" na página 330
O Spring é uma estrutura para desenvolvimento de aplicativos Java. O WebSphere eXtreme Scale fornece suporte para permitir que o Spring gerencie as transações e configure clientes e servidores que compõem a grade de dados em memória implementada.

Java "Beans de Extensão Spring e Suporte a Espaço de Nomes" na página 684
O WebSphere eXtreme Scale fornece um recurso para declarar Plain Old Java Objects (POJOs) para uso como pontos de extensão no arquivo `objectgrid.xml`, além de uma maneira de nomear os beans e especificar o nome da classe. Normalmente, as instâncias da classe especificada são criadas, e tais objetos são usados como plug-ins. Agora, o eXtreme Scale pode delegar que Spring obtenha instâncias destes objetos plug-in. Se um aplicativo utiliza o Spring, então, normalmente, tais POJOs possuem um requisito de serem conectados ao resto do aplicativo.

Referências relacionadas:

Java "Beans de Extensão Gerenciados pelo Spring" na página 682
É possível declarar que os POJOs sejam usados como pontos de extensão no arquivo `objectgrid.xml`. Se você nomear os beans e, em seguida, especificar o nome de classe, o eXtreme Scale normalmente cria instâncias da classe especificada e usa essas instâncias como o plug-in. O WebSphere eXtreme Scale pode delegar para que o Spring aja como o bean factory para obter instâncias desses objetos de plug-in.

Java Arquivo XML descritor do Spring
Use um arquivo XML descritor do Spring para configurar e integrar o eXtreme Scale com o Spring.

Java Arquivo `objectgrid.xsd` Spring
Use o arquivo `objectgrid.xsd` Spring para integrar o eXtreme Scale ao Spring para gerenciar as transações do eXtreme Scale e configurar os clientes e servidores.

Configurando Clientes na Estrutura Spring

Java

É possível substituir as configurações do ObjectGrid do lado do cliente com o Spring Framework.

Sobre Esta Tarefa

O arquivo XML de exemplo a seguir mostra como construir um elemento ObjectGridConfiguration e utilizá-lo para substituir algumas configurações do lado do cliente. Uma configuração semelhante pode ser criada usando a configuração programática ou configurando o arquivo XML do descritor do ObjectGrid.

Para obter informações sobre como usar os beans ObjectGridClientBean e ObjectGridCatalogServiceDomainBean para suportar a abstração de cache do Spring Framework Versão 3.1, consulte Configurando um Provedor de Cache Spring.

Procedimento

1. Crie um arquivo XML para configurar os clientes com a estrutura Spring.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE beans PUBLIC "-//SPRING//DTD BEAN//EN"
  "http://www.springframework.org/dtd/spring-beans.dtd">
<beans>
```

```
  <bean id="companyGrid" factory-bean="manager" factory-method="getObjectGrid"
    singleton="true">
    <constructor-arg type="com.ibm.websphere.objectgrid.ClientClusterContext">
      <ref bean="client" />
    </constructor-arg>
    <constructor-arg
type="java.lang.String" value="CompanyGrid" />
</bean>

  <bean id="manager" class="com.ibm.websphere.objectgrid.ObjectGridManagerFactory"
    factory-method="getObjectGridManager" singleton="true">
    <property name="overrideObjectGridConfigurations">
      <map>
        <entry key="DefaultDomain">
          <list>
            <ref bean="ogConfig" />
          </list>
        </entry>
      </map>
    </property>
  </bean>

  <bean id="ogConfig"
    class="com.ibm.websphere.objectgrid.config.ObjectGridConfigFactory"
    factory-method="createObjectGridConfiguration">
    <constructor-arg type="java.lang.String">
      <value>CompanyGrid</value>
    </constructor-arg>
    <property name="plugins">
      <list>
   <bean class="com.ibm.websphere.objectgrid.config.ObjectGridConfigFactory"
         factory-method="createPlugin">
         <constructor-arg type="com.ibm.websphere.objectgrid.config.PluginType"
           value="TRANSACTION_CALLBACK" />
         <constructor-arg type="java.lang.String"
           value="com.company.MyClientTxCallback" />
       </bean>
       <bean class="com.ibm.websphere.objectgrid.config.ObjectGridConfigFactory"
         factory-method="createPlugin">
         <constructor-arg type="com.ibm.websphere.objectgrid.config.PluginType"
           value="OBJECTGRID_EVENT_LISTENER" />
         <constructor-arg
type="java.lang.String" value="" />
       </bean>
      </list>
 </property>
      <property name="backingMapConfigurations">
        <list>
     <bean class="com.ibm.websphere.objectgrid.config.ObjectGridConfigFactory"
           factory-method="createBackingMapConfiguration">
           <constructor-arg
type="java.lang.String" value="Customer" />
             <property name="plugins">
      <bean class="com.ibm.websphere.objectgrid.config.ObjectGridConfigFactory"
                 factory-method="createPlugin">
                 <constructor-arg type="com.ibm.websphere.objectgrid.config.PluginType"
     value="EVICTOR" />
   <constructor-arg type="java.lang.String"
                   value="com.ibm.websphere.objectgrid.plugins.builtins.LRUEvictor" />
               </bean>
             </property>

           </bean>
           <bean class="com.ibm.websphere.objectgrid.config.ObjectGridConfigFactory"
             factory-method="createBackingMapConfiguration">
               <constructor-arg
type="java.lang.String" value="OrderLine" />
                  <property name="timeToLive" value="800" />
   <property name="ttlEvictorType">
                  <value type="com.ibm.websphere.objectgrid.
          TTLType">LAST_ACCESS_TIME</value>
   </property>
         </bean>
        </list>
       </property>
     </bean>

     <bean id="client" factory-bean="manager" factory-method="connect"
       singleton="true">
       <constructor-arg type="java.lang.String">
    <value>localhost:2809</value>
       </constructor-arg>
   <constructor-arg
```

```
            type="com.ibm.websphere.objectgrid.security.
          config.ClientSecurityConfiguration">
            <null />
          </constructor-arg>
        <constructor-arg type="java.net.URL">
          <null />
            </constructor-arg>
          </bean>
</beans>
```

2. Carregue o arquivo XML criado e construa o ObjectGrid.

```
BeanFactory beanFactory = new XmlBeanFactory(newUrlResource
  ("file:test/companyGridSpring.xml"));
ObjectGrid companyGrid = (ObjectGrid) beanFactory.getBean("companyGrid");
```

   Consulte o "Visão Geral da Estrutura Spring" na página 330 para obter mais informações sobre como criar um arquivo descritor XML.

Desenvolvendo Aplicativos da Grade de Dados com o Gateway REST

É possível usar o gateway Representational State Transfer (REST) para acessar grades de dados simples que são hospedados por um coletivo. Este gateway REST é útil quando você tiver que acessar os dados de grade a partir de ambientes não Java.

Antes de Iniciar

- **8.6+** É possível utilizar o gateway REST com o WebSphere eXtreme Scale Versão 8.6 ou posterior.

Sobre Esta Tarefa

Use o gateway REST para acessar os dados da grade de dados simples a partir de ambientes não Java como o aplicativo DataPower XI50 Appliance ou .NET. Também é possível usar o gateway REST para acessar os dados do mapa a partir de uma Java virtual machine que não pode hospedar o IBM Object Request Broker (ORB) que é usado pela API ObjectMap baseada em Java.

Transações

Cada operação REST para o WebSphere eXtreme Scale inicia e termina em uma transação independente para a grade de dados. Não é possível encadear diversas operações em uma única transação.

Equilíbrio de Carga

Quando você estiver usando o gateway REST, será responsabilidade do cliente balancear a carga de suas solicitações no coletivo WebSphere eXtreme Scale. É possível usar o balanceador de carga externo ou incluir a lógica adicional no cliente HTTP que você está usando no programa cliente.

Segurança

A comunicação através do gateway REST não resultará em uma configuração segura. Leia sobre a segurança do aplicativo da web no Centro de Informações do WebSphere Application Server para ativar o controle de acesso no gateway REST.

Relacionamento para WebSphere eXtreme Scale serviço de dados REST

O gateway REST é uma entidade separada do serviço de dados WebSphere eXtreme Scale REST, que implementa a interface Microsoft ADO.NET Data Services.

Gateway REST: Formato de URI

Ao especificar um URI em um formato específico, é possível acessar e executar operações em sua grade de dados simples.

Formato de URI

A URI de REST para acessar uma grade de dados simples no WebSphere eXtreme Scale está no seguinte formato:

```
/[context_root]/datacaches/[grid_name]/[map_name]/[key]
```

A raiz de contexto padrão é `recursos`.

Se você criar uma grade de dados simples denominada `MyMap` com o nome do host `mydatagrid.ibm.com`, a URL resultante para acessar o nome da chave `my.data.item` será:

```
http://mydatagrid.ibm.com/resources/datacaches/MyDataGrid/MyMap/my.data.item
```

No exemplo anterior, o mapa `MyMap` era usado na grade `MyDataGrid`. Este mapa não possui nenhum despejo de tempo de vida (TTL). As entradas que são colocadas na suspensão da grade de dados na grade de dados até que sejam explicitamente removidas. Para configurar o despejo TTL, consulte "Exemplo do Gateway REST: Expiração do Tempo de Vida (TTL)" na página 695.

Gateway REST: Formato de Dados

O gateway REST usa o cabeçalho de Tipo de Conteúdo em suas solicitações HTTP para determinar o formato de dados dos dados armazenados na grade de dados.

Formato de Dados

O gateway REST usa o cabeçalho de Tipo de Conteúdo em suas solicitações HTTP para determinar o formato de dados dos dados armazenados na grade de dados. Se inserir o conteúdo do tipo `application/xml`, quando o seu aplicativo entrar em uma operação GET para a mesma chave de cache, o corpo de resposta e o Tipo de Conteúdo estarão no tipo de formato equivalente. Neste exemplo, o corpo de resposta estaria no formato `application/xml`. É possível armazenar os dados de diversos tipos de conteúdo na mesma grade de dados. A seguir os exemplos de alguns tipos de conteúdo válidos:

Tabela 24. Tipos de Conteúdo para o Cabeçalho de Tipo de Conteúdo nas Solicitações de HTTP

Tipo de conteúdo	Utilização
`application/xml`	XML
`application/json`	Dados JavaScript
`application/octet-stream`	Objetos serializados, dados de propósito geral

Gateway REST: Operações REST

Use operações HTTP POST, GET e DELETE para inserir ou atualizar, obter e remover os dados da grade de dados.

Operações REST

Tabela 25. Operações com Métodos HTTP Equivalentes e Definições do Código de Resposta

Operação	Método HTTP	Código de Resposta
Inserir ou Atualizar	POST	• 200 CREATED: Os dados foram inseridos ou atualizados com êxito na grade de dados. • 400 BAD REQUEST: A operação de atualização ou inserção de dados não foi concluída com êxito.
Get	GET	• 200 OK: O corpo de resposta e o tipo de conteúdo são recuperados de uma operação de atualização ou inserção anterior. • 404 NOT FOUND: A chave especificada não está presente na grade de dados. • 400 BAD REQUEST: A grade de dados não pôde processar a solicitação.
Excluir	EXCLUIR	• 200 NO CONTENT: A entrada foi excluída da grade de dados. • 400 BAD REQUEST: A grade de dados não pôde processar a solicitação.

Exemplo de Gateway REST: Inserindo e Obtendo Entradas de Mapa de Grade de Dados

É possível usar os métodos POST e GET HTTP para inserir e obter entradas do mapa da grade de dados.

Exemplo: Operação de Inserção

Usando a URI definida e o formato de dados, é possível inserir as informações na grade de dados. O exemplo a seguir insere uma chave "bob" na grade MyGrid e no mapa MyGrid:

```
POST /resources/datacaches/MyGrid/MyGrid/bob
Content-type: application/xml
<mydata>this is some data</mydata>
```

Exemplo: Operação Get

Para recuperar essa chave que foi inserida no exemplo anterior, é possível usar a seguinte URI:

```
GET /resources/datacaches/MyGrid/MyGrid/bob
```

Você deve executar as operações GET em uma chave individual. Não é possível recuperar todas as entradas do mapa.

Exemplo de Gateway REST: Limpando Entradas de Mapa de Grade de Dados

É possível usar o método HTTP DELETE do gateway REST para limpar um mapa em uma grade de dados.

Limpando uma Entrada Individual

Para excluir uma entrada individual, use o método DELETE e o nome da chave do objeto:

```
DELETE http://mydatagrid.ibm.com/resources/datacaches/MyDataGrid/MyDataGrid/my.data.item
```

Limpando um Mapa Inteiro na Grade de Dados

Para limpar um mapa inteiro na grade de dados, use o método HTTP DELETE e omita a parte da chave da URI. Por exemplo, para limpar o mapa MyDataMap.LUT na grade de dados MyDataGrid, use a seguinte operação:

```
DELETE http://mydatagrid.ibm.com/resources/datacaches/MyDataGrid/MyDataMap.LUT
```

Exemplo de Gateway REST: Criando Mapas Dinâmicos

Você pode utilizar modelos de mapa para criar mapas conforme seu aplicativo requer.

Criação de Mapa Dinâmico

A primeira operação para um mapa que corresponde ao modelo de mapa, mas que ainda não foi criado resulta na criação de um novo mapa dinâmico. Como exemplo, para criar um novo mapa dinâmico, você pode utilizar o seguinte URI em uma operação GET, DELETE ou POST:

```
http://mydatagrid.ibm.com/resources/datacaches/MyDataGrid/MyMap1/a.key
```

No exemplo anterior, o mapa criado dinamicamente é `MyMap1`, em que o nome do modelo do mapa é `MyMap.*` e o atributo `template` nesse mapa é configurado como `true`.

Consulte “Opções de Configuração de Mapa Dinâmico” na página 382 para obter informações adicionais sobre como nomear mapas dinâmicos.

Exemplo do Gateway REST: Expiração do Tempo de Vida (TTL)

Você pode configurar uma expiração de TTL em chaves no WebSphere eXtreme Scale.

Exemplo

Para configurar um valor de TTL, forneça o parâmetro de solicitação de TTL com um valor em segundos. Por exemplo, para configurar um valor TTL de 600 segundos na chave `a.key`, especifique o parâmetro de solicitação `ttl` quando o valor for inserido ou atualizado na grade de dados usando o método HTTP POST:

```
http://mydatagrid.ibm.com/resources/datacaches/MyDataGrid/MyMap.LUT/a.key?ttl=600
```

Desenvolvendo Aplicativos .NET

.NET

É possível desenvolver aplicativos Microsoft .NET que usam a mesma grade de dados que seus aplicativos Java.

Informações relacionadas:

.NET 8.6+ "Lição 3.3 do Tutorial de Introdução: Executando o Aplicativo Cliente de Amostra .NET" na página 248
Use as etapas a seguir para executar um aplicativo cliente .NET para interagir com a grade de dados. O servidor de catálogos, o servidor de contêiner e o cliente são todos executados em um único servidor neste exemplo.

Configurando o Ambiente de Desenvolvimento .NET

.NET

Para usar o WebSphere eXtreme Scale Client para .NET no Microsoft Visual Studio, você deve instalar o ambiente de desenvolvimento e configurar seu projeto para usar a montagem do WebSphere eXtreme Scale Client para .NET.

Antes de Iniciar

- Para obter uma lista das liberações suportadas do Microsoft Visual Studio, consulte "Considerações sobre o Microsoft .NET" na página 308.
- Instale o WebSphere eXtreme Scale Client para .NET. No assistente de instalação, escolha o caminho **Customizado** e selecione o ambiente de desenvolvimento. Para obter informações adicionais, consulte Instalando o WebSphere eXtreme Scale Client para .NET.

Procedimento

1. Em seu ambiente do Microsoft Visual Studio, abre seu projeto.
2. Inclua uma referência para o conjunto WebSphere eXtreme Scale Client para .NET. O conjunto está no diretório *net_client_home*\bin. Escolha o arquivo IBM.WebSphere.Caching.dll.
3. Inclua as seguintes linhas em seu aplicativo para utilizar as APIs do WebSphere eXtreme Scale Client para .NET:

```
using IBM.WebSphere.Caching;
using IBM.WebSphere.Caching.Map;
```

Resultados

Quando você integra os conjuntos no ambiente de desenvolvimento, o IntelliSense é ativado para as APIs do WebSphere eXtreme Scale Client para .NET.

O que Fazer Depois

Use as APIs do WebSphere eXtreme Scale Client para .NET em seu aplicativo cliente. Para obter mais informações sobre como acessar a documentação da API, consulte "Acessando o WebSphere eXtreme Scale Client para Documentação da API .NET" na página 697.

Informações relacionadas:

.NET 8.6+ "Tutorial de Introdução - Lição 2.2: Criando um Aplicativo Cliente .NET" na página 240
Para inserir, excluir, atualizar e recuperar dados de sua grade de dados, você deverá gravar um aplicativo cliente. A introdução de amostra inclui um aplicativo cliente .NET que pode ser usado para saber mais sobre a criação de seu próprio aplicativo cliente.

Acessando o WebSphere eXtreme Scale Client para Documentação da API .NET

.NET

É possível acessar a documentação do WebSphere eXtreme Scale Client para a API .NET em um arquivo `.chm` ou visualizando a documentação da API no centro de informações.

Procedimento

Utilize uma das seguintes opções para abrir a documentação do WebSphere eXtreme Scale Client para a API .NET:

- Use a documentação da API do Cliente .NET que é instalada com o produto. Para abrir a documentação da API do cliente .NET localmente, abra o arquivo *net_client_home*`\doc\IBM.WebSphere.Caching.chm`.
- Visualize a documentação da API no centro de informações. Para obter mais informações, consulte Documentação do Cliente para API .NET.

Informações relacionadas:

.NET 8.6+ "Tutorial de Introdução - Lição 2.2: Criando um Aplicativo Cliente .NET" na página 240
Para inserir, excluir, atualizar e recuperar dados de sua grade de dados, você deverá gravar um aplicativo cliente. A introdução de amostra inclui um aplicativo cliente .NET que pode ser usado para saber mais sobre a criação de seu próprio aplicativo cliente.

.NET 8.6+ "Lição 3.3 do Tutorial de Introdução: Executando o Aplicativo Cliente de Amostra .NET" na página 248
Use as etapas a seguir para executar um aplicativo cliente .NET para interagir com a grade de dados. O servidor de catálogos, o servidor de contêiner e o cliente são todos executados em um único servidor neste exemplo.

Definindo Anotações ClassAlias e FieldAlias para Correlacionar Classes Java e .NET

Use as anotações ClassAlias e FieldAlias para ativar o compartilhamento de dados da grade de dados entre suas classes Java e .NET.

Antes de Iniciar

- Você deve ter o IBM eXtremeIO configurado. Para obter informações adicionais, consulte "Configurando o IBM eXtremeIO (XIO)" na página 119.
- Seu atributo copyMode em seu arquivo XML do descritor do ObjectGrid deve ser configurado como COPY_TO_BYTES. Para obter informações adicionais, consulte "Configurando Grades de Dados para Utilizar o eXtreme Data Format (XDF)" na página 121.

Sobre Esta Tarefa

Você pode considerar o uso das anotações ClassAlias e FieldAlias se tiver uma classe Java existente e desejar criar uma classe C# correspondente. Neste cenário, você inclui as anotações em sua classe C# que inclui o nome de classe Java. Para obter mais informações sobre as anotações ClassAlias e FieldAlias, consulte "Anotações ClassAlias e FieldAlias" na página 125.

Procedimento

Utilize as anotações ClassAlias e FieldAlias para correlacionar os objetos entre uma classe Java e uma classe C#. Java

.NET

Java

```
@ClassAlias("Employee")
class com.company.department.Employee {

     @FieldAlias("id")
     int myId;

      String name;
}
```

Figura 45. Exemplo de Java com as Anotações ClassAlias e FieldAlias

.NET

```
[ ClassAlias( "Employee") ]
class Com.MyCompany.Employee {

     [ FieldAlias("id") ]
      int identifier;

      string name;
}
```

Figura 46. Exemplo de .NET com os Atributos ClassAlias e FieldAlias

Conceitos relacionados:

8.6+ "Anotações ClassAlias e FieldAlias" na página 125
Use as anotações ClassAlias e FieldAlias para ativar o compartilhamento de dados da grade de dados entre classes. É possível compartilhar dados entre duas classes Java ou entre uma classe Java e uma .NET.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Informações relacionadas:

8.6+ "Lição 2.3: Criando um Aplicativo de Grade de Dados Corporativos" na página 243
Para criar um aplicativo de grade de dados corporativos no qual clientes Java e .NET podem atualizar a mesma grade de dados, você deve tornar suas classes compatíveis. Nos aplicativos de amostra de introdução, o aplicativo de amostra .NET tem aliases para corresponderem aos padrões Java.

Anotações ClassAlias e FieldAlias

Use as anotações ClassAlias e FieldAlias para ativar o compartilhamento de dados da grade de dados entre classes. É possível compartilhar dados entre duas classes Java ou entre uma classe Java e uma .NET.

Se você definir duas classes com o mesmo nome e campos, os dados da grade de dados serão automaticamente compartilhados entre as classes. Por exemplo, se você tiver uma classe Customer1 em seu aplicativo Java e uma classe Customer1 em seu aplicativo .NET que tenha os mesmos campos, os dados serão compartilhados entre as classes. Isso supõe que o nome de classe também inclui o qualificador de classe, que também é o nome do pacote em Java e namespace em C#. O nome do pacote e o namespace são compartilhados automaticamente porque o namespace e os nomes de pacotes correspondem. Consulte o exemplo a seguir, em que ambos os nomes não fazem distinção entre maiúsculas e minúsculas:

```
Java:
package com.mycompany.app
public class SampleClass {
int field1;
String field2;
}

C#
namespace Com.MyCompany.App
public class SampleClass {
int field1;
string field2;
}
```

No entanto, você também pode correlacionar dados entre as classes que possuem nomes diferentes. Para correlacionar dados a serem armazenados na grade de dados entre os nomes de classe diferentes, utilize as anotações ClassAlias ou FieldAlias.

Entre dois aplicativos Java: É possível definir duas classes diferentes com nomes diferentes em ambientes de aplicativos Java separados. Marcando as classes com a mesma anotação de ClassAlias, e todos os campos e tipos de campo são correspondidos entre estas duas classes, as classes são correlacionadas com o mesmo ID de tipo de classe, embora tenham os nomes de classe diferentes. O mesmo ID de tipo de classe e os metadados podem, então, ser reutilizados entre as classes nos diferentes tempos de execução de aplicativos Java.

Entre um aplicativo Java e um aplicativo .NET: É possível usar anotações semelhantes em seu aplicativo C# para correlacionar a classe C# com uma classe Java. Os atributos ClassAlias definidos para a classe C# e os campos são correspondidos a uma classe Java com a mesma anotação de ClassAlias.

Tarefas relacionadas:

8.6+ "Definindo Anotações ClassAlias e FieldAlias para Correlacionar Classes Java e .NET" na página 124
Use as anotações ClassAlias e FieldAlias para ativar o compartilhamento de dados da grade de dados entre suas classes Java e .NET.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Informações relacionadas:

8.6+ "Lição 2.3: Criando um Aplicativo de Grade de Dados Corporativos" na página 243
Para criar um aplicativo de grade de dados corporativos no qual clientes Java e .NET podem atualizar a mesma grade de dados, você deve tornar suas classes compatíveis. Nos aplicativos de amostra de introdução, o aplicativo de amostra .NET tem aliases para corresponderem aos padrões Java.

Mapeando Chaves para Partições com Anotações PartitionKey

Um alias PartitionKey é usado para identificar os campos ou atributos nos quais um cálculo de código hash é executado para determinar a partição na qual dados são salvos. A anotação PartitionKey é válida somente nos atributos-chave.

Antes de Iniciar

Você deve estar usando eXtreme Data Format. Para obter informações adicionais, consulte "Configurando Grades de Dados para Utilizar o eXtreme Data Format (XDF)" na página 121.

Sobre Esta Tarefa

Você configura um alias PartitionKey para assegurar que diversas classes salvem dados na mesma partição. Por exemplo, se você configurar o valor de PartitionKey para ser a chave departmentID, registros de funcionários serão colocados na mesma partição.

A interface PartionableKey é a interface Java existente e tem precedência sobre a anotação PartitionableKey em C#.

Procedimento

- Java Defina anotações PartitionKey em um campo em um aplicativo Java.

Java

```
class Employee {
    int empId;

    @PartitionKey(order = 0)
    int deptId;

}
```

É possível configurar anotações PartitionKey em diversas chaves ou configurar o alias PartitionKey em uma classe. Para obter exemplos adicionais sobre como configurar anotações PartitionKey em aplicativos Java, consulte Documentação de API Java: Tipo de Anotação PartitionKeys.

- .NET Defina atributos de PartitionKey em um campo em um aplicativo .NET.

```
class Employee {
    int empId;

    [PartitionKey]
    int deptId;
}
```

Também é possível configurar atributos de PartitionKey em classes .NET. Para obter informações adicionais, consulte Documentação de API .NET: Classe PartitionKeyAttribute.

Configurando a Segurança da Grade de Dados e SSL para .NET

.NET

É possível configurar .NET e Java para comunicação por meio de Secure Sockets Layer (SSL) e para usar a lógica de autenticação UserPassword.

Antes de Iniciar

Você deve ter os arquivos `key.jks` e `trust.jks` para seu ambiente. Para obter informações adicionais sobre como criar arquivos de keystore e de armazenamento confiável, consulte "Tutorial de Segurança do Java SE - Etapa 6" na página 34.

Procedimento

1. Ative e configure a segurança em seus servidores. Se a segurança ainda não estiver configurada em seus servidores, use as etapas a seguir para configurar a segurança com a amostra do autenticador externo.
   a. Obtenha os arquivos de segurança de amostra. Faça download dos arquivos de amostra no arquivo `security_extauth.zip` do wiki do WebSphere eXtreme Scale.
      - `xsjaas3.config` : Define a configuração de Java Authentication and Authorization Service (JAAS).
      - `sampleKS3.jks` Contém o keystore de valores de usuário e senha do JAAS.
      - `security3.xml` Define o autenticador para utilização para segurança.
   b. Edite o arquivo `xsjaas3.config` e corrija o caminho para o arquivo `sampleKS3.jks`.
   c. Se desejar gerar seu próprio keystore privado em vez de usar o arquivo `sampleKS3.jks` de amostra, utilize o utilitário **`keytool`** para gerar a chave privada.

      ```
      keytool -genkey -alias myalias -keysize 2048 -keystore key.jks -keyalg rsa -dname
       "CN=www.mydomain.com" -storepass password -keypass password -validity 3650
      ```

   d. Edite o `sampleServer.properties` para ativar a segurança. O arquivo `sampleServer.properties` está no diretório *wxs_install_root*`\properties`. Remova o comentário e edite os seguintes valores da propriedade:

```
securityEnabled=true
secureTokenManagerType=none
alias=ogsample
contextProvider=IBMJSSE2
protocol=SSL
keyStoreType=JKS
keyStore=../../../../xio.test/etc/test/security/key.jks
keyStorePassword=ogpass
trustStoreType=JKS
trustStore=../../../../xio.test/etc/test/security/trust.jks
trustStorePassword=ogpass
```

e. Inicie os servidores de catálogo e contêiner.

```
startXsServer.bat cs0 -catalogServiceEndPoints
cs0:localhost:6600:6601 -listenerPort 2809 -objectgridFile
gettingstarted\xml\objectgrid.xml
-deploymentPolicyFile gettingstarted\xml\deployment.xml
-serverProps ..\properties\sampleServer.properties
-clusterSecurityFile security3.xml -jvmArgs
-Djava.security.auth.login.config="xsjaas3.config"
```

```
startXsServer.bat c0 -catalogServiceEndPoints
localhost:2809 -objectgridFile gettingstarted\xml\objectgrid.xml
-deploymentPolicyFile gettingstarted\xml\deployment.xml
-serverProps ..\properties\sampleServer.properties
-clusterSecurityFile security3.xml -jvmArgs
-Djava.security.auth.login.config="xsjaas3.config"
```

2. Configure a segurança para o cliente .NET.

a. Opcional: Usando o utilitário keytool, extraia o certificado público do arquivo `key.jks` que você configurou para o servidor.

```
keytool -export -alias myalias -keystore key.jks -file public.cer -storepass password
```

Importe essa chave pública para o armazenamento de certificados do Windows com o Certificate Management Tool, `certmgr.msc`, para importar a chave para a pasta de certificados 'Trusted Root Certification Authority' ou 'Trusted People'. (A propriedade **keyStore** no arquivo `client.properties` pode apontar para esse arquivo)

b. Edite o arquivo `Client.Net.properties` para incluir os valores de propriedades a seguir:

```
securityEnabled=true
credentialAuthentication=supported
authenticationRetryCount=3
credentialGeneratorAssembly=IBM.WebSphere.Caching.C
CredentialGenerator,Version=8.6.0.0,
Culture=neutral,PublicKeyToken=b439a24ee43b0816
credentialGeneratorProps=manager manager1
transportType=ssl-supported
publicKeyFile=<name>.cer
```

O valor da propriedade credentialGeneratorProps, `manager manager1` é usado como os valores de nome de usuário e senha que são fornecidos ao servidor no objeto de Credencial.

A propriedade **publicKeyFile** é configurada como um caminho relativo para o tempo de execução de .NET. Se a propriedade **publicKeyFile** não estiver configurada, no armazenamento de certificados do Windows 'a' é procurado o arquivo `public.cer`. Se a propriedade **publicKeyFile** for configurada, então, o arquivo especificado será usado para o arquivo de certificado público de SSL. Se o arquivo especificado não puder ser localizado, o cliente .NET tenta localizar um arquivo `public.cer` correspondente no armazenamento de certificados.

c. Copie *net_client_home*\IBM.WebSphere.Caching.CredentialGenerator.dll para o diretório *net_client_home*\sample\SimpleClient\bin\<*ConfigurationName*>.

d. Construa uma amostra com o contexto de projeto *ConfigurationName*. Execute a amostra em seu servidor.

Autenticação de Cliente .NET de Programação

.NET

Para enviar credenciais do cliente .NET para o lado do servidor, você deve implementar as interfaces ICredentialGenerator e ICredential. Essas interfaces geram um objeto de credencial que é transmitido para a grade de dados e interpretados no lado do servidor. No lado do servidor, o plug-in correspondente interpreta o objeto de credencial.

Sobre Esta Tarefa

Para concluir a autenticação, o aplicativo .NET deve implementar as seguintes interfaces:

- ICredential: Um Credential representa uma credencial de cliente, tal como um par de ID do usuário e senha.
- ICredentialGenerator: Um CredentialGenerator representa uma factory de credencial para gerar a credencial.

Quando um aplicativo cliente .NET se conecta a um servidor que requer autenticação, o cliente precisa fornecer uma credencial de cliente. Uma credencial de cliente é representada pela interface ICredential. Uma credencial de cliente pode ser um par de nome de usuário e senha, um registro do Kerberos, um certificado cliente ou dados em qualquer formato concordado entre o cliente e o servidor. Esta interface explicitamente define os métodos equals(Object) e hashCode. Estes métodos são importantes porque os objetos Subject autenticados são armazenados em cache utilizando o objeto Credential como a chave no lado do servidor. Também é possível gerar uma credencial com a interface ICredentialGenerator. Esta interface é útil quando a credencial pode expirar. Uma nova credencial é gerada sempre que a propriedade Credential for obtida.

Também é possível usar o plug-in CredentialGenerator fornecido para criar uma credencial baseada na configuração **Client.Net.Properties credentialGeneratorProps=** no arquivo Client.Net.Properties. As configurações adicionais que definem plug-in de credencial são **credentialGeneratorAssembly** e **credentialGeneratorClass**.

Procedimento

Implemente as interfaces ICredentialGenerator e ICredential no aplicativo cliente .NET. É possível utilizar os seguintes exemplos para desenvolver seu aplicativo:

- “Exemplo: Implementando uma Credencial de Senha de Usuário para Aplicativos .NET” na página 704
- “Exemplo: Implementando um Gerador de Credencial do Usuário para Aplicativos .NET” na página 706

Referências relacionadas:

"Exemplo: Implementando uma Credencial de Senha de Usuário para Aplicativos .NET"
É possível usar este exemplo para gravar sua própria implementação da interface ICredential. A credencial de senha do usuário armazena um ID de usuário e uma senha.

"Exemplo: Implementando um Gerador de Credencial do Usuário para Aplicativos .NET" na página 706
É possível usar este exemplo para gravar sua própria implementação da interface ICredentialGenerator. A interface utiliza um ID do usuário e uma senha. O objeto UserPasswordCredential contém o ID do usuário e a senha, que são obtidos da propriedade Credential somente leitura.

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Informações relacionadas:

Interface ICredential

Interface ICredentialGenerator

Exemplo: Implementando uma Credencial de Senha de Usuário para Aplicativos .NET

.NET

É possível usar este exemplo para gravar sua própria implementação da interface ICredential. A credencial de senha do usuário armazena um ID de usuário e uma senha.

UserPasswordCredential.cs

```
// Module  :  UserPasswordCrediential.cs

using System;
using IBM.WebSphere.Caching.Security;

namespace com.ibm.websphere.objectgrid.security.plugins.builtins
{
    public class UserPasswordCredential : ICredential
    {
        private String ivUserName;

        private String ivPassword;

        /// <summary>
        ///Creates a UserPasswordCredential with the specified user name and
        /// password.
        ///
        /// ArgumentException if userName or password is null
        /// </summary>
        /// <param name="userName">the user name for this credential</param>
        /// <param name="password">the password for this credential</param>
        public UserPasswordCredential(String userName, String password) {
            if (userName == null || password == null) {
                throw new ArgumentException("User name and password cannot be null.");
            }
            this.ivUserName = userName;
            this.ivPassword = password;
        }

        /// <summary>Gets the user name for this credential.</summary>
        /// <returns>the user name argument that was passed to the constructor
        ///or the setUserName(String) method of this class </returns>
        public String GetUserName() {
            return ivUserName;
        }
```

```
        /// <summary>Sets the user name for this credential.
        ///ArgumentException if userName is null
        /// </summary>
        /// <param name="userName">userName the user name to set.</param>
        public void SetUserName(String userName) {
            if (userName == null) {
                throw new ArgumentException("User name cannot be null.");
            }
            this.ivUserName = userName;
        }

        /// <summary>Gets the password for this credential.
        /// </summary>
        /// <returns>the password argument that was passed to the constructor or the setPassword(String) method of this class</returns>
        public String GetPassword() {
            return ivPassword;
        }

        /// <summary>Sets the password for this credential.
        ///ArgumentException if password is null
        /// </summary>
        /// <param name="password">the password to set.</param>
        public void SetPassword(String password) {
            if (password == null) {
                throw new ArgumentException("Password cannot be null.");
            }
            this.ivPassword = password;
        }

        /// <summary>Checks two UserPasswordCredential objects for equality.
        ///<p>
        /// Two UserPasswordCredential objects are equal if and only if their user names
        /// and passwords are equal.
        /// </summary>
        /// <param name="o">the object we are testing for equality with this object.</param>
        /// <returns>true if both UserPasswordCredential objects are equivalent.</returns>
        public bool Equals(ICredential credential)
        {
            if (this == credential) {
                return true;
            }
            if (credential is UserPasswordCredential) {
                UserPasswordCredential other = (UserPasswordCredential)credential;
                return other.ivPassword.Equals(ivPassword) && other.ivUserName.Equals(ivUserName);
            }
            return false;
        }

        /// <summary>Returns the hashcode of the UserPasswordCredential object.
        /// </summary>
        /// <returns>return the hash code of this object</returns>
        public override int GetHashCode() {
            int ret = ivUserName.GetHashCode() + ivPassword.GetHashCode();
            return ret;
        }

        /// <summary>this.Object as a string
        /// </summary>
        /// <returns>return the string presentation of the UserPasswordCredential object.</returns>
        public override String ToString() {
            return typeof(UserPasswordCredential).FullName + "[" + ivUserName + ",xxxxxx]";
        }

    }
}
```

Tarefas relacionadas:

"Autenticação de Cliente .NET de Programação" na página 703
Para enviar credenciais do cliente .NET para o lado do servidor, você deve implementar as interfaces ICredentialGenerator e ICredential. Essas interfaces geram um objeto de credencial que é transmitido para a grade de dados e interpretados no lado do servidor. No lado do servidor, o plug-in correspondente interpreta o objeto de credencial.

Informações relacionadas:

Interface ICredential

Interface ICredentialGenerator

Exemplo: Implementando um Gerador de Credencial do Usuário para Aplicativos .NET

É possível usar este exemplo para gravar sua própria implementação da interface ICredentialGenerator. A interface utiliza um ID do usuário e uma senha. O objeto UserPasswordCredential contém o ID do usuário e a senha, que são obtidos da propriedade Credential somente leitura.

UserPasswordCredentialGenerator.cs

```
// Module  :  UserPasswordCredientialGenerator.cs
//
// Source File Description: Reference Documentation
//
using System;
using System.Security.Authentication;
using IBM.WebSphere.Caching.Security;
using com.ibm.websphere.objectgrid.security.plugins.builtins;

namespace IBM.WebSphere.Caching.Security
{
    public class UserPasswordCredentialGenerator : ICredentialGenerator
    {

        private String ivUser;

        private String ivPwd;

        public ICredential Credential { get { return _getCredential(); } }

        public string Properties { set {_setProperties(value);} }

        public UserPasswordCredentialGenerator() {
            ivUser = null;
            ivPwd = null;
        }


        public UserPasswordCredentialGenerator(String user=null, String pwd=null)
        {
            ivUser = user;
            ivPwd = pwd;
        }

        /// <summary>Creates a new UserPasswordCredential object using this object's user name and password.
        /// </summary>
        /// <returns>new UserPasswordCredential instance</returns>
        private ICredential _getCredential()
        {
            try
            {
                ICredential MyCredential = new UserPasswordCredential(ivUser, ivPwd) as ICredential;
                return (ICredential) MyCredential;
            }
            catch (Exception e)
            {
                AuthenticationException CannotGenerateCredentialException = new AuthenticationException(e.ToString());
                throw CannotGenerateCredentialException;
            }
        }
```

```
/// <summary>Gets the password for this credential generator.
/// </summary>
/// <returns>the password argument that was passed to the constructor</returns>
public String getPassword() {
    return ivPwd;
}

/// <summary>Gets the user name for this credential.
/// </summary>
/// <returns>the user argument that was passed to the constructor of this class</returns>
public String getUserName()
{
    return ivUser;
}

/// <summary>Sets additional properties namely a user name and password.
///Throws ArgumentException if the format is not valid
/// </summary>
/// <param name="properties">properties a properties string  with a user name and a password separated by a blank.</param>
private void _setProperties(string properties)
{
    String token = properties;
    char[] Seperator = { ' ' };
    String[] StringProperty = properties.Split(Seperator);
    if (StringProperty.Length != 2)
    {
        throw new ArgumentException(
            "The properties should have a user name and password and separated by a space.");
    }

    ivUser = StringProperty[0];
    ivPwd = StringProperty[1];
}

/// <summary>Checks two UserPasswordCredentialGenerator objects for equality.
///<p>
///Two UserPasswordCredentialGenerator objects are equal if and only if
///their user names and passwords are equal.
/// </summary>
/// <param name="obj">the object we are testing for equality with this object.</param>
/// <returns><code>true</code> if both UserPasswordCredentialGenerator objects are equivalent</returns>
public override bool Equals(Object obj)
{
    if (obj == this) {
        return true;
    }

    if (obj != null && obj is UserPasswordCredentialGenerator)
    {
        UserPasswordCredentialGenerator other = (UserPasswordCredentialGenerator) obj;

        Boolean bothUserNull = false;
        Boolean bothPwdNull = false;

        if (ivUser == null) {
            if (other.ivUser == null) {
                bothUserNull = true;
            }
            else
            {
                return false;
            }
        }

        if (ivPwd == null) {
            if (other.ivPwd == null) {
                bothPwdNull = true;
            }
            else
            {
                return false;
            }
        }
        return (bothUserNull || ivUser.Equals(other.ivUser)) && (bothPwdNull || ivPwd.Equals(other.ivPwd));
    }
    return false;
}
```

```
        /// <summary>Returns the hashcode of the UserPasswordCredentialGenerator object.
        /// </summary>
        /// <returns>the hash code of this object</returns>
        public override int GetHashCode()
        {
           return ivUser.GetHashCode() + ivPwd.GetHashCode();
        }

    }

}
```

Tarefas relacionadas:

"Autenticação de Cliente .NET de Programação" na página 703
Para enviar credenciais do cliente .NET para o lado do servidor, você deve implementar as interfaces ICredentialGenerator e ICredential. Essas interfaces geram um objeto de credencial que é transmitido para a grade de dados e interpretados no lado do servidor. No lado do servidor, o plug-in correspondente interpreta o objeto de credencial.

Informações relacionadas:

Interface ICredential

Interface ICredentialGenerator

Capítulo 6. Ajuste do desempenho

É possível ajustar as configurações em seu ambiente para aumentar o desempenho geral de seu ambiente do WebSphere eXtreme Scale.

Ajustando Sistemas Operacionais e Configurações de Rede

O ajuste da rede pode reduzir o atraso da pilha do Protocolo de Controle de Transmissões (TCP) por meio da mudança das configurações de conexão e melhorar o rendimento por meio da mudança dos buffers TCP.

Sistemas Operacionais

Um sistema Windows precisa do mínimo de ajuste enquanto que o sistema Solaris precisa do máximo de ajuste. As informações a seguir referem-se a cada sistema especificado e podem aumentar o desempenho do WebSphere eXtreme Scale. Você deve ajustar de acordo com sua carga de rede e do aplicativo.

Windows

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
Tcpip\Parameters
MaxFreeTcbs = dword:00011940
MaxHashTableSize = dword:00010000
MaxUserPort = dword:0000fffe
TcpTimedWaitDelay = dword:0000001e
```

Solaris

```
ndd -set /dev/tcp tcp_time_wait_interval 60000
fndd -set /dev/tcp tcp_keepalive_interval 15000
ndd -set /dev/tcp tcp_fin_wait_2_flush_interval 67500
ndd -set /dev/tcp tcp_conn_req_max_q 16384
ndd -set /dev/tcp tcp_conn_req_max_q0 16384
ndd -set /dev/tcp tcp_xmit_hiwat 400000
ndd -set /dev/tcp tcp_recv_hiwat 400000
ndd -set /dev/tcp tcp_cwnd_max 2097152
ndd -set /dev/tcp tcp_ip_abort_interval 20000
ndd -set /dev/tcp tcp_rexmit_interval_initial 4000
ndd -set /dev/tcp tcp_rexmit_interval_max 10000
ndd -set /dev/tcp tcp_rexmit_interval_min 3000
ndd -set /dev/tcp tcp_max_buf 4194304
```

AIX

```
/usr/sbin/no -o tcp_sendspace=65536
/usr/sbin/no -o tcp_recvspace=65536
/usr/sbin/no -o udp_sendspace=65536
/usr/sbin/no -o udp_recvspace=65536
/usr/sbin/no -o somaxconn=10000
/usr/sbin/no -o tcp_nodelayack=1
/usr/sbin/no –o tcp_keepinit=40
/usr/sbin/no –o tcp_keepintvl=10
```

LINUX

```
sysctl -w net.ipv4.tcp_timestamps=0
sysctl -w net.ipv4.tcp_tw_reuse=1
sysctl -w net.ipv4.tcp_tw_recycle=1
sysctl -w net.ipv4.tcp_fin_timeout=30
sysctl -w net.ipv4.tcp_keepalive_time=1800
sysctl -w net.ipv4.tcp_rmem="4096 87380 8388608"
sysctl -w net.ipv4.tcp_wmem="4096 87380 8388608"
sysctl -w net.ipv4.tcp_max_syn_backlog=4096
```

HP-UX

```
ndd -set /dev/tcp tcp_ip_abort_cinterval 20000
```

Propriedades do ORB

Java

(Descontinuado) As propriedades do Object Request Broker (ORB) modificam o comportamento de transporte da grade de dados. Essas propriedades podem ser configuradas com um arquivo `orb.properties`, como configurações no console administrativo do WebSphere Application Server ou como propriedades customizadas no ORB no console administrativo do WebSphere Application Server.

Reprovado:  8.6+ O Object Request Broker (ORB) foi descontinuado. Se você não estava usando o ORB em uma liberação anterior, use o IBM eXtremeIO (XIO) para seu mecanismo de transporte. Se estiver usando o ORB, considere migrar sua configuração para usar XIO.

orb.properties

O arquivo `orb.properties` está no diretório `java/jre/lib`. Quando você modifica o arquivo `orb.properties` em um diretório `java/jre/lib` do WebSphere Application Server, as propriedades do ORB são atualizadas no agente do nó e quaisquer outras Java virtual machines (JVMs) que estão utilizando o Java runtime environmen (JRE). Se você desejar esse comportamento, use as propriedades customizadas ou as configurações do ORB no console administrativo do WebSphere Application Server.

Configurações Padrão do WebSphere Application Server

O WebSphere Application Server possui algumas propriedades definidas no ORB por padrão. Essas configurações estão nos serviços de contêiner do servidor de aplicativos e no gerenciador de implementação. Essas definições padrão substituem quaisquer configurações criadas no arquivo `orb.properties`. Para cada propriedade descrita, consulte a seção **Onde especificar** para determinar o local para definir o valor sugerido.

Configurações do Descritor de Arquivo

Para sistemas UNIX e Linux, existe um limite para o número de arquivos abertos que são permitidos por processo. O sistema operacional especifica a quantidade de arquivos abertos permitidos. Se este valor for configurado muito baixo, ocorrerá um erro de alocação de memória no AIX e muitos arquivos abertos serão registrados no log.

Na janela de terminal do sistema UNIX, configure este valor para um valor mais alto que o valor do sistema padrão. Para máquinas SMP maiores com clones, configure para ilimitado.

Para configurações do AIX, defina esta valor como ilimitado com o comando: `ulimit -n unlimited`.

Para configurações Solaris, configure este valor como `16384` com o comando: `ulimit -n 16384`.

Para exibir o valor atual, use o comando: `ulimit -a`.

Configurações de Linha de Base

As seguintes configurações são uma linha de base ideal mas não necessariamente as melhores configurações para cada ambiente. Entenda as configurações para ajudar a tomar uma boa decisão sobre quais valores são apropriados no seu ambiente.

```
com.ibm.CORBA.RequestTimeout=30
com.ibm.CORBA.ConnectTimeout=10
com.ibm.CORBA.FragmentTimeout=30
com.ibm.CORBA.LocateRequestTimeout=10
com.ibm.CORBA.ThreadPool.MinimumSize=256
com.ibm.CORBA.ThreadPool.MaximumSize=256
com.ibm.CORBA.ThreadPool.IsGrowable=false
com.ibm.CORBA.ConnectionMultiplicity=1
com.ibm.CORBA.MinOpenConnections=1024
com.ibm.CORBA.MaxOpenConnections=1024
com.ibm.CORBA.ServerSocketQueueDepth=1024
com.ibm.CORBA.FragmentSize=0
com.ibm.CORBA.iiop.NoLocalCopies=true
com.ibm.CORBA.NoLocalInterceptors=true
```

Descrições de Propriedades

Configurações de Tempo Limite

As seguintes configurações referem-se à quantia de tempo em que o ORB aguardará antes que as operações sobre pedidos sejam canceladas. Use essas configurações para evitar que encadeamentos em excesso sejam criados em uma situação anormal.

Tempo Limite do Pedido

Nome da Propriedade: com.ibm.CORBA.RequestTimeout

Valor válido: Valor de número inteiro para o número de segundos.

Valor sugerido : 30

Onde especificar: Console administrativo do WebSphere Application Server

Descrição: Indica quantos segundos uma solicitação aguarda por uma resposta antes de ser cancelada. Essa propriedade influencia a quantia de tempo em que um cliente precisa para efetuar failover se ocorrer uma falha de interrupção de rede. Se você configurar essa propriedade muito baixo, os pedidos poderão atingir o tempo limite involuntariamente. Considere cuidadosamente o valor dessa propriedade para evitar tempos limites acidentais.

Tempo Limite de Conexão

Nome da Propriedade: com.ibm.CORBA.ConnectTimeout

Valor válido: Valor de número inteiro para o número de segundos.

Valor sugerido : 10

Onde especificar: arquivo `orb.properties`

Descrição: Indica quantos segundos uma tentativa de conexão de soquete aguarda antes de ser cancelada. Essa propriedade, como o tempo limite de pedido, pode influenciar no tempo em que um cliente precisa para efetuar failover se ocorrer uma falha de interrupção de rede. Em geral, configure

essa propriedade para um valor menor do que o valor do tempo limite de solicitação porque a quantia de tempo para estabelecer conexões é relativamente constante.

Tempo Limite de Fragmento

Nome da Propriedade: com.ibm.CORBA.FragmentTimeout

Valor válido: Valor de número inteiro para o número de segundos.

Valor sugerido : 30

Onde especificar: arquivo `orb.properties`

Descrição: Indica quantos segundos uma solicitação de fragmento aguarda antes de ser cancelada. Essa propriedade é semelhante à propriedade de tempo limite de pedido.

Configurações do Conjunto de Encadeamentos

Essas propriedades restringem o tamanho do conjunto de encadeamentos a um número específico de encadeamentos. Os encadeamentos são usados pelo ORB para distribuir os pedidos do servidor depois de serem recebidos no soquete. Configurar esses valores da propriedade muito baixo resulta em um aumento de profundidade da fila de soquete e possivelmente em tempos limites.

Multiplicidade de Conexão

Nome da Propriedade: com.ibm.CORBA.ConnectionMultiplicity

Valor válido: Valor de número inteiro para número de conexões entre o cliente e o servidor. O valor padrão é 1. Configurar um valor maior define uma multiplicidade entre várias conexões.

Valor sugerido : 1

Onde especificar: arquivo `orb.properties`**Descrição:** Permite que o ORB use várias conexões em qualquer servidor. Na teoria, configurar esse valor promove paralelismo sobre as conexões. Na prática, o desempenho não é beneficiado pela configuração da multiplicidade de conexão. Não configure esse parâmetro.

Conexões Abertas

Nomes da Propriedade: com.ibm.CORBA.MinOpenConnections, com.ibm.CORBA.MaxOpenConnections

Valor válido: Um valor de número inteiro para número de conexões.

Valor sugerido : 1024

Onde especificar: Console administrativo do WebSphere Application Server**Descrição:** Especifica um número mínimo e máximo de conexões abertas. O ORB mantém um cache de conexões que foram estabelecidas com os clientes. Essas conexões são limpas quando este valor for transmitido. A limpeza das conexões pode prejudicar o comportamento na grade de dados.

É Aumentável

Nome da Propriedade: com.ibm.CORBA.ThreadPool.IsGrowable

Valor válido: booleano; configure para `true` ou `false`.

Valor sugerido : `false`

Onde especificar: arquivo `orb.properties`**Descrição:** Se configurado como `true`, o conjunto de encadeamentos que o ORB usa para solicitações recebidas pode crescer além do que o conjunto suporta. Se o tamanho do conjunto for excedido, novos encadeamentos serão criados para manipular o pedido, mas os encadeamentos não serão agrupados. Evite o crescimento do conjunto de encadeamentos ao definir o valor para `false`.

Profundidade da Fila de Soquete do Servidor

Nome da Propriedade: com.ibm.CORBA.ServerSocketQueueDepth

Valor válido: Um valor de número inteiro para número de conexões.

Valor sugerido : `1024`

Onde especificar: arquivo `orb.properties`**Descrição:** Especifica o comprimento da fila para conexões recebidas dos clientes. As filas ORB recebem conexões dos clientes. Se a fila estiver cheia, as conexões serão recusadas. Recusar conexões pode prejudicar o comportamento na grade de dados.

Tamanho do Fragmento

Nome da Propriedade: com.ibm.CORBA.FragmentSize

Valor válido: Um número inteiro que especifica o número de bytes. O padrão é 1024.

Valor sugerido : `0`

Onde especificar: arquivo `orb.properties`**Descrição:** Especifica o tamanho máximo do pacote que o ORB usa ao enviar um pedido. Se um pedido for maior que o limite de tamanho de fragmento, esse pedido será dividido em fragmentos de pedido e enviados, cada um, separadamente e remontados no servidor. Os pedidos de fragmentação são úteis em redes não-confiáveis onde os pacotes podem precisar ser reenviados. No entanto, se a rede for confiável, dividir as solicitações em fragmentos pode causar processamento desnecessário.

Nenhuma Cópia Local

Nome da Propriedade: com.ibm.CORBA.iiop.NoLocalCopies

Valor válido: booleano; configure para `true` ou `false`.

Valor sugerido : `true`

Onde especificar: No console administrativo do WebSphere Application Server, configuração **Transmitir por Referência**. **Descrição:** Especifica se o ORB é transmitido por referência. O ORB usa a chamada transmitir por valor por padrão. A chamada Transmitir por valor causa custos extras de lixo e de serialização para o caminho quando uma interface é iniciada localmente. Ao configurar esse valor para true, o ORB usa um método transmitir por referência que é mais eficiente do que a chamada transmitir por valor.

Nenhum Interceptor Local

Nome da Propriedade: com.ibm.CORBA.NoLocalInterceptors

Valor válido: booleano; configure para `true` ou `false`.

Valor sugerido : `true`

Onde especificar: arquivo `orb.properties` **Descrição:** Especifica se o ORB inicia os interceptores de solicitação mesmo ao fazer solicitações locais

(intraprocesso). Os interceptores que o WebSphere eXtreme Scale usa são para segurança e os identificadores de rota não serão necessários se o pedido for tratado dentro do processo. Os interceptores que estão entre os processos são necessários apenas para as operações de chamada de procedimento remoto (RPC). Ao configurar 'Nenhum interceptor local', é possível evitar o processamento extra ao usar introduções de interceptores locais.

Atenção: Se a segurança do WebSphere eXtreme Scale estiver sendo usada, configure o valor da propriedade com.ibm.CORBA.NoLocalInterceptors para `false`. A infraestrutura de segurança usa interceptores para autenticação.

Ajustando o IBM eXtremeIO (XIO)

É possível usar propriedades de servidor XIO para sintonizar o comportamento do transporte do XIO na grade de dados.

Propriedades de Servidor para Ajuste do XIO

É possível configurar as seguintes propriedades no arquivo de propriedades do servidor:

maxXIONetworkThreads
Configura o número máximo de encadeamentos para alocar no conjunto de encadeamentos de rede de transporte eXtremeIO.

Padrão: `50`

minXIONetworkThreads
Configura o número mínimo de encadeamentos para alocar no conjunto de encadeamentos de rede de transporte eXtremeIO.

Padrão: `50`

maxXIOWorkerThreads
Configura o número máximo de encadeamentos para alocar no conjunto de encadeamentos de processamento de solicitação de transporte eXtremeIO.

Padrão: `128`

minXIOWorkerThreads
Configura o número mínimo de encadeamentos para alocar no conjunto de encadeamentos de processamento de solicitação de transporte eXtremeIO.

Padrão: `128`

8.6+ transporte

Especifica o tipo de transporte a ser utilizado para todos os servidores no domínio do serviço de catálogo. É possível configurar o valor como `XIO` ou `ORB`.

Ao utilizar os comandos **`startOgServer`** ou **`startXsServer`**, não é necessário configurar esta propriedade. O script substitui esta propriedade. No entanto, se você iniciar servidores com outro método, o valor desta propriedade será utilizado.

Esta propriedade se aplica apenas ao serviço de catálogo.

Se você tiver o parâmetro **-transport** no script inicial e a propriedade de servidor **transport** definida em um servidor de catálogos, o valor do parâmetro **-transport** será usado.

8.6+ xioTimeout
Configura o tempo limite para solicitações do servidor que estão utilizando o transporte IBM eXtremeIO (XIO) em segundos. O valor pode ser configurado para qualquer valor maior ou igual a um segundo.

Padrão: 30 segundos

Tarefas relacionadas:

"Configurando o IBM eXtremeIO (XIO)" na página 119
O IBM eXtremeIO (XIO) é um mecanismo de transporte que substitui o Object Request Broker (ORB).

Ajustando as Java virtual machines

Java

Você deve levar em conta vários aspectos específicos do ajuste da Java Virtual Machine (JVM) para melhorar o desempenho do WebSphere eXtreme Scale. Na maioria dos casos, poucas ou nenhuma configuração da JVM é necessária. Se muitos objetos estiverem sendo armazenados na grade de dados, ajuste o tamanho de heap para um nível apropriado a fim de evitar execução sem memória.

IBM eXtremeMemory

Ao configurar o eXtremeMemory, é possível armazenar os objetos na memória nativa em vez de armazenar no heap Java. Configurar o eXtremeMemory ativa o eXtremeIO como um novo mecanismo de transporte. Movendo objetos para fora do heap Java, é possível evitar pausas da coleta de lixo, levando ao desempenho mais constante e tempos de resposta atribuíveis. Para obter informações adicionais, consulte Configurando o IBM eXtremeMemory.

Plataformas Testadas

Os testes de desempenho ocorreram principalmente no AIX (32 vias), Linux (quatro vias) e computadores Windows (oito vias). Com computadores AIX sofisticados, é possível testar fortemente cenários multiencadeados para identificar e corrigir os pontos de contenção.

Coleta de Lixo

O WebSphere eXtreme Scale cria objetos temporários associados a cada transação, como pedido e reposta e sequência de log. Como esses objetos afetam a eficiência da coleta de lixo, o ajuste da coleta de lixo é fundamental.

Todas as JVMs modernas usam algoritmos de coleta de lixo paralela, o que significa que o uso de mais núcleos pode reduzir pausas na coleta de lixo. A coleta de lixo em um servidor físico com oito núcleos é mais rápida do que em um servidor físico com quatro núcleos.

Quando o aplicativo deve gerenciar uma grande quantidade de dados para cada partição, a coleta de lixo pode ser um fator. Na maioria das vezes, um cenário de leitura tem um bom desempenho mesmo com heaps grandes (20 GB ou mais) se um coletor geracional é utilizado. Contudo, depois que o heap de estabilidade é

preenchido, ocorre uma pausa proporcional ao tamanho do heap ativo e ao número de processadores no computador. Essa pausa pode ser maior ou menor em máquinas com grandes heaps.

Máquina Virtual IBM para Coleta de Lixo Java

Para a máquina virtual IBM para Java, use o coletor **optavgpause** para cenários com alta taxa de atualização (100% das entradas de modificação de transações). O coletor **gencon** funciona muito melhor que o coletor **optavgpause** nos cenários em que os dados são atualizados relativamente com pouca frequência (10% do tempo ou menos). Experimente ambos os coletores para ver qual funciona melhor no seu cenário. Executar com a coleta de lixo detalhada ativada para verificar a porcentagem de tempo gasto na coleta de lixo. Ocorreram cenários em que 80% do tempo foi gasto na coleta de lixo até que um que o ajuste resolvesse o problema.

Use o parâmetro **-Xgcpolicy** para alterar o mecanismo de coleta de lixo. O valor do parâmetro **-Xgcpolicy** pode ser configurado como: **-Xgcpolicy:gencon** ou **-Xgcpolicy:optavgpause**, dependendo de qual coletor de lixo você deseja usar.

- Em uma configuração do WebSphere Application Server, configure o parâmetro **-Xgcpolicy** no console administrativo. Clique em **Servidores** > **Servidores de Aplicativos** > **server_name** > **Definição de Processo** > **Java Virtual Machine**. Inclua o parâmetro no campo **Argumentos da JVM Genéricos**.
- Em uma configuração independente, transmita o parâmetro **-jvmArgs** para o script de servidor de início para especificar o coletor de lixo. O parâmetro **-jvmArgs** deve ser o último parâmetro que é transmitido ao script.

Outras Opções de Coleta de Lixo

Atenção: Se você estiver usando um Oracle JVM, podem ser necessários ajustes na coleta de lixo padrão e na política de ajuste.

O WebSphere eXtreme Scale suporta o WebSphere Real Time Java. Com o WebSphere Real Time Java, a resposta de processamento de transação do WebSphere eXtreme Scale é mais consistente e previsível. Como resultado, o impacto da coleta de lixo e do planejamento do encadeamento é enormemente minimizado. O impacto é reduzido ao nível no qual o tempo de desvio de resposta padrão é inferior a 10% da Java regular.

Desempenho da JVM

O WebSphere eXtreme Scale pode ser executado em versões diferentes do Java Platform, Standard Edition. O WebSphere eXtreme Scale suporta Java SE Versão 6. Para produtividade e desempenho do desenvolvedor aprimorados, use o Java SE Versão 6 ou posterior ou Java SE Versão 7 para tirar vantagem de anotações e da coleta de lixo melhorada. O WebSphere eXtreme Scale funciona em Java virtual machines de 32 ou 64 bits.

O WebSphere eXtreme Scale é testado com um subconjunto das máquinas virtuais disponíveis, todavia, a lista suportada não é exclusiva. É possível executar o WebSphere eXtreme Scale em qualquer JVM do fornecedor na Edição 5 ou posterior. No entanto, se ocorrer um problema com uma JVM do fornecedor, você deverá contatar o fornecedor da JVM para obter suporte. Se possível, use a JVM a partir do tempo de execução do WebSphere em qualquer plataforma que o WebSphere Application Server suporta.

Em geral, utilize a versão mais recente disponível do Java Platform, Standard Edition para obter melhor desempenho.

Tamanho de Heap

A recomendação é heaps de 1 a 2 GB com uma JVM para cada quatro núcleos. O número do tamanho de heap ideal depende dos seguintes fatores:

- Quantidade de objetos ativos no heap.
- Complexidade dos objetos ativos no heap.
- Quantidade de núcleos disponíveis para a JVM.

Por exemplo, um aplicativo que armazena matrizes de 10 KB pode executar um heap muito maior do que um aplicativo que usa gráficos complexos de POJOs.

Contagem de Encadeamentos

A contagem de encadeamentos depende de poucos fatores. Há um limite de quantos encadeamentos um único shard pode gerenciar. Um shard é uma instância de uma partição e pode ser primário ou de réplica. Com mais shards para cada JVM, você possui mais encadeamentos com cada shard adicional fornecendo mais caminhos simultâneos para os dados. Embora cada shard é simultâneo o máximo possível, essa simultaneidade ainda é limitada.

Requisitos do Object Request Broker (ORB)

O IBM SDK inclui uma implementação IBM ORB que foi testada com o WebSphere Application Server e o WebSphere eXtreme Scale. Para facilitar o processo de suporte, use um JVM fornecido pela IBM. Outras implementações de JVM utilizam um ORB diferente. O IBM ORB é fornecido apenas com Java virtual machines fornecidas pela IBM. O WebSphere eXtreme Scale requer um ORB em funcionamento para operar. O WebSphere eXtreme Scale pode ser usado com ORBs a partir de outros fornecedores. No entanto, se você tiver um problema com um ORB do fornecedor, você deve entrar em contato com o fornecedor do ORB para obter suporte. A implementação do IBM ORB é compatível com Java virtual machines de terceiros e pode ser substituído, se necessário.

Ajuste de orb.properties

No laboratório, o seguinte arquivo foi usado nas grades de dados de até 1500 JVMs. O arquivo `orb.properties` está na pasta `lib` do ambiente de tempo de execução.

```
# IBM JDK properties for ORB
org.omg.CORBA.ORBClass=com.ibm.CORBA.iiop.ORB
org.omg.CORBA.ORBSingletonClass=com.ibm.rmi.corba.ORBSingleton

# WS Interceptors
org.omg.PortableInterceptor.ORBInitializerClass.com.ibm.ws.objectgrid.corba.ObjectGridInitializer

# WS ORB & Plugins properties
com.ibm.CORBA.ForceTunnel=never
com.ibm.CORBA.RequestTimeout=10
com.ibm.CORBA.ConnectTimeout=10

# Needed when lots of JVMs connect to the catalog at the same time
com.ibm.CORBA.ServerSocketQueueDepth=2048

# Clients and the catalog server can have sockets open to all JVMs
com.ibm.CORBA.MaxOpenConnections=1016

# Thread Pool for handling incoming requests, 200 threads here
com.ibm.CORBA.ThreadPool.IsGrowable=false
com.ibm.CORBA.ThreadPool.MaximumSize=200
com.ibm.CORBA.ThreadPool.MinimumSize=200
```

```
com.ibm.CORBA.ThreadPool.InactivityTimeout=180000

# No splitting up large requests/responses in to smaller chunks
com.ibm.CORBA.FragmentSize=0
```

Referências relacionadas:

Script **startOgServer** (ORB)
(Descontinuado) O script **startOgServer** inicia servidores de contêiner e de catálogos que usam o mecanismo de transporte do Object Request Broker (ORB). É possível utilizar uma variedade de parâmetros quando você inicia seu servidores para ativar o rastreio, especificar números de porta e assim por diante.

Informações relacionadas:

Ajustando a Máquina Virtual IBM para Java

Ajustando a Configuração do Intervalo de Pulsação para Detecção de Failover

É possível configurar a quantidade de tempo entre verificações do sistema para servidores com falha com a configuração do intervalo de pulsação. Esta configuração se aplica apenas aos servidores de catálogos.

Sobre Esta Tarefa

A configuração de failover varia dependendo do tipo de ambiente que você está usando. Se você estiver utilizando um ambiente independente, é possível configurar o failover com a linha de comandos. Se você estiver usando um ambiente do WebSphere Application Server Network Deployment, é necessário configurar o failover no console administrativo do WebSphere Application Server Network Deployment.

Procedimento

- Configurar o failover para ambientes independentes.

  É possível configurar intervalos de pulsação para o servidor de catálogos usando o parâmetro **-heartbeat** no arquivo de script **startOgServer** ou **startXsServer**. Configure esse parâmetro para um dos seguintes valores:

  Tabela 26. Intervalos de Pulsações

Valor	Ação	Descrição
0	Típica (padrão)	Failovers são tipicamente detectados em 30 segundos.
-1	Agressiva	Failovers são tipicamente detectados em 5 segundos.
1	Moderada	Failovers são tipicamente detectado em 180 segundos.

  Um intervalo de pulsação agressivo pode ser útil quando os processos e a rede estão estáveis. Se a rede ou os processos não são configurados de maneira ideal, as pulsações podem ser perdidas, o que pode resultar em uma falsa detecção de falhas.

- Configurar o failover para ambientes do WebSphere Application Server.

  É possível configurar o WebSphere Application Server Network Deployment Versão 7.0 e posterior para permitir que o WebSphere eXtreme Scale efetue failover muito rapidamente. O tempo de failover padrão para falhas "hard" é de aproximadamente 200 segundos. Uma falha de disco rígido é um travamento de computador ou de um servidor físico, uma desconexão de cabo de rede ou um erro do sistema operacional. As falhas causadas por travamentos de processo ou por falhas de software normalmente executam failover em menos de um segundo. A detecção de falha para falhas "soft" ocorre quando os soquetes de

rede a partir de um processo inativo são fechados automaticamente pelo sistema operacional para o servidor que hospeda o processo.

Configuração de pulsação do grupo principal

O WebSphere eXtreme Scale que executa um processo do WebSphere Application Server herda as características de failover a partir das configurações de grupo principal do servidor de aplicativos. As seguintes seções descrevem como definir as configurações de pulsação do grupo principal para versões diferentes do WebSphere Application Server Network Deployment:

– **Atualize as configurações do grupo principal para o WebSphere Application Server Network Deployment Versão 7.0:**

  O WebSphere Application Server Network Deployment Versão 7.0 fornece duas configurações de grupo principal que podem ser ajustadas para aumentar ou diminuir a detecção de failover:

  - **Período de transmissão de pulsação.** O padrão é 30000 milissegundos.
  - **Período de tempo limite de pulsação.** O padrão é 180000 milissegundos.

  Para obter mais detalhes sobre como alterar essas configurações, consulte o Centro de Informações do WebSphere Application Server Network Deployment: Configurações de Falha e Detecção de Descoberta.

  Use as seguintes configurações para alcançar um tempo de detecção de falha de 1500 milissegundos para os servidores WebSphere Application Server Network Deployment Versão 7:

  - Configure o período de transmissão de pulsação para 750 milissegundos.
  - Configure o tempo limite da pulsação para 1500 milissegundos.

O que Fazer Depois

Quando estas configurações são modificadas para fornecer tempos de failover curtos, há alguns problemas de ajuste de sistema a considerar. Primeiro, Java não é um ambiente em tempo real. É possível que os encadeamentos sejam atrasados se a JVM estiver experimentando longos tempos de coleta de lixo. Os encadeamentos também podem ser atrasados se a máquina que hospeda o JVM estiver sobrecarregada (devido ao próprio JVM ou outros processos que são executados na máquina). Se os encadeamentos forem atrasados, as pulsações talvez não sejam enviadas a tempo. No pior dos casos, elas podem ser atrasadas pelo tempo necessário de failover. Se os encadeamentos forem atrasados, ocorrerão falsas detecções de falhas. O sistema deve ser ativado e dimensionado para garantir que falsas detecções de falhas não aconteçam na produção. O teste de carregamento adequado é a melhor maneira de garantir isto.

Nota: A versão atual do eXtreme Scale suporta o WebSphere Real Time.

Ajustando a Coleta de Lixo com o WebSphere Real Time

O uso do WebSphere eXtreme Scale com WebSphere Real Time aumenta a consistência e a previsibilidade a um custo de rendimento de desempenho em comparação com a política de coleta de lixo padrão empregada no IBM Java™ SE Runtime Environment (JRE) padrão. O custo versus a proposta de benefício pode variar. WebSphere eXtreme Scale cria vários objetos temporários que são associados a cada transação. Esses objetos temporários lidam com pedidos, respostas, sequências de log e sessões. Sem o WebSphere Real Time, o tempo de resposta de transação pode ultrapassar centenas de milissegundos. Entretanto, usar o

WebSphere Real Time com o WebSphere eXtreme Scale pode aumentar a eficiência da coleta de lixo e reduzir o tempo de resposta em 10% do tempo de resposta de configuração independente.

Tarefas relacionadas:

Configurando o Gerenciador de Sessões HTTP para Vários Servidores de Aplicativos
O WebSphere eXtreme Scale é fornecido com uma implementação de gerenciamento de sessões que substitui o gerenciador de sessões padrão para um contêiner da web. Esta implementação fornece replicação de sessão, alta disponibilidade, melhor escalabilidade e opções de configuração. É possível ativar o gerenciador de replicação de sessão do WebSphere eXtreme Scale e a inicialização de contêiner de ObjectGrid integrada genérica.

Configurando o Gerenciador de Sessões HTTP com WebSphere Portal
É possível persistir as sessões HTTP a partir do WebSphere Portal em uma grade de dados.

Configurando o Gerenciador de Sessões HTTP com WebSphere Application Server
Enquanto o WebSphere Application Server fornece a função de gerenciamento de sessões, o desempenho diminui conforme o número de solicitações aumenta. O WebSphere eXtreme Scale vem com uma implementação de gerenciamento de sessões que fornece opções de replicação de sessão, alta disponibilidade, melhor escalabilidade e configuração mais firme.

Configurando o WebSphere eXtreme Scale com o WebSphere Application Server
É possível executar um serviço de catálogo e processos de servidor de contêiner no WebSphere Application Server. O processo para configurar esses servidores é diferente de uma configuração independente. O serviço de catálogo pode ser iniciado automaticamente nos servidores ou gerenciadores de implementação do WebSphere Application Server. O processo do contêiner é iniciado quando um aplicativo eXtreme Scale for implementado e iniciado no ambiente do WebSphere Application Server.

Referências relacionadas:

Script **startOgServer** (ORB)
(Descontinuado) O script **startOgServer** inicia servidores de contêiner e de catálogos que usam o mecanismo de transporte do Object Request Broker (ORB). É possível utilizar uma variedade de parâmetros quando você inicia seu servidores para ativar o rastreio, especificar números de porta e assim por diante.

Informações relacionadas:

Configure o WebSphere Commerce para usar o WebSphere eXtreme Scale para que o cache dinâmico melhore o desempenho e a escala

Integração do WebSphere Business Process Management and Connectivity

Ajustando a Máquina Virtual IBM para Java

WebSphere Real Time em um Ambiente Independente

É possível usar o WebSphere Real Time com o WebSphere eXtreme Scale. Ao ativar o WebSphere Real Time, é possível obter uma coleta de lixo mais previsível com um tempo de resposta e rendimento estável e consistente em um ambiente independente do eXtreme Scale.

Vantagens do WebSphere Real Time

WebSphere eXtreme Scale cria vários objetos temporários que são associados a cada transação. Esses objetos temporários lidam com pedidos, respostas, sequências de log e sessões. Sem o WebSphere Real Time, o tempo de resposta de transação pode

ultrapassar centenas de milissegundos. Entretanto, usar o WebSphere Real Time com o WebSphere eXtreme Scale pode aumentar a eficiência da coleta de lixo e reduzir o tempo de resposta em 10% do tempo de resposta de configuração independente.

Ativando o WebSphere Real Time

Instale o WebSphere Real Time e o WebSphere eXtreme Scale independente nos computadores onde você planeja executar o eXtreme Scale . Configure a variável de ambiente JAVA_HOME para apontar para o Java SE Runtime Environment (JRE) padrão.

Configure a variável de ambiente JAVA_HOME para apontar para o WebSphere Real Time instalado. Em seguida, ative o WebSphere Real Time da seguinte forma.

1. Edite o arquivo de instalação padrão `objectgridRoot/bin/setupCmdLine.sh | .bat` ao remover o comentário da seguinte linha.

   ```
   WXS_REAL_TIME_JAVA="-Xrealtime -Xgcpolicy:metronome
   -Xgc:targetUtilization=80"
   ```

2. Salve o arquivo.

Agora você ativou o WebSphere Real Time. Se desejar desativar o WebSphere Real Time, poderá incluir o comentário de volta para a mesma linha.

Práticas Recomendáveis

WebSphere Real Time permite que transações do eXtreme Scale tenham um tempo de resposta mais previsível. Os resultados mostram que o desvio de um tempo de resposta de uma transação do eXtreme Scale aumenta significativamente com o WebSphere Real Time em comparação com o Java padrão com seu coletor de lixo padrão. A ativação do WebSphere Real Time com o eXtreme Scale é ótima se a estabilidade e o tempo de resposta de seu aplicativo forem essenciais.

As boas práticas descritas nesta seção explicam como tornar o WebSphere eXtreme Scale mais eficiente por meio do ajuste e de práticas de código dependendo de sua carga esperada.

- Configure o nível de uso correto do processador para o aplicativo e coletor de lixo.

  O WebSphere Real Time fornece a capacidade de controlar o uso do processador para que o impacto da coleta de lixo em seu aplicativo seja controlado e minimizado. Use o parâmetro `-Xgc:targetUtilization=NN` para especificar a porcentagem `NN` do processador que é usado pelo aplicativo a cada 20 segundos. O padrão para WebSphere eXtreme Scale é 80%, mas é possível modificar o script no arquivo `objectgridRoot/bin/setupCmdLine.sh` para configurar um número diferente, como `70`, que fornece mais capacidade de processador para o coletor de lixo. Implemente servidores suficientes para manter a carga do processador abaixo de 80% para seus aplicativos.
- Configure um tamanho maior de memória de heap.

  O WebSphere Real Time usa mais memória do que o Java comum, assim, planeje seu WebSphere eXtreme Scale com uma memória de heap e configure o tamanho de heap ao iniciar os servidores de catálogo e os contêineres com o parâmetro `–jvmArgs –XmxNNNM` no comando **ogStartServer**. Por exemplo, é possível usar o parâmetro `–jvmArgs –Xmx500M` para iniciar os servidores de catálogo e usar o tamanho de memória apropriado para iniciar os contêineres. O tamanho de memória pode ser configurado de 60 a 70% do tamanho de dados esperado por

JVM. Se você não configurar esse valor, ocorrerá um erro OutOfMemoryError. Opcionalmente, use o parâmetro `–jvmArgs –Xgc:noSynchronousGCOnOOM` para evitar um comportamento indesejável quando a JVM ficar sem memória.

- Ajuste os encadeamentos para a coleta de lixo.

  O WebSphere eXtreme Scale cria muitos objetos temporários associados a cada transação e encadeamentos Remote Procedure Call (RPC). A coleta de lixo possui benefícios de desempenho se o computador tiver ciclos de processadores suficientes. O número padrão de encadeamentos é 1. É possível alterar o número de encadeamentos com o argumento `–Xgcthreads n`. O valor sugerido para esse argumento é o número de núcleos que estão disponíveis em relação ao número de Java virtual machines por computador.

- Ajuste o desempenho para aplicativos de curta duração com oWebSphere eXtreme Scale.

  O WebSphere Real Time é ajustado para aplicativos de execução longa. Geralmente, é necessário executar transações contínuas do WebSphere eXtreme Scale por duas horas para obter dados de desempenho confiáveis. É possível usar o parâmetro `–Xquickstart` para melhorar o desempenho de aplicativos de curta duração. Esse parâmetro informa ao compilador just-in-time (JIT) para usar um nível menor de otimização.

- Minimize a fila do cliente do WebSphere eXtreme Scale e a retransmissão do cliente do WebSphere eXtreme Scale.

  A principal vantagem de usar o WebSphere eXtreme Scale com o WebSphere Real Time é que o tempo de resposta da transação é altamente confiável, o que normalmente representa várias vezes melhorias na magnitude de ordem no desvio do tempo de resposta da transação. Todos os pedidos do cliente enfileirados e retransmissões de pedido do cliente por meio de outro software afetam o tempo de resposta que está além do controle do WebSphere Real Time e do WebSphere eXtreme Scale. É necessário alterar seus encadeamentos e parâmetros de soquete para manter uma carga estável e leve sem nenhum atraso significativo e diminuição da profundidade da fila.

- Escreva aplicativos WebSphere eXtreme Scale para usar o encadeamento do WebSphere Real Time.

  Sem modificar seu aplicativo, é possível obter tempo de reposta de transação WebSphere eXtreme Scale altamente confiável com diversas melhorias da magnitude de ordem no desvio do tempo de resposta. É possível explorar ainda mais a vantagem do encadeamento de seus aplicativos transacionais a partir do encadeamento Java normal para RealtimeThread o que oferece melhor controle sobre a prioridade de encadeamento e controle de planejamento.

  Seu aplicativo atualmente inclui o código a seguir.

  ```
  public class WXSCacheAppImpl extends Thread implements WXSCacheAppIF
  ```

  É possível substituir opcionalmente este código pelo seguinte.

  ```
  public class WXSCacheAppImpl extends RealtimeThread implements
  WXSCacheAppIF
  ```

WebSphere Real Time no WebSphere Application Server

É possível utilizar o WebSphere® Real Time com eXtreme Scale em um ambiente do WebSphere Application Server Network Deployment versão 7.0. Ao ativar o WebSphere Real Time, é possível obter uma coleta de lixo mais previsível com tempo de resposta e rendimento estáveis e consistentes das transações.

Vantagens

O uso do WebSphere eXtreme Scale com WebSphere Real Time aumenta a consistência e a previsibilidade a um custo de rendimento de desempenho em comparação com a política de coleta de lixo padrão empregada no IBM Java™ SE Runtime Environment (JRE) padrão. O custo versus a proposta de benefício pode variar com base em vários critérios. A seguir estão alguns dos principais critérios:

- Recursos do servidor - Memória disponível, tamanho e velocidade da CPU e velocidade e uso da rede
- Carregamentos do servidor - Carregamento de CPU sustentado, carregamento de CPU de pico
- Configuração Java – Tamanhos de heap, uso de destino, encadeamentos de coleta de lixo
- Configuração do modo de cópia do WebSphere eXtreme Scale - Matriz de byte vs. armazenamento POJO
- Características específicas do aplicativo – Uso de encadeamento, requisitos de resposta e tolerância, tamanho do objeto, entre outras.

Além dessa política de coleta de lixo de metrônomo disponível no WebSphere Real Time, existem políticas de coleta de lixo opcionais disponíveis no IBM Java™ SE Runtime Environment (JRE) padrão. Essas políticas, optthruput (padrão), gencon, optavgpause e subpool são projetadas especificamente para solucionar ambientes e requisitos de aplicativo diferentes. Para obter mais informações sobre essas políticas, consulte “Ajustando as Java virtual machines” na página 715. Dependendo dos requisitos, recursos e restrições do aplicativo e do ambiente, a criação de um protótipo de uma ou mais dessas políticas de coleta de lixo pode garantir que você atenda aos seus requisitos e determine a política ideal.

Recursos com o WebSphere Application Server Network Deployment

1. A seguir estão algumas versões suportadas.
   - WebSphere Application Server Network Deployment versão 7.0.0.5 e acima.
   - WebSphere Real Time V2 SR2 para Linux e acima. Consulte IBM WebSphere Real Time V2 para Linux para obter mais informações.
   - WebSphere eXtreme Scale versão 7.0.0.0 e acima.
   - Sistemas operacionais Linux de 32 e 64 bits.
2. Servidores WebSphere eXtreme Scale não podem ser colocados junto com um WebSphere Application Server DMgr.
3. Real Time não suporta DMgr.
4. Real Time não suporta WebSphere Node Agents.

Ativando o WebSphere Real Time

Instale o WebSphere Real Time e o WebSphere eXtreme Scale nos computadores nos quais você pretende executar o eXtreme Scale. Atualize o WebSphere Real Time Java para SR2.

É possível especificar as configurações de JVM para cada servidor por meio do console do WebSphere Application Server versão 7.0 da seguinte forma.

Escolha **Servidores** > **Tipos de Servidor** > **WebSphere Application Servers** > **<servidor instalado necessário>**

Na página resultante, escolha "Definição de Processo".

Na próxima página, clique em Java Virtual Machine na parte superior da coluna à direita. (Aqui é possível configurar tamanhos de heap, coleta de lixo e outros sinalizadores para cada servidor.)

Configure os seguintes sinalizadores no campo "Argumentos de JVM Genéricos":

```
-Xrealtime -Xgcpolicy:metronome
-Xnocompressedrefs -Xgc:targetUtilization=80
```

Aplique e salve as mudanças.

Para utilizar o Real Time no WebSphere Application Server 7.0 com servidores eXtreme Scale, incluindo os sinalizadores JVM acima, você deverá criar a variável de ambiente JAVA_HOME.

Configure JAVA_HOME da seguinte forma.

1. Expanda "Ambiente".
2. Selecione "Variáveis do WebSphere".
3. Certifique-se de "Todos os Escopos" esteja marcado em “Mostrar Escopo".
4. Selecione o servidor necessário na lista suspensa. (Não selecione DMgr ou servidores de agente do nó.)
5. Se a variável de ambiente JAVA_HOME não estiver listada, selecione "Novo" e especifique JAVA_HOME para o nome da variável. No campo "Valor", insira o nome do caminho completo para o Real Time.
6. Aplique e salve suas mudanças.

Práticas Recomendáveis

Para um conjunto de boas práticas, consulte a seção de boas práticas em “Ajustando a Coleta de Lixo com o WebSphere Real Time” na página 719. Existem algumas modificações importantes que devem ser observadas nesta lista de boas práticas para um ambiente WebSphere eXtreme Scale independente durante a implementação em um ambiente WebSphere Application Server Network Deployment.

Você deve colocar todos os parâmetros da linha de comandos adicionais da JVM no mesmo local que os parâmetros da política de coleta de lixo especificados na seção anterior.

Um destino inicial aceitável para carregamentos do processador sustentados é 50% com carregamentos de pico de duração curta atingindo até 75%. Além disso, você deve incluir capacidade adicional antes de ver a degradação mensurável na previsibilidade e consistência. É possível aumentar um pouco o desempenho se você puder tolerar tempos de resposta mais longos. Se você exceder 80% do limite, isso pode levar à degradação significativa da consistência e da previsibilidade.

Ajustando o Agente de Dimensionamento de Cache para Estimativas Exatas de Consumo de Memória

O WebSphere eXtreme Scale suporta o dimensionamento do consumo de memória das instâncias BackingMap em grades de dados distribuídas. O dimensionamento do consumo de memória não é suportado para instâncias de grades de dados locais. O valor relatado por WebSphere eXtreme Scale para um determinado mapa

é muito próximo do valor relatado pela análise de dump do heap. Se o objeto do mapa for complexo, os dimensionamentos poderão ser menos precisos. A mensagem CWOBJ4543 é exibida no log para qualquer objeto de entrada de cache que não pode ser dimensionada com exatidão porque ela é excessivamente complexa. É possível obter medidas mais precisas para evitar uma complexidade desnecessária no mapa.

Procedimento

- Ative o agente de dimensionamento.

  Se estiver usando uma Java virtual machine Java 5 ou superior, use o agente de dimensionamento. Com o agente de dimensionamento, o WebSphere eXtreme Scale pode obter informações adicionais a partir da JVM para melhorar suas estimativas. O agente pode ser carregado incluindo o seguinte argumento na linha de comandos JVM:

  ```
  -javaagent:WXS lib directory/wxssizeagent.jar
  ```

  Para uma topologia integrada, inclua o argumento na linha de comandos do processo do WebSphere Application Server.

  Para uma topologia distribuída, inclua o argumento na linha de comandos dos processos (contêineres) do eXtreme Scale e do processo do WebSphere Application Server.

  Quando carregada corretamente, a seguinte mensagem é gravada no arquivo `SystemOut.log`.

  ```
  CWOBJ4541I: O dimensionamento de memória de BackingMap aprimorado está ativado.
  ```

- Prefira os tipos de dados Java no lugar de tipos de dados customizados, onde possível.

  O WebSphere eXtreme Scale pode dimensionar com exatidão o custo de memória dos seguintes tipos:

  – java.lang.String e matrizes em que String é a classe do componente (String[])
  – Todos os tipos de wrapper primitivos (Byte, Short, Character, Boolean, Long, Double, Float, Integer) e matrizes em que os wrappers primitivos são o tipo de componente (por exemplo, Integer[], Character[])
  – java.math.BigDecimal e java.math.BigInteger e matrizes em que essas duas classes são o tipo de componente (BigInteger[] e BigDecimal[])
  – Tipos temporais (java.util.Date, java.sql.Date, java.util.Time, java.sql.Timestamp)
  – java.util.Calendar e java.util.GregorianCalendar

- Evite a internação do objeto, quando possível.

  Quando um objeto é inserido em um mapa, o WebSphere eXtreme Scale assume que ele possui referência apenas ao objeto e todos os objetos a todos os objetos aos quais ele referecia diretamente. Se inserir 1000 Objetos customizados em um mapa e cada um tiver uma referência à mesma instância da sequência, o WebSphere eXtreme Scale dimensionará esse instância da sequência em 1.000 vezes, superestimando o tamanho real do mapa no heap. No entanto, o WebSphere eXtreme Scale compensa corretamente para os seguintes cenários de internação comuns:

  – Referências a Enumerações de Java 5
  – Referências a Classes que seguem o Padrão de Enumeração Typesafe. As classes que seguem este padrão possuem apenas construtores privados definidos, possuem pelo menos um campo final estático privado de seu próprio tipo e, se Serializável for implementado, a classe implementará o método readResolve().

– Internação de wrapper Primitivo Java 5. Por exemplo, use Integer.valueOf(1) em vez do novo Integer(1)

Se você tiver que usar a internação, use uma das técnicas anteriores para obter estimativas mais exatas.

- Use tipos customizados com atenção.

  Ao usar tipos customizados, prefira tipos de dados primitivos para campos vs tipos de Objeto.

  Além disso, prefira os tipos de Objeto listados na entrada 2 no lugar de suas próprias implementações customizadas.

  Ao usar tipos customizados, mantenha a árvore de Objeto para um nível. Ao inserir um Objeto customizado em um mapa, o WebSphere eXtreme Scale calculará apenas o custo do Objeto inserido, que inclui os campos primitivos e todos os Objetos aos quais ele faz referência diretamente. O WebSphere eXtreme Scale não seguirá referências adicionais na árvore de Objeto. Se inserir um Objeto no mapa e o WebSphere eXtreme Scale detectar referências que não foram seguidas durante o processo de dimensionamento, uma mensagem codificada CWOBJ4543, que inclui o nome da Classe que não pôde ser totalmente dimensionada, é exibida. Quando esse erro ocorrer, trate as estatísticas de tamanho no mapa como dados de tendência, em vez de confiar nas estatísticas de dimensionamento como sendo totalmente exatas.

- Use o modo de cópia CopyMode.COPY_TO_BYTES, se possível.

  Use o modo de cópia de CopyMode.COPY_TO_BYTES para remover qualquer dúvida sobre como dimensionar os Objetos de valor que estão sendo inseridos no mapa, mesmo quando uma árvore de Objeto tiver muitos níveis para serem dimensionados normalmente (resultando na mensagem CWOBJ4543).

Conceitos relacionados:

"Dimensionamento do Consumo do Cache de Memória"
O WebSphere eXtreme Scale pode estimar precisamente o uso de memória do heap Java de um determinado BackingMap em bytes. Use esse recurso para ajudar a dimensionar corretamente as configurações de heap do Java virtual machine e as políticas de desocupação. O comportamento deste recurso varia com a complexidade dos Objects que estão sendo colocados no mapa de retorno e com a forma como o mapa é configurado. Atualmente, este recurso é suportado apenas para grades de dados distribuídas. As instâncias de grade de dados local não suportam o dimensionamento de bytes usados.

Dimensionamento do Consumo do Cache de Memória

O WebSphere eXtreme Scale pode estimar precisamente o uso de memória do heap Java de um determinado BackingMap em bytes. Use esse recurso para ajudar a dimensionar corretamente as configurações de heap do Java virtual machine e as políticas de desocupação. O comportamento deste recurso varia com a complexidade dos Objects que estão sendo colocados no mapa de retorno e com a forma como o mapa é configurado. Atualmente, este recurso é suportado apenas para grades de dados distribuídas. As instâncias de grade de dados local não suportam o dimensionamento de bytes usados.

Considerações sobre o Consumo de Heap

O eXtreme Scale armazena todos os seus dados dentro do espaço de heap dos processos JVM que compõem a grade de dados. Para um determinado mapa, o espaço de heap que ele consome pode ser dividido nos seguintes componentes:

- O tamanho de todos os objetos principais atualmente no mapa
- O tamanho de todos os objetos de valor atualmente no mapa

- O tamanho de todos os objetos EvictorData que estão em uso pelos plug-ins Evictor no mapa
- A sobrecarga da estrutura de dados subjacente

O número de bytes usados que são relatados pelas estatísticas de dimensionamento é a soma desses quatro componentes. Esses valores são calculados por entrada nas operações de inserção, atualização e remoção de mapa, significando que o mapa eXtreme Scale tem um valor atual para o número de bytes que um determinado mapa de apoio consume.

Quando grades são particionadas, cada partição contém uma parte do mapa de apoio. Como as estatísticas de dimensionamento são calculadas no nível mais baixo do código do eXtreme Scale, cada partição de um mapa de apoio rastreia seu próprio tamanho. É possível usar as APIs de Estatísticas do eXtreme Scale para rastrear o tamanho acumulativo do mapa e também o tamanho de suas partições individuais.

Em geral, use o dimensionamento de dados como uma medida das tendências de dados ao longo do tempo, e não como uma medida exata do espaço de heap usado pelo mapa. Por exemplo, se o tamanho relatado de um mapa dobra de 5 MB para 10 MB, visualize o consumo de memória do mapa como tendo dobrado. A medida real de 10 MB pode ser exata por vários motivos. Se você levar em conta os motivos e seguir as boas práticas, a exatidão das medidas de tamanho se aproximará daquelas do pós-processamento de um dump de heap Java.

O principal problema com a exatidão é que o Modelo de Memória Java não é restritivo o suficiente para permitir medidas de memória que devem ser exatas. O problema fundamental é que um objeto pode estar ativo no heap devido a várias referências. Por exemplo, se a mesma instância de objeto de 5 KB for inserida em três mapas separados, qualquer um desses três mapas impede que o Object seja posto na lixeira. Nesta situação, qualquer uma das medidas a seguir seria justificável:

- O tamanho de cada mapa é aumentado em 5 KB.
- O tamanho do primeiro mapa no qual o Object é posicionado é aumentado em 5 KB.
- O tamanho dos outros dois mapas não é aumentado. O tamanho de cada mapa é aumentado em uma fração do tamanho do objeto.

Esta ambiguidade se deve porque essas medidas devem ser consideradas como dados de tendência, a não ser que você tenha removido a ambiguidade por meio das opções de design, melhores práticas e do entendimento das opções de implementação que podem fornecer estatísticas mais precisas.

O eXtreme Scale supõe que um determinado mapa retém a única referência de vida longa para os Objects de chave e de valor que ele contém. Se o mesmo objeto de 5 KB for posicionado em três mapas, o tamanho de cada mapa será aumentado em 5 KB. O aumento, geralmente, não é um problema, pois o recurso é suportado apenas para grades de dados distribuídas. Se você inserir o mesmo Object em três mapas diferentes em um cliente remoto, cada mapa recebe sua própria cópia do Object. As configurações COPY MODE transacionais padrão também geralmente garantem que cada mapa tenha sua própria cópia de um determinado Object.

Internalização do Object

A internalização de objeto pode provocar um desafio ao estimar ouso de memória do heap. Ao implementar a internalização de um objeto, o código do aplicativo assegura propositalmente que todas as referências a um determinado valor de objeto realmente apontem para a instância do mesmo objeto no heap e, portanto, o mesmo local na memória. Um exemplo disso pode ser a seguinte classe:

```
public class ShippingOrder implements Serializeable,Cloneable{

    public static final STATE_NEW = "new";
    public static final STATE_PROCESSING = "processing";
    public static final STATE_SHIPPED = "shipped";

    private String state;
    private int orderNumber;
private int customerNumber;

public Object clone(){
       ShippingOrder toReturn = new ShippingOrder();
       toReturn.state = this.state;
       toReturn.orderNumber = this.orderNumber;
       toReturn.customerNumber = this.customerNumber;
       return toReturn;
    }

    private void readResolve(){
        if (this.state.equalsIgnoreCase("new")
            this.state = STATE_NEW;
        else if (this.state.equalsIgnoreCase("processing")
            this.state = STATE_PROCESSING;
        else if (this.state.equalsIgnoreCase("shipped")
            this.state = STATE_SHIPPED:
    }
}
```

A internalização do Object causa uma superestimativa ao dimensionar as estatísticas porque o eXtreme Scale supõe que os objetos usam locais de memória diferentes. Se um milhão de objetos ShippingOrder existir, as estatísticas de dimensionamento exibirão o custo de um milhão de Sequências que mantêm as informações de estado. Na realidade, apenas três Sequências existentes são membros estáticos da classe. O custo da memória para os membros estáticos da classe nunca deve ser incluído em nenhum mapa do eXtreme Scale. No entanto, essa situação não pode ser detectada no tempo de execução. Há diversas maneiras pelas quais a internalização de objeto semelhante pode ser implementada, o que explica por que é tão difícil de detectar. Não é prático o eXtreme Scale proteger-se contra todas as implementações possíveis. Entretanto, o eXtreme Scale não protege contra os tipos de internalização de objeto mais normalmente usados. Para otimizar o uso da memória com a internalização de Object, implemente a internalização apenas em objetos personalizados que entram nas duas categorias a seguir para aprimorar a exatidão das estatísticas de consumo de memória:

- O eXtreme Scale é ajustado automaticamente para enumerações do Java 5 e para o padrão Typesafe Enum, conforme descrito em Visão Geral do Java 2 Platform Standard Edition 5.0: Enumerações.
- O eXtreme Scale automaticamente leva em consideração a internalização automática de tipos de wrapper primitivos, como Número Inteiro. A internalização automática para tipos de wrapper primitivos foi introduzida no Java 5 por meio da utilização de métodos estáticos do valueOf.

Estatísticas de Consumo de Memória

Use um dos métodos a seguir para acessar as estatísticas de consumo de memória.

API de Estatísticas

Use o método MapStatsModule.getUsedBytes() que fornece estatísticas para um único mapa, incluindo o número de entradas e a taxa de ocorrências.

Para obter detalhes, consulte Módulos Estatísticos.

Beans Gerenciados (MBeans)

Use a estatística MBean gerenciada pelo MapUsedBytes. É possível usar vários tipos diferentes de Java Management Extensions (JMX) MBeans para administrar e monitorar as implementações. Cada MBean faz referência a uma entidade específica, como um mapa, um eXtreme Scale, um servidor, um grupo de replicação ou um membro do grupo de replicação.

Para obter detalhes, consulte Administrando com Beans Gerenciados (MBeans).

Módulos PMI (Performance Monitoring Infrastructure)

É possível monitorar o desempenho de seus aplicativos com os módulos PMI. Especificamente, use o módulo PMI de mapa para contêineres integrados no WebSphere Application Server.

Para obter detalhes, consulte Módulos PMI.

Console do WebSphere eXtreme Scale

Com o console, é possível visualizar as estatísticas de consumo de memória. Consulte o Monitorando com o Console da Web.

Todos esses métodos acessam a mesma medida subjacente do consumo de memória de uma determinada instância BaseMap. O tempo de execução do WebSphere eXtreme Scale tenta, com o melhor esforço, calcular o número de bytes de memória de heap consumidos pelos objetos de chave e de valor que são armazenados no mapa e também a sobrecarga do próprio mapa. É possível ver quanta memória de heap cada mapa consume entre todas as grades de dados distribuídas.

Na maioria dos casos, o valor relatado por WebSphere eXtreme Scale para um determinado mapa é muito próximo do valor relatado pela análise de dump do heap. O WebSphere eXtreme Scale dimensiona exatamente sua própria sobrecarga, mas não pode considerar cada objeto possível que pode ser posicionado em um mapa. Seguir as melhores práticas descritas no “Ajustando o Agente de Dimensionamento de Cache para Estimativas Exatas de Consumo de Memória” na página 724 pode melhorar a exatidão do tamanho em medidas de bytes fornecidas pelo WebSphere eXtreme Scale.

Tarefas relacionadas:

"Ajustando o Agente de Dimensionamento de Cache para Estimativas Exatas de Consumo de Memória" na página 724
O WebSphere eXtreme Scale suporta o dimensionamento do consumo de memória das instâncias BackingMap em grades de dados distribuídas. O dimensionamento do consumo de memória não é suportado para instâncias de grades de dados locais. O valor relatado por WebSphere eXtreme Scale para um determinado mapa é muito próximo do valor relatado pela análise de dump do heap. Se o objeto do mapa for complexo, os dimensionamentos poderão ser menos precisos. A mensagem CWOBJ4543 é exibida no log para qualquer objeto de entrada de cache que não pode ser dimensionada com exatidão porque ela é excessivamente complexa. É possível obter medidas mais precisas para evitar uma complexidade desnecessária no mapa.

Ajustando o Desempenho para Desenvolvimento de Aplicativos

Para melhorar o desempenho de sua grade de dados em memória ou do espaço de processamento de banco de dados, é possível examinar várias considerações, como o uso das melhores práticas para recursos de produto, como bloqueio, serialização e desempenho de consulta.

Ajustando o Modo de Cópia

O WebSphere eXtreme Scale faz uma cópia do valor com base nas configurações de CopyMode disponíveis. Determine qual configuração funciona melhor para seus requisitos de implementação.

É possível usar o método setCopyMode(CopyMode, valueInterfaceClass) da API BackingMap para configurar o modo de cópia para um dos seguintes campos estáticos finais que estão definidos na classe com.ibm.websphere.objectgrid.CopyMode.

Quando um aplicativo usa a interface ObjectMap para obter uma referência para uma entrada de mapa, use essa referência somente dentro da transação da grade de dados que obteve a referência. O uso da referência em uma transação diferente pode gerar erros. Por exemplo, se você usar a estratégia de bloqueio pessimista para o BackingMap, uma chamada de método get ou getForUpdate adquire um bloqueio S (compartilhado) ou U (atualização), dependendo da transação. O método get retorna a referência ao valor e o bloqueio que foi obtido é liberado quando a transação é concluída. A transação deve chamar o método get ou getForUpdate para bloquear a entrada do mapa em uma transação diferente. Cada transação deve obter sua própria referência para o valor chamando o método get ou getForUpdate em vez de reutilizar a mesma referência de valor em múltiplas transações.

CopyMode para Mapas de Entidade

Ao usar um mapa associado a uma entidade da API EntityManager, o mapa sempre retorna os objetos Tuple da entidade diretamente sem fazer uma cópia, a menos que o modo de cópia COPY_TO_BYTES esteja sendo usado. É importante que o CopyMode seja atualizado ou que a Tupla seja copiada apropriadamente ao fazer alterações.

COPY_ON_READ_AND_COMMIT

O modo COPY_ON_READ_AND_COMMIT é o modo padrão. O argumento valueInterfaceClass é ignorado quando este modo é utilizado. Esse modo assegura que um aplicativo não contém uma referência ao objeto de valor que está no BackingMap. Em vez disso, o aplicativo está sempre trabalhando com uma cópia do valor que está no BackingMap. O modo COPY_ON_READ_AND_COMMIT assegura que o aplicativo nunca possa danificar os dados que estão em cache no BackingMap. Quando uma transação do aplicativo chama um método ObjectMap.get para uma chave especificada e é o primeiro acesso da entrada do ObjectMap para essa chave, será retornada uma cópia do valor. Quando a transação for confirmada, todas as alterações feitas pelo aplicativo são copiadas no BackingMap para assegurar que o aplicativo não tenha uma referência ao valor confirmado no BackingMap.

COPY_ON_READ

O modo COPY_ON_READ aprimora o desempenho no modo COPY_ON_READ_AND_COMMIT, eliminando a cópia que ocorre quando uma transação é confirmada. O argumento valueInterfaceClass é ignorado quando este modo é utilizado. Para preservar a integridade dos dados do BackingMap, o aplicativo assegura que cada referência que ele possui para uma entrada será destruída após a confirmação da transação. Com esse modo, o método ObjectMap.get retorna uma cópia do valor em vez de retornar uma referência ao valor para assegurar que essas alterações feitas pelo aplicativo no valor não afetem o valor de BackingMap até que a transação seja confirmada. No entanto, quando a transação não é confirmada, não é feita uma cópia de alterações. Em vez disso, a referência à cópia que foi retornada pelo método ObjectMap.get é armazenada no BackingMap. O aplicativo destrói todas as referências de entrada do mapa após a confirmação da transação. Se o aplicativo não destruir as referências de entrada do mapa, o aplicativo pode fazer com que os dados em cache no BackingMap sejam danificados. Se um aplicativo estiver utilizando este modo e tiver problemas, vá para o modo COPY_ON_READ_AND_COMMIT para verificar se o problema ainda existe. Se o problema não existir mais, isto indica que o aplicativo está falhando ao destruir todas as suas referências após a confirmação da transação.

COPY_ON_WRITE

O modo COPY_ON_WRITE aprimora o desempenho no modo COPY_ON_READ_AND_COMMIT, eliminando a cópia que ocorre quando o método ObjectMap.get é chamado pela primeira vez por uma transação para uma chave especificada. O método ObjectMap.get retorna um proxy para o valor em vez de uma referência direta ao objeto de valor. O proxy assegura que não seja feita uma cópia do valor, a menos que o aplicativo chame um método set na interface de valor especificada pelo argumento valueInterfaceClass. O proxy fornece uma cópia na implementação de gravação. Quando uma transação é confirmada, o BackingMap examina o proxy para determinar se foi feita alguma cópia como resultado da chamada de um método set. Se tiver sido feita uma cópia, a referência a essa cópia será armazenada no BackingMap. A grande vantagem deste modo é que um valor nunca é copiado durante uma leitura ou em uma confirmação quando a transação nunca chama um método set para alterar o valor.

Os modos COPY_ON_READ_AND_COMMIT e COPY_ON_READ fazem uma cópia detalhada quando um valor é recuperado do ObjectMap. Se um aplicativo atualizar apenas alguns dos valores recuperados em uma transação, este modo não será o ideal. O modo COPY_ON_WRITE suporta este comportamento de maneira

eficiente, mas requer que o aplicativo use um padrão simples. Os objetos de valor devem suportar uma interface. O aplicativo deve usar os métodos nessa interface quando estiver interagindo com o valor em uma sessão. Se este for o caso, os proxies serão criados para os valores retornados ao aplicativo. O proxy possui uma referência ao valor real. Se o aplicativo executa operações de leitura apenas, as operações de leitura sempre executam contra a cópia real. Se o aplicativo modificar um atributo no objeto, o proxy fará uma cópia do objeto real e, em seguida, modificará a cópia. O proxy então utiliza a cópia desse ponto em diante. O uso das cópia permite que a operação de cópia seja completamente evitada para objetos que são apenas de leitura pelo aplicativo. Todas as operações de modificação devem começar com o prefixo configurado. Os Enterprise JavaBeans normalmente são codificados para usarem este estilo de nomenclatura de métodos para métodos que modificam os atributos dos objetos. Esta convenção deve ser seguida. Todos os objetos modificados são copiados no momento em que forem modificados pelo aplicativo. Este cenário de leitura e gravação é o cenário mais eficiente suportado pelo eXtreme Scale. Para configurar um mapa para utilizar o modo COPY_ON_WRITE, utilize o seguinte exemplo: Nesse exemplo, o aplicativo armazena objetos Person que são chaveados utilizando o nome no Mapa. O objeto pessoal é representado no seguinte fragmento de código.

```
class Person {
    String name;
    int age;
    public Person() {
    }
    public void setName(String n)  {
        name = n;
    }
    public String getName() {
        return name;
    }
    public void setAge(int a) {
        age = a;
    }
    public int getAge() {
        return age;
    }
}
```

O aplicativo utiliza apenas a interface IPerson quando interage com valores que são recuperados de um ObjectMap. Modifique o objeto para utilizar uma interface como no exemplo a seguir.

```
interface IPerson
{
    void setName(String n);
    String getName();
    void setAge(int a);
    int getAge();
}
// Modificar Person para implementar a interface IPerson
class Person implements IPerson {
    ...
}
```

O aplicativo precisa então configurar o BackingMap para utilizar modo COPY_ON_WRITE, como no exemplo a seguir:

```
ObjectGrid dg = ...;
BackingMap bm = dg.defineMap("PERSON");
// use COPY_ON_WRITE for this Map with
// IPerson as the valueProxyInfo Class
bm.setCopyMode(CopyMode.COPY_ON_WRITE,IPerson.class);
// The application should then use the following
```

```
// pattern when using the PERSON Map.
Session sess = ...;
ObjectMap person = sess.getMap("PERSON");
...
sess.begin();
// the application casts the returned value to IPerson and not Person
IPerson p = (IPerson)person.get("Billy");
p.setAge( p.getAge() + 1 );
...
// make a new Person and add to Map
Person p1 = new Person();
p1.setName("Bobby");
p1.setAge(12);
person.insert(p1.getName(), p1);
sess.commit();
// the following snippet WON'T WORK. Will result in ClassCastException
sess.begin();
// the mistake here is that Person is used rather than
// IPerson
Person a = (Person)person.get("Bobby");
sess.commit();
```

A primeira seção do aplicativo recupera um valor que foi chamado de `Billy` no mapa. O aplicativo lança o valor retornado para o objeto IPerson, não para o objeto Person porque o proxy retornado implementa duas interfaces:

- A interface especificada na chamada de método BackingMap.setCopyMode
- A interface com.ibm.websphere.objectgrid.ValueProxyInfo

É possível lançar o proxy para dois tipos. A última parte do trecho de código anterior demonstra o que não é permitido no modo COPY_ON_WRITE. O aplicativo recupera o registro do Bobby e tenta converter o registro para um objeto Person. Esta ação falha com uma exceção de lançamento de classe, porque o proxy retornado não é um objeto Person. O proxy retornado implementa o objeto IPerson e ValueProxyInfo.

A interface ValueProxyInfo e o suporte de atualização parcial: Esta interface permite que um aplicativo recupere o valor somente leitura consolidado referenciado pelo proxy ou o conjunto de atributos que foram modificados durante esta transação.

```
public interface ValueProxyInfo {
    List /**/ ibmGetDirtyAttributes();
    Object ibmGetRealValue();
}
```

O método ibmGetRealValue retorna uma cópia de somente leitura do objeto. O aplicativo não deve modificar este valor. O método ibmGetDirtyAttributes retorna uma lista de sequências que representam os atributos que foram modificados pelo aplicativo durante essa transação. O principal caso de uso para o método ibmGetDirtyAttributes está em um Java database connectivity (JDBC) ou um carregador baseado em CMP. Apenas os atributos que estão denominados na lista precisam ser atualizados na instrução SQL ou no objeto mapeado para a tabela. Essa prática leva a um SQL mais eficiente gerado pelo Carregador. Quando uma transação de cópia na gravação é confirmada e se um carregador for conectado, o carregador poderá lançar os valores dos objetos modificados na interface ValueProxyInfo para obter essas informações.

Manipulação do método equals ao usar COPY_ON_WRITE ou proxies: Por exemplo, o código a seguir constrói um objeto Person e, então, o insere em um ObjectMap. Em seguida, ele recupera o mesmo objeto utilizando o método

ObjectMap.get. O valor é lançado para a interface. Se o valor for lançado na interface Person, isto resultará em uma exceção ClassCastException, porque o valor retornado é um proxy que implementa a interface IPerson e não é um objeto Person. A verificação de igualdade falha ao utilizar a operação == porque eles não são o mesmo objeto.

```
session.begin();
// novo objeto Person
Person p = new Person(...);
personMap.insert(p.getName, p);
// recupere-o novamente, lembre-se de utilizar a interface para o lançamento
IPerson p2 = personMap.get(p.getName());
if(p2 == p) {
    // they are the same
} else {
    // they are not
}
```

Outra consideração é quando é necessário substituir o método equals. O método equals deve verificar se o argumento é um objeto que implementa a interface IPerson e lança o argumento para ser um objeto IPerson. Como o argumento pode ser um proxy que implementa a interface IPerson, você deve usar os métodos getAge e getName ao comparar as variáveis da instância por igualdade. Consulte o seguinte exemplo:

```
{
    if ( obj == null ) return false;
    if ( obj instanceof IPerson ) {
        IPerson x = (IPerson) obj;
        return ( age.equals( x.getAge() ) && name.equals( x.getName() ) )
    }
    return false;
}
```

Requisitos de configuração ObjectQuery e HashIndex: Ao usar o COPY_ON_WRITE com os plug-ins ObjectQuery ou HashIndex, você deve configurar o esquema ObjectQuery e o plug-in HashIndex para acessar os objetos usando os métodos de propriedade, que é o padrão. Se você tiver configurado o acesso ao campo, o mecanismo de consulta e o índice tentarão acessar os campos no objeto proxy, o que sempre retorna nulo ou 0 porque a instância do objeto é um proxy.

NO_COPY

O modo NO_COPY permite que um aplicativo obtenha melhorias de desempenho, mas requer que o aplicativo nunca modifique um objeto de valor que seja obtido com o uso de um método ObjectMap.get. O argumento valueInterfaceClass será ignorado quando este modo for usado. Se este modo for utilizado, nunca será feita uma cópia do valor. Se o aplicativo modificar alguma instância do objeto de valor que seja recuperada de ou incluída no ObjectMap, os dados no BackingMap serão corrompidos. O modo NO_COPY é útil, principalmente para mapas de leitura nos quais os dados nunca são modificados pelo aplicativo. Se o aplicativo estiver utilizando este modo e tiver problemas, vá para o modo COPY_ON_READ_AND_COMMIT para verificar se o problema ainda existe. Se o problema não existir mais, isto indica que o aplicativo está modificando o valor retornado pelo método ObjectMap.get, durante ou após a confirmação da transação. Todos os mapas associados às entidades da API EntityManager automaticamente usam este modo, independentemente do que está especificado na configuração do eXtreme Scale.

Todos os mapas associados às entidades da API EntityManager automaticamente usam este modo, independentemente do que está especificado na configuração do eXtreme Scale.

COPY_TO_BYTES

É possível armazenar objetos em um formato serializado em vez do formato POJO. Ao usar a configuração COPY_TO_BYTES, é possível reduzir a área de cobertura da memória que um gráfico grande de objetos pode consumir. Para obter informações adicionais, consulte “Aprimorando o Desempenho com Mapas de Matriz de Byte” na página 736.

Restrição: 8.6+

Ao usar o bloqueio otimista com COPY_TO_BYTES, você pode experienciar exceções ClassNotFoundException durante operações comuns, tal como invalidar entradas de cache. Estas exceções ocorrem porque o mecanismo de bloqueio otimista deve chamar o método "equals(...)" do objeto de cache para detectar quaisquer mudanças antes de a transação ser confirmada. Para chamar o método equals(...), o servidor eXtreme Scale deve poder desserializar o objeto em cache, o que significa que eXtreme Scale deve carregar a classe de objetos.

Para resolver estas exceções, você pode empacotar as classes de objeto em cache para que o servidor eXtreme Scale possa carregar as classes em ambientes independentes. Portanto, você deve colocar as classes no caminho de classe.

Se seu ambiente incluir a estrutura OSGi, empacote as classes em um fragmento do pacote configurável `objectgrid.jar`. Se estiver executando servidores do eXtreme Scale no Perfil do Liberty, empacote as classes como um pacote configurável OSGi e exporte os pacotes Java para essas classes. Em seguida, instale o pacote configurável copiando-o no diretório `grids`.

No WebSphere Application Server, empacote as classes no aplicativo ou em uma biblioteca compartilhada que o aplicativo pode acessar.

Como alternativa, é possível usar serializadores customizados que podem comparar as matrizes de bytes que são armazenadas no eXtreme Scale para detectar quaisquer mudanças.

COPY_TO_BYTES_RAW

Com o modo COPY_TO_BYTES_RAW, é possível acessar diretamente o formulário serializado de seus dados. Este modo de cópia oferece uma maneira eficiente para você interagir com bytes serializados, que permite ignorar o processo de desserialização para acessar objetos na memória.

No arquivo XML descritor do ObjectGrid, é possível configurar o modo de cópia para COPY_TO_BYTES, e configurar programaticamente o modo de cópia para COPY_TO_BYTES_RAW nas instâncias em que você desejar acessar os dados brutos serializados. Configure o modo de cópia COPY_TO_BYTES_RAW no arquivo XML descritor do ObjectGrid apenas quando seu aplicativo usar os dados brutos como parte de um processo de aplicativo principal.

Uso Incorreto do CopyMode

Ocorrem erros quando um aplicativo tenta melhorar o desempenho utilizando o modo de cópia COPY_ON_READ, COPY_ON_WRITE ou NO_COPY, conforme descrito acima. Os erros intermitentes não ocorrem quando você altera o modo de cópia para COPY_ON_READ_AND_COMMIT.

Problema

O problema pode ser devido a dados danificados no mapa do ObjectGrid, que é um resultado de um aplicativo que está violando o contrato de programação do modo de cópia que está sendo utilizado. O dano dos dados pode causar erros imprevisíveis de forma intermitente ou de maneira inexplicada ou inesperada.

Solução

O aplicativo deve estar em conformidade com o contrato de programação estabelecido para o modo de cópia em utilização. Para os modos de cópia COPY_ON_READ e COPY_ON_WRITE, o aplicativo utiliza uma referência a um objeto de valor fora do escopo da transação a partir do qual a referência foi obtida. Para utilizar esses modos, o aplicativo deverá excluir a referência ao objeto de valor depois da conclusão da transação e obter uma nova referência em cada transação que acesse tal objeto. Para o modo de cópia NO_COPY, o aplicativo deve nunca alterar o objeto de valor. Nesse caso, programe o aplicativo de modo que ele não altere o objeto de valor ou configure-o para utilizar um modo de cópia diferente.

Referências relacionadas:

Arquivo XML descritor do ObjectGrid
Para configurar o WebSphere eXtreme Scale, utilize um arquivo XML descritor do ObjectGrid e a API do ObjectGrid.

Aprimorando o Desempenho com Mapas de Matriz de Byte

É possível armazenar os valores em seus mapas em uma matriz de byte em vez do formulário POJO, o que reduz a área de cobertura da memória que um grande gráfico de objetos pode consumir.

Vantagens

A quantidade de memória que é consumida aumenta com o número de objetos em um gráfico de objetos. Ao reduzir um gráfico de objetos complicado a uma matriz de bytes, somente um objeto é mantido na pilha em vez de vários objetos. Com esta redução do número de objetos na pilha, o tempo de execução Java tem menos objetos para procurar durante a coleta de lixo.

O mecanismo de cópia padrão usado pelo WebSphere eXtreme Scale é a serialização, que é dispendiosa. Por exemplo, se o modo de cópia padrão de `COPY_ON_READ_AND_COMMIT` é usado, uma cópia é feita no tempo de leitura e no tempo de obtenção. Em vez de fazer uma cópia no tempo de leitura, com matrizes de byte, o valor é aumentado a partir dos bytes, e em vez de fazer uma cópia no tempo de consolidação, o valor é serializado para bytes. Usar matrizes de byte resulta em consistência de dados equivalentes à configuração padrão com uma redução da memória usada.

Ao usar matrizes de byte, note que ter um mecanismo de serialização otimizado é crítico para ver uma redução do consumo de memória. Para obter mais informações, consulte “Ajustando o Desempenho de Serialização” na página 743.

Configurando Mapas de Matriz de Byte

É possível ativar mapas de matriz de byte com o arquivo XML ObjectGrid modificando o atributo CopyMode que é usado por um mapa para a configuração COPY_TO_BYTES, mostrada no exemplo a seguir:

```
<backingMap name="byteMap" copyMode="COPY_TO_BYTES" />
```

Considerações

Você deve considerar se usará ou não os mapas da matriz de byte em um determinado cenário. Embora seja possível reduzir o uso de memória, o uso do processador aumenta quando você usa matrizes de byte.

A seguinte lista destaca vários fatores que devem ser considerados antes de escolher usar da função do mapa de matriz de byte.

Tipo de Objeto

Comparativamente, a redução de memória pode não ser possível com o uso de mapas de matriz de byte para alguns tipos de objeto. Consequentemente, vários tipos de objetos existem para os quais você não deve usar mapas de matriz de byte. Se você estiver usando qualquer um dos wrappers primitivos Java como valores, ou um POJO que não contenha referências a outros objetos (somente campos primitivos de armazenamento), o número de Objetos Java já é o mais baixo possível–há apenas um. Como a quantidade de memória usada pelo objeto já está otimizada, usar um mapa de matriz de byte para esses tipos de objetos não é recomendado. Os mapas de matriz de byte são mais adequados a tipos de objeto que contenham outros objetos ou coletas de objetos nos quais o número total de objetos POJO seja maior que um.

Por exemplo, se você tiver um objeto Cliente que tenha um Endereço comercial e um Endereço residencial, assim como uma coleta de Pedidos, o número de objetos na heap e o número de bytes usados por esses objetos pode ser reduzido usando-se mapas de matriz de byte.

Acesso local

Ao usar outros modos de cópia, os aplicativos poderão ser otimizados quando as cópias forem feitas, se os objetos forem Clonáveis com o ObjectTransformer padrão ou quando um ObjectTransformer customizado for fornecido com um método copyValue otimizado. Comparado com outros modos de cópia, a cópia de operações de leituras, gravações ou consolidações terá um custo adicional ao acessar os objetos localmente. Por exemplo, se você tiver um cache perto em uma topologia distribuída ou estiver acessando diretamente uma instância ObjectGrid local ou de servidor, o tempo de acesso e de confirmação aumentará com o uso de mapas de matriz de bytes devido ao custo de serialização. Você verá um custo similar em uma topologia distribuída se usar agentes da grade de dados ou acessar o servidor primário ao utilizar o plug-in ObjectGridEventGroup.ShardEvents.

Interações de Plug-in

Com mapas de matriz de byte, os objetos não são aumentados durante a comunicação de um cliente com um servidor a menos que o servidor precise do formulário POJO. Os plug-ins que interagem com o valor do mapa experimentarão uma redução no desempenho devido ao requisito para aumentar o valor.

Qualquer plug-in que use o LogElement.getCacheEntry ou LogElement.getCurrentValue verá esse custo adicional. Se você desejar obter a chave, é possível usar LogElement.getKey, que evita o custo adicional associado com o método LogElement.getCacheEntry().getKey. As seções a seguir discutem os plug-ins sob a perspectiva do uso de matrizes de byte.

Índices e consultas

Quando os objetos são armazenados em formato POJO, o custo de fazer indexação e consulta é mínimo porque o objeto não precisa ser aumentado. Ao usar um mapa de matriz de byte, você terá o custo adicional de aumentar o objeto. Em geral, se o seu aplicativo usar índices ou consultas, é recomendado usar mapas de matriz de byte a menos que você execute somente consultas sobre atributos-chave.

Bloqueio Otimista

Ao usar a estratégia de bloqueio otimista, você terá o custo adicional durante atualizações e operações inválidas. Isso advém da necessidade de aumentar o valor no servidor para obter o valor da versão para fazer verificação de colisão otimista. Se você estiver apenas usando o bloqueio otimista para garantir operações de busca e não precisar de verificação de colisão otimista, é possível usar o com.ibm.websphere.objectgrid.plugins.builtins.NoVersioningOptimisticCallback para desativar a verificação de versão.

Utilitário de carga

Com um Utilitário de Carga, você também terá o custo no tempo de execução do eXtreme Scale de aumentar e reserializar o valor quando ele for usado pelo Utilitário de Carga. Também é possível usar mapas de matriz de byte com Utilitários de Carga, mas considere o custo de fazer alterações no valor em tal cenário. Por exemplo, é possível usar o recurso de matriz de byte no contexto de um cache principalmente de leitura. Neste caso, o benefício de ter menos objetos na heap e menos memória usada excederá o custo incorrido de usar matrizes de byte em operações de inserção e atualização.

ObjectGridEventListener

Ao utilizar o método transactionEnd method no plug-in ObjectGridEventListener, você terá um custo adicional no lado do servidor para pedidos remotos ao acessar um CacheEntry ou o valor atual de LogElement. Se a implementação do método não acessar esses campos, então você não terá o custo adicional.

Referências relacionadas:

Arquivo XML descritor do ObjectGrid
Para configurar o WebSphere eXtreme Scale, utilize um arquivo XML descritor do ObjectGrid e a API do ObjectGrid.

Ajustando Operações de Cópia com a Interface ObjectTransformer

A interface ObjectTransformer utiliza retornos de chamada para o aplicativo para fornecer implementações customizadas de operações comuns e caras, como serialização de objeto e cópias detalhadas em objetos.

 A interface ObjectTransformer foi substituída pelos plug-ins DataSerializer, que podem ser usados para armazenar dados arbitrários eficientemente no

WebSphere eXtreme Scale para que as APIs do produto existentes possam ser interagir de modo eficiente com seus dados.

Visão Geral

As cópias de valores são sempre feitas, exceto quando o modo NO_COPY é usado. O mecanismo de cópia padrão que é empregado no eXtreme Scale é a serialização, que é conhecida como uma operação cara. A interface ObjectTransformer é usada nesta situação. A interface ObjectTransformer usa retornos de chamadas para o aplicativo fornecer uma implementação customizada de operações comuns e caras, como serialização de objetos e cópias detalhadas em objetos.

Um aplicativo pode oferecer uma implementação da interface ObjectTransformer para um mapa, e o eXtreme Scale então delega os métodos neste objeto e confia no aplicativo para oferecer uma versão otimizada de cada método na interface. A interface ObjectTransformer é a seguinte:

```
public interface ObjectTransformer {
    void serializeKey(Object key, ObjectOutputStream stream) throws IOException;
    void serializeValue(Object value, ObjectOutputStream stream) throws IOException;
    Object inflateKey(ObjectInputStream stream) throws IOException, ClassNotFoundException;
    Object inflateValue(ObjectInputStream stream) throws IOException, ClassNotFoundException;
    Object copyValue(Object value);
    Object copyKey(Object key);
}
```

É possível associar uma interface ObjectTransformer com um BackingMap usando o seguinte código de exemplo:

```
ObjectGrid g = ...;
BackingMap bm = g.defineMap("PERSON");
MyObjectTransformer ot = new MyObjectTransformer();
bm.setObjectTransformer(ot);
```

Ajustar Operações de Cópia Detalhada

Depois que um aplicativo receber um objeto de um ObjectMap, o eXtreme Scale executará uma cópia detalhada no valor do objeto para assegurar que a cópia no mapa BaseMap mantenha a integridade dos dados. O aplicativo pode então modificar o valor de objeto de maneira segura. Quando a transação for confirmada, a cópia do valor de objeto no mapa BaseMap será atualizada para o novo valor modificado e o aplicativo parará de utilizar o valor desse ponto em diante. Você poderia ter copiado o objeto novamente na fase de confirmação para fazer uma cópia privada. Entretanto, nesse caso, o custo do desempenho desta ação foi equilibrado ao solicitar que o programador do aplicativo não utilize o valor após a confirmação da transação. O ObjectTransformer padrão tenta utilizar um clone ou um par de serialize e inflate para gerar uma cópia. O par de serialize e inflate é o cenário de desempenho de pior caso. Se o traçado de perfil indicar que serialize e inflate são um problema para seu aplicativo, grave um método de clone apropriado para criar uma cópia detalhada. Se você não conseguir alterar a classe, crie um plug-in ObjectTransformer customizado e implemente mais métodos copyValue e copyKey eficientes.

Ajustando Evictors

Java

Se você utilizar evictores de plug-in, eles não ficarão ativos até você criá-los e associá-los a um mapa de apoio. As boas práticas a seguir aumentarão o desempenho para least frequently used (LFU) e menos utilizado recentemente used (LRU).

Evictor LFU (Least Frequently Used)

O conceito de um evictor LFU é remover entradas do mapa que não são utilizadas frequentemente. As entradas do mapa são distribuídas em uma quantidade de heaps binários configurados. Conforme aumenta o uso de uma determinada entrada de cache, ela ocupa uma posição mais alta no heap. Quando o evictor tenta um conjunto de evicções, ele remove apenas as entradas de cache que estão localizadas abaixo de um ponto específico no heap binário. Por isso, as entradas Least Frequently Used são liberadas.

Evictor LRU (Least Recently Used)

O Evictor LRU segue os mesmos conceitos do Evictor LFU com algumas diferenças. A principal diferença é que o LRU utiliza uma fila PEPS (Primeiro a Entrar, Primeiro a Sair) em vez de um conjunto de heaps binários. Sempre que uma entrada de cache é acessada, ela é movida para o início da fila. Consequentemente, a frente da fila contém as entradas de mapa recentemente mais usadas e, seu final, as entradas de mapa recentemente menos usadas. Por exemplo, a entrada de cache A é utilizada 50 vezes e a entrada de cache B é utilizada apenas uma vez após a entrada de cache A. Neste caso, a entrada de cache B está no início da fila, porque foi utilizada mais recentemente e a entrada de cache A está no final da fila. O evictor LRU libera as entradas de cache que estão no final da fila, que são as entradas do mapa Least Recently Used.

Propriedades LFU e LRU e Boas Práticas para Aprimorar o Desempenho

Número de heaps

Ao utilizar o evictor LFU, todas as entradas de cache para um determinado mapa são ordenadas sobre o número de heaps especificado, aprimorando o desempenho significativamente e impedindo que todas as evicções sejam sincronizadas em um heap binário que contenha todas as ordenações para o mapa. Uma maior quantidade de heaps também acelera o tempo requerido para reordenação dos heaps, porque cada heap tem menos entradas. Configure o número de heaps como 10% do número de entradas em seu BaseMap.

Número de filas

Ao utilizar o evictor LFU, todas as entradas de cache para um determinado mapa são ordenadas sobre o número de filas LRU especificado, aprimorando o desempenho significativamente e impedindo que todas as evicções sejam sincronizadas em uma fila que contenha todas as ordenações para o mapa. Configure o número de filas como 10% do número de entradas em seu BaseMap.

Propriedade MaxSize

Quando um evictor LFU ou LRU começa a liberar entradas, ele utiliza a propriedade do evictor MaxSize para determinar quantos heaps binários ou elementos de fila LRU serão liberados. Por exemplo, suponha que você tenha configurado o número de heaps ou filas para ter aproximadamente 10 entradas do mapa em cada fila do mapa. Se sua propriedade MaxSize estiver configurada como 7, o evictor liberará 3 entradas de cada heap ou objeto de fila para retornar o tamanho de cada heap ou fila para abaixo de 7. O evictor libera apenas entradas do mapa de um heap ou fila quando esse heap ou fila tiver mais do que o valor da propriedade MaxSize de elementos contidos nele. Configure MaxSize como 70% do

tamanho de heap ou de fila. Para este exemplo, o valor é configurado como 7. É possível obter um tamanho aproximado de cada heap ou fila, dividindo o número de entradas BaseMap pelo número de heaps ou filas utilizadas.

Propriedade SleepTime

Um evictor não remove constantemente entradas de seu mapa. Ao invés disso, ele está inativo para uma quantidade de tempo configurada, verificando o mapa apenas a cada n segundos, em que n faz referência à propriedade SleepTime. Esta propriedade também afeta de forma positiva o desempenho: a execução muito frequente de uma limpeza por evicção reduz o desempenho devido aos recursos necessários para esse processamento. Porém, não usar o evictor frequentemente pode resultar em um mapa que tem três entradas que não são necessárias. Um mapa completo de entradas desnecessárias pode afetar negativamente os requisitos de memória e os recursos de processamento requeridos para seu mapa. A configuração de limpezas por despejo como quinze segundos é uma boa prática para a maioria dos mapas. Se houver gravações frequentes no mapa e ele for utilizado em uma alta taxa de transações, considere a configuração do valor com um tempo inferior. No entanto, se o mapa for acessado com pouca frequência, será possível configurar o tempo com um valor superior.

Exemplo

O exemplo a seguir define um mapa, cria um novo evictor LFU, configura as propriedades do evictor e configura o mapa para utilizar o evictor:

```
//Utilizar ObjectGridManager para criar/obter o ObjectGrid. Refer to
// a seção do ObjectGridManger
ObjectGrid objGrid = ObjectGridManager.create.....
BackingMap bMap = objGrid.defineMap("SomeMap");

//Configurar propriedades assumindo 50.000 entradas do mapa
LFUEvictor someEvictor = new LFUEvictor();
someEvictor.setNumberOfHeaps(5000);
someEvictor.setMaxSize(7);
someEvictor.setSleepTime(15);
bMap.setEvictor(someEvictor);
```

A utilização do evictor LRU é muito semelhante à utilização de um evictor LFU. Este é um exemplo:

```
ObjectGrid objGrid = new ObjectGrid;
BackingMap bMap = objGrid.defineMap("SomeMap");

//Configurar propriedades assumindo 50.000 entradas do mapa
LRUEvictor someEvictor = new LRUEvictor();
someEvictor.setNumberOfLRUQueues(5000);
someEvictor.setMaxSize(7);
someEvictor.setSleepTime(15);
bMap.setEvictor(someEvictor);
```

Notice that only two lines are different from the LFUEvictor example.

Tarefas relacionadas:

Java Ativando Evictors Programaticamente
Os evictors estão associados às instâncias do BackingMap.

Java Configurando Evictores com Arquivos XML
Além de configurar programaticamente um evictor de tempo de vida (TTL) com a interface BackingMap, é possível utilizar um arquivo XML para configurar um evictor em cada instância de BackingMap.

Referências relacionadas:

Java Arquivo XML descritor do ObjectGrid
Para configurar o WebSphere eXtreme Scale, utilize um arquivo XML descritor do ObjectGrid e a API do ObjectGrid.

Ajustando o Desempenho de Bloqueio

Estratégias de bloqueio e configurações de isolamento de transação afetam o desempenho dos seus aplicativos.

Recuperar uma Instância Armazenada em Cache

Para obter mais informações, consulte “Gerenciador de Bloqueio” na página 472:

Estratégia de Bloqueio Pessimista

Utilize a estratégia de bloqueio pessimista para operações de leitura e gravação de mapas em que, normalmente, ocorrem conflitos de chaves. A estratégia de bloqueio pessimista tem o maior impacto no desempenho.

Isolamento de Transação de Leitura Committed e Uncommitted

Ao usar a estratégia de bloqueio pessimista, consulte o nível de isolamento de transação usando o método Session.setTransactionIsolation. Para o isolamento de leitura confirmada e de leitura não-confirmada, use os argumentos Session.TRANSACTION_READ_COMMITTED ou Session.TRANSACTION_READ_UNCOMMITTED dependendo do isolamento. Para reconfigurar o nível de isolamento de transação para o comportamento de bloqueio pessimista padrão, use o método Session.setTransactionIsolation com o argumento Session.REPEATABLE_READ.

O isolamento de leitura committed reduz a duração dos bloqueios compartilhados, o que pode melhorar a simultaneidade e reduzir a chance de conflitos. Este nível de isolamento deve ser utilizado quando uma transação não precisa de garantias de que os valores de leitura permanecerão inalterados ao longo da duração da transação.

Utilize uma leitura não-confirmada quando a transação não precisa visualizar os dados confirmados.

Estratégia de Bloqueio Otimista

O bloqueio otimista é a configuração padrão. Tal estratégia melhora o desempenho e a escabilidade quando comparada com a estratégia pessimista. Utilize-a quando seus aplicativos tolerarem algumas falhas de atualização otimista e o desempenho ainda mostrar-se melhor do que com a estratégia pessimista. Essa estratégia é excelente para operações de leitura e aplicativos cuja atualização não ocorre com frequência.

Plug-in OptimisticCallback

A estratégia de bloqueio optimistic faz uma cópia das entradas de cache e as compara, conforme necessário. Esta operação pode ser custosa porque a cópia da entrada pode envolver clonagem ou serialização. Para implementar o desempenho mais rápido possível, implemente o plug-in customizado para os mapas de não entidade.

Consulte “Plug-ins para Versão e Comparação de Objetos de Cache” na página 555 para obter informações adicionais.

Utilize Campos de Versão para Entidades

Quando você está utilizando o bloqueio optimistic com entidades, utilize a anotação @Version ou o atributo equivalente no arquivo descritor dos metadados da Entidade. A anotação da versão fornece ao ObjectGrid uma maneira muito eficiente de controlar a versão de um objeto. Se a entidade não possui um campo de versão e bloqueio optimistic é utilizado para a entidade, então, a entidade inteira deve ser copiada e comparada.

Estratégia de Bloqueio None

Não utilize nenhuma estratégia de bloqueio para aplicativos de somente leitura. A estratégia de bloqueio none não obtém nenhum bloqueio nem utilizar um gerenciador de bloqueios. Portanto, essa estratégia oferece maior simultaneidade, desempenho e escalabilidade.

Ajustando o Desempenho de Serialização

WebSphere eXtreme Scale utiliza vários processos Java para conter dados. Esses processos serializam os dados: ou seja, convertem os dados (que estão no formato de instâncias de objeto Java) em bytes e volta em objetos novamente, conforme necessário, para mover os dados entre processos do cliente e do servidor. Serializar os dados é a operação mais dispendiosa e deve ser endereçada pelo desenvolvedor de aplicativos ao projetar o esquema, configurar a grade de dados e interagir com as APIs de acesso a dados.

As rotinas de cópia e serialização Java são relativamente lentas e podem consumir de 60% a 70% do processador em uma configuração típica. As seções a seguir são escolhas para melhorar o desempenho da serialização.

 A interface ObjectTransformer foi substituída pelos plug-ins DataSerializer, que podem ser usados para armazenar dados arbitrários eficientemente no WebSphere eXtreme Scale para que as APIs do produto existentes possam ser interagir de modo eficiente com seus dados.

Gravação em um ObjectTransformer para cada BackingMap

Um ObjectTransformer pode ser associado a um BackingMap. O aplicativo pode ter uma classe que implementa a interface ObjectTransformer e fornece implementações para as seguintes operações:

- Copiando valores
- Serializando e aumentando chaves para e de fluxos
- Serializando e aumentando valores para e de fluxos

O aplicativo não precisa copiar chaves, porque elas são consideradas imutáveis.

Nota: O ObjectTransformer é chamado apenas quando o ObjectGrid conhece os dados que estão sendo transformados. Por exemplo, quando agentes de API do DataGrid são utilizados, os próprios agentes bem como os dados da instância do agente ou dados retornados do agente devem ser otimizados utilizando técnicas de serialização customizadas. O ObjectTransformer não é chamado para os agentes de API do DataGrid.

Usando Entidades

Ao utilizar a API do EntityManager com entidades, o ObjectGrid não armazena os objetos de entidade diretamente nos BackingMaps. A API do EntityManager converte o objeto de entidade em objetos de Tupla. Os mapas de entidade são automaticamente associados com um ObjectTransformer altamente otimizado. Sempre que a API do ObjectMap ou a API do EntityManager for utilizada para interagir com mapas de entidade, o ObjectTransformer da entidade será chamado.

Serialização Customizada

Há alguns casos em que os objetos devem ser modificados para usar a serialização customizada, tais como implementar a interface java.io.Externalizable ou implementar os métodos writeObject e readObject para classes implementando a interface java.io.Serializable. As técnicas de serialização customizadas devem ser empregadas quando os objetos são serializados utilizando mecanismos que não os métodos da API do ObjectGrid ou da API do EntityManager.

Por exemplo, quando objetos ou entidades são armazenados como dados da instância em um agente da API do DataGrid ou o agente retorna objetos ou entidades, tais objetos não são transformados utilizando um ObjectTransformer. O agente, entretanto, utilizará automaticamente o ObjectTransformer ao utilizar a interface `EntityMixin`. Consulte Agentes do DataGrid e Mapas Baseados em Entidade para obter mais detalhes.

Matrizes de Byte

Ao usar as APIs ObjectMap ou DataGrid, os objetos de valor e chave são serializados sempre que os clientes interagem com a grade de dados e quando os objetos são replicados. Para evitar o gasto adicional de serialização, use matrizes de byte em vez de objetos Java. As matrizes de byte são muito mais baratas para armazenar em memória porque o JDK tem menos objetos para buscar durante a coleta de lixo e elas podem ser aumentadas somente quando necessário. As matrizes de byte somente devem ser usadas se você não precisar acessar os objetos usando consultas ou índices. Como os dados são armazenados como bytes, os dados somente podem ser acessados através de sua chave.

O WebSphere eXtreme Scale pode armazenar dados automaticamente como matrizes de bytes usando a opção de configuração de mapa CopyMode.COPY_TO_BYTES, ou ele pode ser manipulado manualmente pelo cliente. Esta opção armazenará os dados de maneira eficiente na memória e também pode aumentar automaticamente os objetos dentro da matriz de bytes para uso por consulta e índices sob demanda.

Um plug-in MapSerializerPlugin pode ser associado a um plug-in BackingMap quando usar os modos de cópia COPY_TO_BYTES ou COPY_TO_BYTES_RAW. Esta associação permite que os dados sejam armazenados em formato serializado

na memória, em vez de em formato de objeto Java nativo. Armazenando dados serializados preserva a memória e aprimora a replicação e o desempenho no cliente e no servidor. É possível usar um plug-in DataSerializer para desenvolver fluxos de serialização de alto desempenho que podem ser compactados, criptografados e consultados.

Ajustando a Serialização

Os plug-ins DataSerializer expõem os metadados que informa ao WebSphere eXtreme Scale quais atributos ele pode e não pode usar diretamente durante a serialização, o caminho para os dados que serão serializados e o tipo de dados que é armazenado na memória. É possível otimizar a serialização do objeto e o desempenho de desserialização a fim de interagir com eficiência com a matriz de bytes.

Visão Geral

 A interface ObjectTransformer foi substituída pelos plug-ins DataSerializer, que podem ser usados para armazenar dados arbitrários eficientemente no WebSphere eXtreme Scale para que as APIs do produto existentes possam ser interagir de modo eficiente com seus dados.

As cópias de valores são sempre feitas, exceto quando o modo NO_COPY é usado. O mecanismo de cópia padrão que é empregado no eXtreme Scale é a serialização, que é conhecida como uma operação cara. A interface ObjectTransformer é usada nesta situação. A interface ObjectTransformer usa retornos de chamadas para o aplicativo fornecer uma implementação customizada de operações comuns e caras, como serialização de objetos e cópias detalhadas em objetos. No entanto, para obter melhor desempenho na maioria dos casos, é possível usar os plug-ins DataSerializer para serializar os objetos. Você deve usar os modos de cópia COPY_TO_BYTES ou COPY_TO_BYTES_RAW para explorar os plug-ins DataSerializer. Para obter informações adicionais, consulte Serialização Usando os Plug-ins DataSerializer.

Um aplicativo pode oferecer uma implementação da interface ObjectTransformer para um mapa, e o eXtreme Scale então delega os métodos neste objeto e confia no aplicativo para oferecer uma versão otimizada de cada método na interface. A interface ObjectTransformer é a seguinte:

```
public interface ObjectTransformer {
    void serializeKey(Object key, ObjectOutputStream stream) throws IOException;
    void serializeValue(Object value, ObjectOutputStream stream) throws IOException;
    Object inflateKey(ObjectInputStream stream) throws IOException, ClassNotFoundException;
    Object inflateValue(ObjectInputStream stream) throws IOException, ClassNotFoundException;
    Object copyValue(Object value);
    Object copyKey(Object key);
}
```

É possível associar uma interface ObjectTransformer com um BackingMap usando o seguinte código de exemplo:

```
ObjectGrid g = ...;
BackingMap bm = g.defineMap("PERSON");
MyObjectTransformer ot = new MyObjectTransformer();
bm.setObjectTransformer(ot);
```

Ajustar a Serialização e Aumento de Objetos

A serialização de objeto é normalmente a consideração mais importante de desempenho com o eXtreme Scale, que usa o mecanismo serializável padrão se um plug-in ObjectTransformer não for fornecido pelo aplicativo. Um aplicativo pode

fornecer implementações de readObject e writeObject Serializáveis ou pode fazer os objetos implementarem a interface Externalizable, que é aproximadamente dez vezes mais rápida. Se os objetos no mapa não puderem ser modificados, um aplicativo poderá associar uma interface ObjectTransformer ao ObjectMap. Os métodos serialize e inflate são fornecidos para permitir que o aplicativo forneça código customizado para otimizar estas operações devido ao seu grande impacto no desempenho do sistema. O método serializa o objeto para o fluxo fornecido. O método inflate fornece um fluxo de entrada e espera que o aplicativo crie o objeto, aumente-o utilizando dados do fluxo e retorne o objeto. As implementações dos métodos serialize e inflate devem se espelhar entre si.

Os plug-ins DataSerializer substituem os plug-ins do ObjectTransformer, que são descontinuados. Para serializar os dados da forma mais eficiente, use os plug-ins DataSerializer para melhorar o desempenho na maioria dos casos. Por exemplo, se pretender usar funções, como consulta e a indexação, será possível obter vantagem imediatamente do aprimoramento de desempenho que os plug-ins do DataSerializer geram sem fazer mudanças de configuração ou programáticas para seu código do aplicativo.

Ajustando o Desempenho de Consulta

Java

Para ajustar o desempenho de suas consultas, utilize as técnicas e dicas a seguir.

Utilizando Parâmetros

Quando uma consulta é executada, a cadeia de consultas deve ser analisada e um plano desenvolvido para executar a consulta, o que podem ter um alto custo. O WebSphere eXtreme Scale armazena em cache os planos de consulta pela cadeia de consulta. Visto que o cache tem um tamanho limitado, é importante reutilizar as cadeias de consultas sempre que possível. Utilizar os parâmetros nomeados ou posicionais também ajuda no desempenho, estimulando a reutilização do plano de consulta.

```
Positional Parameter Example  Query q = em.createQuery("select c from
Customer c where c.surname=?1");   q.setParameter(1, "Claus");
```

Utilizando Índices

A indexação adequada em um mapa pode ter um impacto significativo no desempenho da consulta, mesmo que a indexação tenha alguma sobrecarga no desempenho total do mapa. Se a indexação em atributos de objetos envolvidos em consultas, o mecanismo de consulta desempenha uma varredura de tabela para cada atributo. A varredura de tabela é a operação mais cara durante a execução de uma consulta. A indexação sobre atributos do objeto que são envolvidos em consultas permite que o mecanismo de consulta evite uma varredura de tabela desnecessária, melhorando o desempenho total da consulta. Se o aplicativo é designado para utilizar a consulta de maneira intensiva em um mapa que é em sua maior parte de leitura, configure índices para os atributos de objeto que estão envolvidos na consulta. Se o mapa for atualizado em sua maior parte, será necessário equilibrar entre o aprimoramento de desempenho de consulta e a sobrecarga de indexação no mapa.

Quando os POJO (Plain Old Java Objects) são armazenados em um mapa, a indexação adequada pode evitar uma reflexão Java. No exemplo a seguir, a

consulta substitui a cláusula WHERE pela pesquisa de índice de intervalo, se o campo budget tiver um índice construído sobre ele. Caso contrário, a consulta varre o mapa inteiro e avalia a cláusula WHERE obtendo primeiro o orçamento utilizando o reflexo Java e, então, comparando o orçamento com o valor 50000:

```
SELECT d FROM DeptBean d WHERE d.budget=50000
```

Consulte “Plano de Consulta” na página 748 para obter detalhes sobre como ajustar melhor consultas individuais e como sintaxe, modelos de objetos e índices diferentes podem afetar o desempenho da consulta.

Utilizando a Paginação

Em ambientes de cliente-servidor, o mecanismo de consulta transporta o mapa de resultado inteiro para o cliente. Os dados retornados deveriam ser divididos em partes razoáveis. As interfaces EntityManager Query e ObjectMap ObjectQuery suportam os métodos setFirstResult e setMaxResults que permitem que a consulta retorne um subconjunto dos resultados.

Valores de Primitiva de Retorno ao invés de Entidades

Com a API EntityManager Query, as entidades são retornadas como parâmetros de consulta. O mecanismo de consulta retorna atualmente as chaves para essas entidades no cliente. Quando o cliente se itera sobre essas entidades utilizando o Iterator do método getResultIterator, cada entidade é automaticamente aumentada e gerenciada, como se fosse criada com o método find na interface EntityManager. Todo o gráfico da entidade é construído a partir da entidade ObjectMap no cliente. Os atributos de valor da entidade e quaisquer entidades relacionadas são ansiosamente resolvidos.

Para evitar a construção do gráfico de alto custo, modifique a consulta para retornar os atributos individuais com navegação de caminho.

Por exemplo:

```
// Returns an entity
SELECT p FROM Person p
// Returns attributes SELECT p.name, p.address.street, p.address.city, p.gender FROM Person p
```

Tarefas relacionadas:

Java "Configurando o Plug-in HashIndex" na página 586
É possível configurar o HashIndex integrado, a classe com.ibm.websphere.objectgrid.plugins.index.HashIndex, com um arquivo XML, programaticamente ou com uma anotação de entidade em um mapa de entidade.

Java "Acessando Dados com Índices (API de Índice)" na página 359
Use indexação para acesso a dados mais eficiente.

Referências relacionadas:

Java "Atributos do Plug-in HashIndex" na página 589
É possível usar os seguintes atributos para configurar o plug-in HashIndex. Esses atributos definem propriedades, como se você estiver usando um atributo ou HashIndex composto ou se a indexação do intervalo estiver ativada.

Java "Atributos do Plug-in InverseRangeIndex" na página 583
É possível usar os seguintes atributos para configurar o plug-in InverseRangeIndex. Esses atributos definem propriedades sobre como o índice é construído.

Java Interface GlobalIndex

Plano de Consulta

Java

Todas as consultas do eXtreme Scale possuem um plano de consulta. O plano descreve como o mecanismo de consulta interage com os ObjectMaps e índices. Exiba o plano de consulta para determinar se a cadeia de consulta ou índices estão sendo utilizados apropriadamente. O plano de consulta também pode ser usado para explorar as diferenças que as mudanças repentinas em uma sequência de consultas fazem na maneira que o eXtreme Scale executa uma consulta.

O plano de consulta pode ser visualizado de uma de duas maneiras:

- Métodos da API getPlan EntityManager Query ou ObjectQuery
- Rastreio de diagnóstico do ObjectGrid

Método getPlan

O método getPlan nas interfaces ObjectQuery e Query retorna uma String que descreve o plano de consulta. Esta cadeia pode ser exibida na saída padrão ou no log para exibir um plano de consulta.

Nota: Em um ambiente distribuído, o método getPlan não é executado junto ao servidor e não refletirá nenhum índice definido. Para visualizar o plano, utilize um agente para visualizar o plano no servidor.

Rastreio de Plano de Consulta

O plano de consulta pode ser exibido utilizando o rastreio do ObjectGrid. Para ativar o rastreio de plano de consulta, utilize a seguinte especificação de rastreio:

```
QueryEnginePlan=debug=enabled
```

Consulte "Coletando Rastreio" na página 858 para obter detalhes sobre como ativar o rastreio e localizar os arquivos de log de rastreio.

Exemplos de Plano de Consulta

O plano de consulta usa a palavra para indicar que a consulta está iterando por meio de uma coleção do ObjectMap ou por meio de uma coleção derivada, tal como: q2.getEmps(), q2.dept, ou uma coleção temporária retornada por um loop interno. Se a coleção for a partir de um ObjectMap, o plano de consulta mostrará se uma varredura sequencial (denotada por `por INDEX SCAN`), índice exclusivo ou não exclusivo, é usado. Planos de consulta utilizam uma cadeia de filtros para lista as expressões de consulta aplicadas a uma coleta.

Geralmente, um produto cartesiano não é utilizado na consulta do objeto. A consulta a seguir varre o mapa EmpBean inteiro no loop externo e varre o mapa DeptBean inteiro no loop interno:

```
SELECT e, d FROM EmpBean e, DeptBean d

Plan trace:

for q2 in EmpBean ObjectMap using INDEX SCAN
     for q3 in DeptBean ObjectMap using INDEX SCAN
   returning new Tuple( q2,  q3  )
```

A consulta a seguir recupera todos os nomes de funcionários a partir de um departamento específico ao varrer sequencialmente o mapa EmpBean para obter um objeto employee. A partir do objeto employee, a consulta navega até seu objeto department e aplica o filtro d.no=1. Neste exemplo, cada funcionário possui apenas uma referência de objeto departamento, assim o loop interno é executado uma vez:

```
SELECT e.name FROM EmpBean e JOIN e.dept d WHERE d.no=1

Plan trace:

for q2 in EmpBean ObjectMap using INDEX SCAN
     for q3 in  q2.dept
      filter ( q3.getNo() = 1 )
   returning new Tuple( q2.name  )
```

O exemplo a seguir é equivalente à consulta anterior. Entretanto, a consulta a seguir executa melhor porque ela primeiro limita o resultado para um objeto departamento ao usar o índice exclusivo que é definido sobre o número do campo de chave primária DeptBean. A partir do objeto department, a consulta navega para os seus objetos employee para obter seus nomes:

```
SELECT e.name FROM DeptBean d JOIN d.emps e WHERE d.no=1

Plan trace:

for q2 in DeptBean ObjectMap using UNIQUE INDEX key=(1)
     for q3 in  q2.getEmps()
   returning new Tuple( q3.name  )
```

A consulta a seguir localiza todos os funcionários que trabalham em desenvolvimento ou vendas. A consulta varre o mapa EmpBean inteiro e executa filtragem adicional avaliando as expressões: d.name = 'Sales' ou d.name='Dev'

```
SELECT e FROM EmpBean e, in (e.dept) d WHERE d.name = 'Sales' or d.name='Dev'

Plan trace:

for q2 in EmpBean ObjectMap using INDEX SCAN
     for q3 in  q2.dept
      filter (( q3.getName() = Sales ) OR ( q3.getName() = Dev ) )
   returning new Tuple( q2  )
```

A consulta a seguir é equivalente à consulta anterior, mas esta consulta executa um plano de consulta diferente e utiliza o índice de intervalo baseado no nome do campo. Em geral, esta consulta desempenha melhor porque o índice sobre o nome do campo é utilizado para restringir em objetos de departamentos, o que é executado mais rapidamente se apenas alguns departamentos forem de desenvolvimento ou vendas.

```
SELECT e FROM DeptBean d, in(d.emps) e WHERE d.name='Dev' or d.name='Sales'

Plan trace:

IteratorUnionIndex of

     for q2 in DeptBean ObjectMap using INDEX on name = (Dev)
       for q3 in  q2.getEmps()


     for q2 in DeptBean ObjectMap using INDEX on name = (Sales)
       for q3 in  q2.getEmps()
```

A consulta a seguir localiza departamentos que não possuem nenhum funcionário:

```
SELECT d FROM DeptBean d WHERE NOT EXISTS(select e from d.emps e)

Plan trace:

for q2 in DeptBean ObjectMap using INDEX SCAN
    filter ( NOT  EXISTS (    correlated collection defined as

       for q3 in  q2.getEmps()
       returning new Tuple( q3  )

   returning new Tuple( q2  )
```

A consulta a seguir é equivalente à consulta anterior, mas utiliza a função escalar SIZE. Esta consulta possui desempenho semelhante, mas é mais fácil de gravar.

```
SELECT d FROM DeptBean d WHERE SIZE(d.emps)=0
for q2 in DeptBean ObjectMap using INDEX SCAN
    filter (SIZE( q2.getEmps()) = 0 )
   returning new Tuple( q2  )
```

O exemplo a seguir é uma outra forma de escrever a mesma consulta como a consulta anterior com desempenho semelhante, mas esta consulta também é mais fácil de escrever:

```
SELECT d FROM DeptBean d WHERE d.emps is EMPTY

Plan trace:

for q2 in DeptBean ObjectMap using INDEX SCAN
    filter ( q2.getEmps() IS EMPTY  )
   returning new Tuple( q2  )
```

A consulta a seguir localiza quaisquer funcionários com um endereço inicial correspondendo a pelo menos um dos endereços do funcionário cujo nome seja igual ao valor do parâmetro. O loop interno não possui nenhuma dependência do loop externo. A consulta é executada no loop interno uma vez.

```
SELECT e FROM EmpBean e WHERE e.home =  any (SELECT e1.home FROM EmpBean e1 WHERE e1.name=?1)
for q2 in EmpBean ObjectMap using INDEX SCAN
    filter ( q2.home =ANY     temp collection defined as
```

```
       for q3 in EmpBean ObjectMap using INDEX on name = ( ?1)
       returning new Tuple( q3.home      )
 )
   returning new Tuple( q2  )
```

A consulta a seguir é equivalente à consulta anterior, mas possui uma subconsulta correlacionada; além disso, o loop interno é executado repetidamente.

```
SELECT e FROM EmpBean e WHERE EXISTS(SELECT e1 FROM EmpBean e1 WHERE
e.home=e1.home and e1.name=?1)

Plan trace:

for q2 in EmpBean ObjectMap using INDEX SCAN
    filter ( EXISTS (    correlated collection defined as

       for q3 in EmpBean ObjectMap using INDEX on name = ( ?1)
        filter ( q2.home =  q3.home )
       returning new Tuple( q3  )

   returning new Tuple( q2  )
```

Otimização de Consulta Utilizando Índices

Java

Definir e utilizar índices adequadamente pode aprimorar significativamente o desempenho da consulta.

As consultas do WebSphere eXtreme Scale podem usar plug-ins HashIndex integrados para aumentar o desempenho de consultas. Os índices podem ser definidos em atributos entity ou object. O mecanismo de consulta usará automaticamente os índices definidos se a sua cláusula WHERE usar uma das seguintes cadeias:

- Uma expressão de comparação com os seguintes operadores: =, <, >, <= ou >= (quaisquer expressões de comparação, exceto não iguais <>)
- Uma expressão BETWEEN
- Operandos das expressões são constantes ou termos simples

Requisitos

Os índices têm os seguintes requisitos quando usados pela Consulta:

- Todos os índices devem usar o plug-in HashIndex integrado.
- Todos os índices devem ser estaticamente definidos. Os índices dinâmicos não são suportados.
- A anotação @Index pode ser usada para criar automaticamente plug-ins HashIndex estáticos.
- Todos os índices de um único atributo devem ter o conjunto de propriedades RangeIndex configurado como true.
- Todos os índices compostos devem ter o conjunto de propriedades RangeIndex configurado como false.
- Todos os índices de associação (relacionamento) devem ter o conjunto de propriedades RangeIndex configurado como false.

Para obter informações sobre a configuração do HashIndex, consulte o “Plug-ins para Indexar Dados” na página 580.

Para obter informações sobre a indexação, consulte o “Indexação” na página 280.

Para obter uma maneira mais eficiente de procurar objetos armazenados em cache, consulte “Usando um Índice Composto” na página 596

Uso de Dicas para Escolher um Índice

Um índice pode ser manualmente selecionado usando o método setHint nas interfaces Query e ObjectQuery com a constante HINT_USEINDEX. Isto pode ser útil quando a otimização de uma consulta usar o melhor índice de desempenho.

Exemplos de consulta que usam índices de atributo

Os exemplos a seguir utilizam termos simples: e.empid, e.name, e.salary, d.name, d.budget e e.isManager. Os exemplos assumem que os índices são definidos sobre os campos name, salary e budget de um objeto entity ou value. O campo empid é uma chave primária e isManager não possui índice definido.

A consulta a seguir utiliza ambos os índices sobre o campos name e salary. Ela retorna todos os funcionários com nomes iguais ao valor do primeiro parâmetro ou um salário igual ao valor do segundo parâmetro:

```
SELECT e FROM EmpBean e where e.name=?1 or e.salary=?2
```

A consulta a seguir usa ambos índices sobre os campos de nome e orçamento. Ela retorna todos os departamentos nomeados 'DEV' com um orçamento que é maior que 2000.

```
SELECT d FROM DeptBean dwhere d.name='DEV' and d.budget>2000
```

A consulta a seguir retorna todos os funcionários com um salário maior do que 3000 e com um valor sinalizador isManager igual ao valor do parâmetro. A consulta utiliza o índice que é definido sobre o campo salary e executa filtragem adicional ao avaliar a expressão de comparação: `e.isManager=?1.`

```
SELECT e FROM EmpBean e where e.salary>3000 and e.isManager=?1
```

A consulta a seguir localiza todos os funcionários que ganham mais que o primeiro parâmetro ou que qualquer funcionário que é um gerente. Embora o campo salary tenha um índice definido, a consulta varre o índice integrado que é baseado em chaves primárias do campo EmpBean e avalia a expressão: `e.salary>?1` ou `e.isManager=TRUE`.

```
SELECT e FROM EmpBean e WHERE e.salary>?1 or e.isManager=TRUE
```

A consulta a seguir retorna funcionários com um nome que contém a letra a. Embora o campo name tenha um índice definido, a consulta não utiliza o índice porque o campo name é utilizado na expressão LIKE.

```
SELECT e FROM EmpBean e WHERE e.name LIKE '%a%'
```

A consulta a seguir localiza todos os funcionários com um nome que não seja "Smith". Embora o campo name tenha um índice definido, a consulta não utiliza o índice porque a consulta utiliza o operador de comparação não iguais (<>).

```
SELECT e FROM EmpBean e where e.name<>'Smith'
```

A seguinte consulta localiza todos os departamentos com um orçamento menor do que o valor do parâmetro e com um salário superior a 3000. A consulta utiliza um índice para o salário, mas não utiliza um índice para o orçamento porque dept.budget não é um termo simples. Os objetos dept são derivados da coleta e. Não é necessário utilizar o índice de orçamento para consultar objetos dept.

```
SELECT dept from EmpBean e, in (e.dept) dept where e.salary>3000 and
dept.budget<?
```

A consulta a seguir localiza todos os funcionários com um salário maior do que o salário dos funcionários que possuem o empid e 1, 2 e 3. O salário do índice não é utilizado porque a comparação envolve uma subconsulta. O empid é uma chave primária, entretanto, ele é utilizado para uma procura de índice exclusiva porque todas as chaves primárias possuem um índice integrado definido.

```
SELECT e FROM EmpBean e WHERE e.salary > ALL (SELECT e1.salary    FROM
EmpBean e1 WHERE e1.empid=1 or e1.empid =2 or e1.empid=99)
```

Para verificar se o índice está sendo utilizado pela consulta, é possível visualizar o "Plano de Consulta" na página 748. A seguir, está um plano de consulta de exemplo para a consulta anterior:

```
for q2 in EmpBean ObjectMap using INDEX SCAN
    filter ( q2.salary >ALL     temp collection defined as
       IteratorUnionIndex of

         for q3 in EmpBean ObjectMap using UNIQUE INDEX key=(1)
        )

         for q3 in EmpBean ObjectMap using UNIQUE INDEX key=(2)
        )

         for q3 in EmpBean ObjectMap using UNIQUE INDEX key=(99)
        )
       returning new Tuple( q3.salary )
   returning new Tuple( q2  )

for q2 in EmpBean ObjectMap using RANGE INDEX on salary with range(3000,)
     for q3 in  q2.dept
      filter ( q3.budget <  ?1 )
   returning new Tuple( q3  )
```

Atributos de Indexação

Os índices podem ser definidos sobre qualquer tipo de atributo único com os limitadores anteriormente definidos.

definição de índices de entidade usando @Index

Para definir um índice em uma entidade, simplesmente defina uma anotação:

Entidades usando anotações

```
  @Entity
  public class Employee {
  @Id int empid;
  @Index String name
  @Index double salary
  @ManyToOne Department dept;
}
@Entity
  public class Department {
```

```
@Id int deptid;
@Index String name;
@Index double budget;
boolean isManager;
@OneToMany Collection<Employee> employees;
}
```

Com XML

Os índices também podem ser definidos usando XML:

Entidades sem anotações

```
public class Employee {
int empid;
String name
double salary
Department dept;
}

public class Department {
int deptid;
String name;
double budget;
boolean isManager;
Collection employees;
}
```

XML do ObjectGrid com índices de atributos

```
<?xml version="1.0" encoding="UTF-8"?>
  <objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
  xmlns="http://ibm.com/ws/objectgrid/config">
  <objectGrids>
  <objectGrid name="DepartmentGrid" entityMetadataXMLFile="entity.xml>
  <backingMap name="Employee" pluginCollectionRef="Emp"/>
  <backingMap name="Department" pluginCollectionRef="Dept"/>
  </objectGrid>
  </objectGrids>
  <backingMapPluginCollections>
  <backingMapPluginCollection id="Emp">
  <bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
  <property name="Name"
type="java.lang.String" value="Employee.name"/>
  <property name="AttributeName"
type="java.lang.String" value="name"/>
  <property name="RangeIndex" type="boolean" value="true"
  description="Ranges are must be set to true for attributes." />
  </bean>
  <bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
  <property name="Name"
type="java.lang.String" value="Employee.salary"/>
  <property name="AttributeName"
type="java.lang.String" value="salary"/>
  <property name="RangeIndex" type="boolean" value="true"
  description="Ranges are must be set to true for attributes." />
  </bean>
  </backingMapPluginCollection>
  <backingMapPluginCollection id="Dept">
  <bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
  <property name="Name"
type="java.lang.String" value="Department.name"/>
  <property name="AttributeName"
type="java.lang.String" value="name"/>
  <property name="RangeIndex" type="boolean" value="true"
  description="Ranges are must be set to true for attributes." />
  </bean>
  <bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
  <property name="Name"
type="java.lang.String" value="Department.budget"/>
  <property name="AttributeName"
type="java.lang.String" value="budget"/>
  <property name="RangeIndex" type="boolean" value="true"
  description="Ranges are must be set to true for attributes." />
  </bean>
  </backingMapPluginCollection>
  </backingMapPluginCollections>
  </objectGridConfig>
```

Entidade XML

```
<?xml version="1.0" encoding="UTF-8"?>
  <entity-mappings xmlns="http://ibm.com/ws/projector/config/emd"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://ibm.com/ws/projector/config/emd ./emd.xsd">

  <description>Department entities</description>
  <entity class-name="acme.Employee" name="Employee" access="FIELD">
  <attributes>
  <id name="empid" />
  <basic name="name" />
  <basic name="salary" />
  <many-to-one name="department"
  target-entity="acme.Department"
  fetch="EAGER">
  <cascade><cascade-persist/></cascade>
  </many-to-one>
  </attributes>
  </entity>
  <entity class-name="acme.Department" name="Department" access="FIELD">
  <attributes>
  <id name="deptid" />
  <basic name="name" />
  <basic name="budget" />
  <basic name="isManager" />
  <one-to-many name="employees"
  target-entity="acme.Employee"
  fetch="LAZY" mapped-by="parentNode">
  <cascade><cascade-persist/></cascade>
  </one-to-many>
  </attributes>
  </entity>
  </entity-mappings>
```

Definição de índices para não-entidades usando XML

Os índices para tipos de não-entidade são definidos em XML. Não há diferença quando a criação do MapIndexPlugin para mapas de entidade e mapas de não-entidade.

Java bean

```
public class Employee {
  int empid;
  String name
  double salary
  Department dept;

 public class Department {
  int deptid;
  String name;
  double budget;
  boolean isManager;
  Collection employees;
  }
```

XML do ObjectGrid com índices de atributos

```
<?xml version="1.0" encoding="UTF-8"?>
  <objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
  xmlns="http://ibm.com/ws/objectgrid/config">
  <objectGrids>
  <objectGrid name="DepartmentGrid">
  <backingMap name="Employee" pluginCollectionRef="Emp"/>
  <backingMap name="Department" pluginCollectionRef="Dept"/>
  <querySchema>
  <mapSchemas>
  <mapSchema mapName="Employee" valueClass="acme.Employee"
  primaryKeyField="empid" />
  <mapSchema mapName="Department" valueClass="acme.Department"
  primaryKeyField="deptid" />
  </mapSchemas>
  <relationships>
  <relationship source="acme.Employee"
  target="acme.Department"
  relationField="dept" invRelationField="employees" />
  </relationships>
  </querySchema>
  </objectGrid>
  </objectGrids>
  <backingMapPluginCollections>
  <backingMapPluginCollection id="Emp">
```

```
  <bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
  <property name="Name"
type="java.lang.String" value="Employee.name"/>
  <property name="AttributeName"
type="java.lang.String" value="name"/>
  <property name="RangeIndex" type="boolean" value="true"
  description="Ranges are must be set to true for attributes." />
  </bean>
  <bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
  <property name="Name"
type="java.lang.String" value="Employee.salary"/>
  <property name="AttributeName"
type="java.lang.String" value="salary"/>
  <property name="RangeIndex" type="boolean" value="true"
  description="Ranges are must be set to true for attributes." />
  </bean>
  </backingMapPluginCollection>
  <backingMapPluginCollection id="Dept">
  <bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
  <property name="Name"
type="java.lang.String" value="Department.name"/>
  <property name="AttributeName"
type="java.lang.String" value="name"/>
  <property name="RangeIndex" type="boolean" value="true"
  description="Ranges are must be set to true for attributes." />
  </bean>
  <bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
  <property name="Name"
type="java.lang.String" value="Department.budget"/>
  <property name="AttributeName"
type="java.lang.String" value="budget"/>
  <property name="RangeIndex" type="boolean" value="true"
  description="Ranges are must be set to true for attributes." />
  </bean>
  </backingMapPluginCollection>
  </backingMapPluginCollections>
  </objectGridConfig>
```

Indexando Relacionamentos

O WebSphere eXtreme Scale armazena as chaves estrangeiras para entidades relacionadas dentro do objeto-pai. Para entidades, as chaves são armazenadas na tupla subjacente. Para objetos não-entidade, as chaves são explicitamente armazenadas no objeto-pai.

Incluir um índice em um atributo de relacionamento pode acelerar consultas que utilizam referências cíclicas ou utilizam os filtros de consulta IS NULL, IS EMPTY, SIZE e MEMBER OF. Ambas as associações únicas e com diversos valores podem ter a anotação @Index ou uma configuração de plug-in HashIndex em um arquivo XML descritor do ObjectGrid.

Definição de índices de relacionamento de entidade usando @Index

O exemplo a seguir define entidades com anotações @Index:

Entidade com anotação

```
@Entity
public class Node {
    @ManyToOne @Index
    Node parentNode;

    @OneToMany @Index
    List<Node> childrenNodes = new ArrayList();

    @OneToMany @Index
    List<BusinessUnitType> businessUnitTypes = new ArrayList();
}
```

Definição dos índices de relacionamento da entidade usando XML

O exemplo a seguir define as mesmas entidades e índices usando XML com plug-ins HashIndex:

Entidade sem anotações

```
public class Node {
int nodeId;
Node parentNode;
List<Node> childrenNodes = new ArrayList();
List<BusinessUnitType> businessUnitTypes = new ArrayList();
}
```

ObjectGrid XML

```
<?xml version="1.0" encoding="UTF-8"?>
  <objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
  xmlns="http://ibm.com/ws/objectgrid/config">
  <objectGrids>
  <objectGrid name="ObjectGrid_Entity" entityMetadataXMLFile="entity.xml">
  <backingMap name="Node" pluginCollectionRef="Node"/>
  <backingMap name="BusinessUnitType" pluginCollectionRef="BusinessUnitType"/>
  </objectGrid>
  </objectGrids>
  <backingMapPluginCollections>
  <backingMapPluginCollection id="Node">
  <bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
  <property name="Name"
type="java.lang.String" value="parentNode"/>
  <property name="AttributeName"
type="java.lang.String" value="parentNode"/>
<property name="RangeIndex" type="boolean" value="false"
  description="Ranges are not supported for association indexes." />  </bean>
  <bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
  <property name="Name"
type="java.lang.String" value="businessUnitType"/>
  <property name="AttributeName"
type="java.lang.String" value="businessUnitTypes"/>

<property name="RangeIndex" type="boolean" value="false"
  description="Ranges are not supported for association indexes." />
 </bean>
  <bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
  <property name="Name"
type="java.lang.String" value="childrenNodes"/>
  <property name="AttributeName"
type="java.lang.String" value="childrenNodes"/>
<property name="RangeIndex" type="boolean" value="false"
  description="Ranges are not supported for association indexes." />
  </bean>
  </backingMapPluginCollection>
  </backingMapPluginCollections>
  </objectGridConfig>
```

Entidade XML

```
  <?xml version="1.0" encoding="UTF-8"?>
  <entity-mappings xmlns="http://ibm.com/ws/projector/config/emd"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://ibm.com/ws/projector/config/emd ./emd.xsd">

  <description>My entities</description>
  <entity class-name="acme.Node" name="Account" access="FIELD">
  <attributes>
  <id name="nodeId" />
  <one-to-many name="childrenNodes"
  target-entity="acme.Node"
  fetch="EAGER" mapped-by="parentNode">
  <cascade><cascade-all/></cascade>
  </one-to-many>
  <many-to-one name="parentNodes"
  target-entity="acme.Node"
  fetch="LAZY" mapped-by="childrenNodes">
  <cascade><cascade-none/></cascade>
  </one-to-many>
  <many-to-one name="businessUnitTypes"
  target-entity="acme.BusinessUnitType"
  fetch="EAGER">
  <cascade><cascade-persist/></cascade>
  </many-to-one>
</attributes>
  </entity>
  <entity class-name="acme.BusinessUnitType" name="BusinessUnitType" access="FIELD">
  <attributes>
  <id name="buId" />
  <basic name="TypeDescription" />
  </attributes>
  </entity>
  </entity-mappings>
```

Usando os índices anteriormente definidos, os exemplos de consulta de entidades a seguir são otimizados:

```
SELECT n FROM Node n WHERE n.parentNode is null
SELECT n FROM Node n WHERE n.businessUnitTypes is EMPTY
  SELECT n FROM Node n WHERE size(n.businessUnitTypes)>=10
  SELECT n FROM BusinessUnitType b, Node n WHERE b member of n.businessUnitTypes and b.name='TELECOM'
```

Definição dos índices de relacionamento de não-entidade

O exemplo a seguir define um plug-in HashIndex para mapas de não-entidade em um arquivo XML descritor do ObjectGrid:

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
  xmlns="http://ibm.com/ws/objectgrid/config">
  <objectGrids>
    <objectGrid name="ObjectGrid_POJO">
      <backingMap name="Node" pluginCollectionRef="Node"/>
      <backingMap name="BusinessUnitType" pluginCollectionRef="BusinessUnitType"/>
      <querySchema>
        <mapSchemas>
          <mapSchema mapName="Node" valueClass="com.ibm.websphere.objectgrid.samples.entity.Node"
            primaryKeyField="id" />
          <mapSchema mapName="BusinessUnitType"
            valueClass="com.ibm.websphere.objectgrid.samples.entity.BusinessUnitType"
            primaryKeyField="id" />
        </mapSchemas>
        <relationships>
          <relationship source="com.ibm.websphere.objectgrid.samples.entity.Node"
            target="com.ibm.websphere.objectgrid.samples.entity.Node"
            relationField="parentNodeId" invRelationField="childrenNodeIds" />
          <relationship source="com.ibm.websphere.objectgrid.samples.entity.Node"
            target="com.ibm.websphere.objectgrid.samples.entity.BusinessUnitType"
            relationField="businessUnitTypeKeys" invRelationField="" />
        </relationships>
      </querySchema>
    </objectGrid>
  </objectGrids>
  <backingMapPluginCollections>
    <backingMapPluginCollection id="Node">
      <bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
        <property name="Name"
type="java.lang.String" value="parentNode"/>
<property name="Name"
type="java.lang.String" value="parentNodeId"/>
<property name="AttributeName"
type="java.lang.String" value="parentNodeId"/>
<property name="RangeIndex" type="boolean" value="false"
  description="Ranges are not supported for association indexes." />
      </bean>
      <bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
        <property name="Name"
type="java.lang.String" value="businessUnitType"/>
        <property name="AttributeName"
type="java.lang.String" value="businessUnitTypeKeys"/>

<property name="RangeIndex" type="boolean" value="false"
  description="Ranges are not supported for association indexes." />
   </bean>
      <bean id="MapIndexPlugin" className="com.ibm.websphere.objectgrid.plugins.index.HashIndex" >
<property name="Name"
type="java.lang.String" value="childrenNodeIds"/>
  <property name="AttributeName"
type="java.lang.String" value="childrenNodeIds"/>
  <property name="RangeIndex" type="boolean" value="false"
      description="Ranges are not supported for association indexes." />
</bean>
    </backingMapPluginCollection>
  </backingMapPluginCollections>
</objectGridConfig>
```

Dadas as configurações de índice acima, o exemplos de consulta do objeto são otimizados:

```
SELECT n FROM Node n WHERE n.parentNodeId is null
SELECT n FROM Node n WHERE n.businessUnitTypeKeys is EMPTY
SELECT n FROM Node n WHERE size(n.businessUnitTypeKeys)>=10
SELECT n FROM BusinessUnitType b, Node n WHERE b member of n.businessUnitTypeKeys and b.name='TELECOM
```

Otimização de Consulta do Cliente Utilizando Índices Globais

Ao executar consultas a partir do ObjectGrid do cliente, é necessário configurar a partição se os mapas envolvidos são particionados. Em um grande ambiente do ObjectGrid particionado, o aplicativo geralmente precisa executar consultas paralelas simultaneamente em todas as partições para obter o resultado da consulta completo. Por exemplo, se houver 100 partições, o aplicativo deverá executar a mesma consulta em todas as 100 partições e mesclar os resultados da consulta para obter o resultado da consulta completo. Isto geralmente consome grandes quantidades de recurso do sistema.

Se qualquer predicado na consulta tem o plug-in HashIndex correspondente definido, a consulta do cliente pode ativar o índice global no plug-in HashIndex e utilizar a API MapGlobalIndex para localizar partições pelo atributo que representa o valor do predicado.

Por exemplo, a consulta a seguir retorna todos os funcionários, em que `employeeCode` é igual a 1. A consulta utiliza o índice que é definido no campo `employeeCode`.

```
SELECT e FROM EmpBean e where e.employeeCode  = 1
```

O exemplo a seguir é a configuração do HashIndex que é utilizada para a consulta:

```
<bean id="MapIndexPlugin"
      className="com.ibm.websphere.objectgrid.plugins.index.HashIndex">
         <property name="Name"
type="java.lang.String" value="CODE"
            description="index name" />
         <property name="AttributeName"
type="java.lang.String" value="employeeCode" description="attribute name" />
  <property name="GlobalIndexEnabled" type="boolean" value="true"
            description="true for global index" />
   </bean>
```

O atributo indexado é `employeeCode` que é utilizado no predicado da consulta. O índice global está ativado nesse índice para que o proxy de índice MapGlobalIndex esteja disponível.

O aplicativo pode usar o método MapGlobalIndex.findPartitions() para localizar partições aplicáveis primeiro. Em seguida, execute a consulta apenas nestas partições aplicáveis. O código a seguir demonstra esta abordagem.

```
// in client ObjectGrid process
MapGlobalIndex mapGlobalIndexCODE = (MapGlobalIndex)m.getIndex("CODE", false);
Object attribute1 = new Integer(1);
Object[] attributes = new Object[] {attribute1};
Collection partitions = mapGlobalIndexCODE.findPartitions(attributes);
// the returned partitions is a subset of all partitions.
Iterator partitionsIter = partitions.iterator();
String query = "SELECT e FROM EmpBean e where e.employeeCode = ?1";
ObjectQuery oQuery = session.createObjectQuery(query);
// set the query parameter value as the attribute1 that is used in
// mapGlobalIndexCode.findPartitions
oQuery.setParameter(1, attribute1);

Set completeQueryResultSet = new HashSet();
// the following code shows serial query pattern, it runs the query on one partition at a time.
// production code should use parallel query pattern to run query on all applicable partitions in parallel.
while (partitionsIter.hasNext()) {
Integer pid = (Integer)partitionsIter.next();
oQuery.setPartition(pid);
Iterator queryResultIter = oQuery.getResultIterator();
while (queryResultIter.hasNext()) {
completeQueryResultSet.add(queryResultIter.next());
}
}
```

O propósito de utilizar índice global em uma consulta do cliente é executar consultas apenas em partições aplicáveis. Fazendo isso, você pode evitar chamadas remotas desnecessárias. No entanto, o índice global não garante melhoria de desempenho. Se as partições retornadas do método MapGlobalIndex.findPartitions() excederem uma determinada percentagem de partições completas, por exemplo 90%, o gasto adicional de utilizar o índice global poderá frustrar seu propósito.

Tarefas relacionadas:

Java "Configurando o Plug-in HashIndex" na página 586
É possível configurar o HashIndex integrado, a classe com.ibm.websphere.objectgrid.plugins.index.HashIndex, com um arquivo XML, programaticamente ou com uma anotação de entidade em um mapa de entidade.

Java "Acessando Dados com Índices (API de Índice)" na página 359
Use indexação para acesso a dados mais eficiente.

Referências relacionadas:

Java "Atributos do Plug-in HashIndex" na página 589
É possível usar os seguintes atributos para configurar o plug-in HashIndex. Esses atributos definem propriedades, como se você estiver usando um atributo ou HashIndex composto ou se a indexação do intervalo estiver ativada.

Java "Atributos do Plug-in InverseRangeIndex" na página 583
É possível usar os seguintes atributos para configurar o plug-in InverseRangeIndex. Esses atributos definem propriedades sobre como o índice é construído.

Java Interface GlobalIndex

Ajustando o Desempenho da Interface EntityManager

Java

A interface EntityManager separa aplicativos do estado de suspensão no armazenamento de dados da grade do servidor.

O custo do uso da interface EntityManager não é alto e depende do tipo de trabalho sendo feito. Sempre use a interface EntityManager e otimize a lógica de negócios crucial após o aplicativo ser concluído. É possível retrabalhar qualquer código que utilize as interfaces EntityManager para usar mapas e tuplas. Geralmente, esse retrabalho de código pode ser necessário para 10% do código.

Se você usar relacionamentos entre objetos, o impacto no desempenho será menor, porque um aplicativo que usa mapas precisa gerenciar esses relacionamentos da mesma forma que a interface EntityManager.

Os aplicativos que usam a interface EntityManager não precisam fornecer uma implementação ObjectTransformer. Os aplicativos são otimizados automaticamente.

Retrabalhando o Código EntityManager para Mapas

Segue uma entidade de amostra:

```
@Entity
public class Person {
 @Id
 String ssn;
 String firstName;
```

```
 @Index
 String middleName;
 String surname;
}
```

Este é um trecho de código para localizar e atualizar a entidade:

```
Person p = null;
s.begin();
p = (Person)em.find(Person.class, "1234567890");
p.middleName = String.valueOf(inner);
s.commit();
```

A seguir, está o mesmo código utilizando Mapas e Tuplas:

```
Tuple key = null;
key = map.getEntityMetadata().getKeyMetadata().createTuple();
key.setAttribute(0, "1234567890");

// The Copy Mode is always NO_COPY for entity maps if not using COPY_TO_BYTES.
// Either we need to copy the tuple or we can ask the ObjectGrid to do it for us:
map.setCopyMode(CopyMode.COPY_ON_READ);
s.begin();
Tuple value = (Tuple)map.get(key);
value.setAttribute(1, String.valueOf(inner));
map.update(key, value);
value = null;
s.commit();
```

Esses fragmentos de código têm o mesmo resultado, e um aplicativo pode utilizar um ou ambos os fragmentos.

O segundo fragmento de código mostra como utilizar mapas diretamente e como trabalhar com as tuplas (os pares de chave e valor). A tupla de valor tem três atributos: **firstName**, **middlename** e **surname**, indexado em 0, 1 e 2. A tupla de chave tem um único atributo e o número de ID é indexado em zero. É possível ver como as Tuplas são criadas utilizando os métodos EntityMetadata#getKeyMetaData ou EntityMetadata#getValueMetaData. Utilize esses métodos para criar as Tuplas para uma Entidade. Não é possível implementar a interface Tuple e passar uma instância em sua implementação de Tupla.

Tarefas relacionadas:

Java "Tutorial: Armazenando Informações de Pedido nas Entidades" na página 9
Este tutorial do gerenciador de entidade mostra como utilizar o WebSphere eXtreme Scale para armazenar informações de pedido em um Web site. É possível criar um aplicativo Java Platform, Standard Edition 5 simples que utiliza um eXtreme Scale local e de memória. As entidades utilizam anotações e genéricos do Java SE 5.

"Colocando Diversos Objetos de Cache na Mesma Partição" na página 429
Ao definir dados relacionados em conjuntos de mapas que são organizados na mesma partição, você pode evitar a duplicação de dados e permitir o acesso a dados de baixa granularidade.

Referências relacionadas:

Java "Agente de Instrumentação de Desempenho da Entidade"
É possível melhorar o desempenho de entidades de acesso ao campo ativando o agente de instrumentação do WebSphere eXtreme Scale ao usar o Java Development Kit (JDK) Versão 6 ou posterior.

Java "Definindo um Esquema de Entidade" na página 391
Um ObjectGrid pode ter inúmeros esquemas de entidade lógicos. As entidades são definidas usando as classes Java anotadas, o XML ou uma combinação de classes XML e Java. Entidades definidas são registradas com um servidor eXtreme Scale e ligadas a BackingMaps, índices e outros plug-ins.

Java "Listeners de Entidade e Métodos de Retorno de Chamada" na página 408
Os aplicativos podem ser notificados quando o estado de uma entidade é alterado de estado para estado. Dois mecanismos de retorno de chamada existem para os eventos de mudança de estado: os métodos de retorno de chamada do ciclo de vida que são definidos em uma classe de entidade e são chamados sempre que o estado da entidade é alterado e os listeners de entidade, que são mais gerais porque o listener da entidade pode ser registrado em várias entidades.

Java "Exemplos do Listener de Entidade" na página 414
É possível gravar EntityListeners com base em seus requisitos. Veja a seguir vários scripts de exemplo.

Java "Interface EntityTransaction" na página 426
É possível utilizar a interface EntityTransaction para demarcar transações.

Informações relacionadas:

Java Amostra: Executando as Consultas em Paralelo Usando um ReduceGridAgent

Agente de Instrumentação de Desempenho da Entidade

Java

É possível melhorar o desempenho de entidades de acesso ao campo ativando o agente de instrumentação do WebSphere eXtreme Scale ao usar o Java Development Kit (JDK) Versão 6 ou posterior.

Ativando o Agente do eXtreme Scale no JDK Versão 6 ou Posterior

O agente ObjectGrid pode ser ativado com uma opção de linha de comandos Java com a seguinte sintaxe:

```
-javaagent:jarpath[=options]
```

O valor *jarpath* é um caminho para um arquivo Java archive (JAR) do tempo de execução do eXtreme Scale que contém a classe do agente do eXtreme Scale e as classes de suporte como os arquivos `objectgrid.jar`, `wsobjectgrid.jar`, `ogclient.jar`, `wsogclient.jar` e `ogagent.jar`. Normalmente, em um programa Java ou em um ambiente Java Platform, Enterprise Edition independente que não executa o WebSphere Application Server, use o arquivo `objectgrid.jar` ou `ogclient.jar`. Em um ambiente do WebSphere Application Server ou de multicarregadores, é necessário usar o arquivo `ogagent.jar` na opção do agente da linha de comandos Java. Forneça o arquivo `ogagent.config` no caminho de classe ou use opções do agente para especificar informações adicionais.

Opções do Agente do eXtreme Scale

config
Substitui o nome do arquivo de configuração.

inclusão
Especifica ou substitui a definição de domínio de transformação que é a primeira parte do arquivo de configuração.

exclude
Especifica ou substitui a definição @Exclude.

fieldAccessEntity
Especifica ou substitui a definição @FieldAccessEntity.

trace Especifica um nível de rastreio. Os níveis podem ser ALL, CONFIG, FINE, FINER, FINEST, SEVERE, WARNING, INFO e OFF.

trace.file
Especifica o local do arquivo de rastreio.

O ponto e vírgula (**;**) é utilizado como um delimitador para separar cada opção. A vírgula (**,**) é utilizada como um delimitador para separar cada elemento em uma opção. O seguinte exemplo mostra a opção do agente eXtreme Scale para um programa Java:

```
-javaagent:objectgridRoot/lib/objectgrid.jar=config=myConfigFile;
include=includedPackage;exclude=excludedPackage;fieldAccessEntity=package1,package2
```

Arquivo `ogagent.config`

O arquivo `ogagent.config` é o nome do arquivo de configuração do agente do eXtreme Scale designado. Se o nome do arquivo estiver no caminho de classe, o agente do eXtreme Scale localiza e analisa o arquivo. É possível substituir o nome do arquivo designado por meio da opção config do agente do eXtreme Scale. O exemplo a seguir mostra como especificar o arquivo de configuração:

```
-javaagent:objectgridRoot/lib/objectgrid.jar=config=myOverrideConfigFile
```

Um arquivo de configuração do agente do eXtreme Scale possui as seguintes partes:

- **Domínio de transformação:** A parte do domínio de transformação é a primeira no arquivo de configuração. O domínio de transformação é uma lista de pacotes e classes que estão incluídos no processo de transformação da classe. Este domínio de transformação deve incluir todas as classes que são classes de entidade field-access e outras classes que fazem referência a estas classes de entidade field-access. As classes de entidade field-access e tais classes que fazem referência a estas classes de entidade field-access constroem o domínio de transformação. Se você planejar especificar classes de entidade field-access na parte @FieldAccessEntity, então não é necessário incluir classes de entidade

field-access aqui. O domínio de transformação deve estar completo. Caso contrário, pode ser possível ver uma exceção FieldAccessEntityNotInstrumentedException.

- **@Exclude:** O token @Exclude indica que os pacotes e as classes listadas após este token são excluídos do domínio de transformação.
- **@FieldAccessEntity:** O token @FieldAccessEntity indica que os pacotes e as classes listados após este token são pacotes e classes Entity field-access. Se não existir nenhuma linha após o token @FieldAccessEntity, então, seu equivalente é "Nenhum @FieldAccessEntity especificado". O agente do eXtreme Scale determina que não há pacotes e classes Entity field-access definidos. Se houver linhas após o token @FieldAccessEntity, então elas representam os pacotes e as classes de entidade de acesso a campos especificados pelo usuário. Por exemplo, "domínio de entidade de acesso a campos". O domínio de entidade de acesso a campos é um subdomínio do domínio de transformação. Os pacotes e as classes que estão listados no domínio de entidade field-access são uma parte do domínio de transformação, mesmo quando não estão listados no domínio de transformação. O token @Exclude, que lista pacotes e classes que são excluídos da transformação, não tem impacto no domínio Entity field-access. Quando o token @FieldAccessEntity é especificado, todas as entidades field-access devem estar este domínio Entity field-access. Caso contrário, uma exceção FieldAccessEntityNotInstrumentedException pode ocorrer.

Arquivo de Configuração do Agente de Exemplo (ogagent.config)

```
##############################
# The # indicates comment line
##############################
# This is an ObjectGrid agent config file (the designated file name is ogagent.config) that can be found and parsed by the ObjectGrid agent
# if it is in classpath.
# If the file name is "ogagent.config" and in classpath, Java program runs with -javaagent:objectgridRoot/ogagent.jar will have
# ObjectGrid agent enabled.
# If the file name is not "ogagent.config" but in classpath, you can specify the file name in config option of ObjectGrid agent
#     -javaagent:objectgridRoot/lib/objectgrid.jar=config=myOverrideConfigFile
# See comments below for more info regarding instrumentation setting override.

# The first part of the configuration is the list of packages and classes that should be included in transformation domain.
# The includes (packages/classes, construct the instrumentation doamin) should be in the beginning of the file.
com.testpackage
com.testClass

# Transformation domain: The above lines are packages/classes that construct the transformation domain.
# The system will process classes with name starting with above packages/classes for transformation.
#
# @Exclude token : Exclude from transformation domain.
# The @Exclude token indicates packages/classes after that line should be excluded from transformation domain.
# It is used when user want to exclude some packages/classes from above specified included packages
#
# @FieldAccessEntity token: Field-access Entity domain.
# The @FieldAccessEntity token indicates packages/classes after that line are field-access Entity packages/classes.
# If there is no lilne after the @FieldAccessEntity token, it is equivalent to "No @FieldAccessEntity specified".
# The runtime will consider the user does not specify any field-access Entity packages/classes.
# The "field-acces Entity domain" is a sub-domain of transformation domain.
#
# Packages/classes listed in the "field-access Entity domain" will always be part of transformation domain,
# even they are not listed in transformation domain.
# The @Exclude, which lists packages/classes excluded from transformation, has no impact on the "field-acces Entity domain".
# Note: When @FieldAccessEntity is specified, all field-access entities must be in this field-acces Entity domain,
#       otherwise, FieldAccessEntityNotInstrumentedException may occur.
#
# The default ObjectGrid agent config file name is ogagent.config
# The runtime will look for this file as a resource in classpath and process it.
# Users can override this designated ObjectGrid agent config file name via config option of agent.
#
# e.g.
# javaagent:objectgridRoot/lib/objectgrid.jar=config=myOverrideConfigFile
#
# The instrumentation definition, including transformation domain, @Exclude, and  @FieldAccessEntity can be overriden individually
# by corresponding designated agent options.
# Designated agent options include:
#    include              -> used to override instrumentation domain definition that is the first part of the config file
#    exclude              -> used to override @Exclude definition
#    fieldAccessEntity    -> used to override @FieldAccessEntity definition
#
# Each agent option should be separated by ";"
# Within the agent option, the package or class should be seperated by ","
#
# The following is an example that does not override the config file name:
#    -javaagent:objectgridRoot/lib/objectgrid.jar=
include=includedPackage;exclude=excludedPackage;fieldAccessEntity=package1,package2
#
##############################

@Exclude
com.excludedPackage
com.excludedClass

@FieldAccessEntity
```

Considerações sobre Desempenho

Para obter melhor desempenho, especifique o domínio de transformação e o domínio de entidade field-access.

Conceitos relacionados:

Java "Ajustando o Desempenho da Interface EntityManager" na página 760
A interface EntityManager separa aplicativos do estado de suspensão no armazenamento de dados da grade do servidor.

Java "Objetos de Armazenamento em Cache e seus Relacionamentos (API EntityManager)" na página 388
A maioria dos produtos de cache utiliza APIs baseadas em mapa para armazenar dados como pares de chave-valor. A API ObjectMap e o cache dinâmico no WebSphere Application Server, entre outros, usam essa abordagem. Entretanto, APIs baseadas em mapas têm limitações. A API EntityManager simplifica a interação com a grade de dados ao fornecer uma maneira fácil de declarar e interagir com um gráfico complexo de objetos relacionados.

Java "Entity Manager em um Ambiente Distribuído" na página 401
É possível usar a API EntityManager com um ObjectGrid local ou em um ambiente distribuído do eXtreme Scale . A principal diferença é como você se conecta a esse ambiente remoto. Após você estabelecer uma conexão, não existe diferença entre o uso de um objeto Session ou uma API do EntityManager.

Java "Interagindo com EntityManager" na página 405
Geralmente os aplicativos primeiro obtêm uma referência do ObjectGrid e, depois, uma Sessão dessa referência para cada encadeamento. As sessões não podem ser compartilhadas entre encadeamentos. Um método extra em Session, o método getEntityManager, está disponível. Este método retorna uma referência para um gerenciador de entidades para uso para este encadeamento. A interface de EntityManager pode substituir as interfaces de Session e ObjectMap para todos os aplicativos. É possível utilizar essas APIs de EntityManager se o cliente tiver acesso às classes de entidade definidas.

Java "Suporte ao Plano de Carregamento do EntityManager" na página 417
Um FetchPlan é a estratégia que o gerenciador de entidade usa para recuperar objetos associados se o aplicativo precisar acessar relacionamentos.

Java "Filas de Consulta da Entidade" na página 421
Filas de consulte permitem que aplicativos criem uma fila qualificada por uma consulta no lado do servidor ou eXtreme Scale local sobre uma entidade. As entidades do resultado da consulta são armazenadas nesta fila. Atualmente, a fila de consulta é suportada apenas em um mapa que está utilizando a estratégia de bloqueio pessimista.

Java "Roteando os Objetos de Cache para a Mesma Partição" na página 432
Quando a configuração do eXtreme Scale usa a estratégia de colocação de partição fixa, ela dependerá do hash da chave para uma partição inserir, obter, atualizar ou remover o valor. O método hashCode é chamado na chave e ele deverá ser bem definido se uma chave customizada for criada. No entanto, outra opção é usar a interface PartitionableKey. Com a interface PartitionableKey, será possível usar um objeto diferente da chave para efetuar hash de uma partição.

Tarefas relacionadas:

Java "Tutorial: Armazenando Informações de Pedido nas Entidades" na página 9
Este tutorial do gerenciador de entidade mostra como utilizar o WebSphere eXtreme Scale para armazenar informações de pedido em um Web site. É possível criar um aplicativo Java Platform, Standard Edition 5 simples que utiliza um eXtreme Scale local e de memória. As entidades utilizam anotações e genéricos do Java SE 5.

"Colocando Diversos Objetos de Cache na Mesma Partição" na página 429

Ao definir dados relacionados em conjuntos de mapas que são organizados na mesma partição, você pode evitar a duplicação de dados e permitir o acesso a dados de baixa granularidade.

Informações relacionadas:

Java Amostra: Executando as Consultas em Paralelo Usando um ReduceGridAgent

Capítulo 7. Segurança

WebSphere eXtreme Scale pode proteger o acesso a dados, incluindo permissão para integração com provedores de segurança externos. Os aspectos de segurança incluem autenticação, autorização, segurança de transporte, segurança da grade de dados, segurança local e segurança JMX (MBean).

Cenário: Protegendo sua Grade de Dados no eXtreme Scale

As grades de dados do WebSphere eXtreme Scale armazenam informações sigilosas que devem ser protegidas.

Antes de Iniciar

- Instale o produto. Você deve instalar o tempo de execução do servidor e os clientes. Para clientes, é possível utilizar os clientes Java e .NET. Para obter informações adicionais, consulte Instalando.
- Se estiver atualizando a partir de uma liberação anterior, você deverá ter todos os seus servidores de contêiner e de catálogos no mesmo nível de liberação. Para obter informações adicionais, consulte Fazendo Upgrade e Migrando o WebSphere eXtreme Scale.

Sobre Esta Tarefa

Para uma implementação segura, use diversas camadas de proteção para segurança ideal. O primeiro elemento da proteção é o uso de firewalls para segmentar a rede. O modelo padrão em camadas para aplicativos da web é formado por web clients, uma camada de apresentação de servidores HTTP, uma camada de aplicativo formada por servidores de aplicativos, uma camada de dados e uma camada de armazenamento.

Os servidores de grade de dados do eXtreme Scale são implementados como parte da camada de dados. A prática padrão é colocar os servidores de camada de apresentação em uma zona desmilitarizada (DMZ) protegida por um firewall e colocar as camadas de aplicativo e de armazenamento nos segmentos de rede protegidos por firewalls adicionais. Não implemente servidores do eXtreme Scale em uma DMZ. Os servidores do eXtreme Scale devem ser protegidos como todos os elementos da camada são, de acordo com a prática padrão do segmento de mercado.

No entanto, para proteção ideal contra ameaças de segurança, use um mecanismo de defesa profundo, em que diversas outras medidas protegem a operação do eXtreme Scale e os dados armazenados na grade de dados. Essas medidas adicionais não apenas ajudam na defesa contra ameaças externas, mas também impedem acesso a dados desautorizado por funcionários e contratados que possam ter acesso a segmentos da rede na qual os servidores do eXtreme Scale residem.

Use as etapas de ponta a ponta a seguir para configurar segurança no WebSphere eXtreme Scale, independentemente de se você tem servidores independentes, o Perfil do Liberty, a estrutura OSGi ou o WebSphere Application Server instalado em seu ambiente:

Autenticação da Grade de Dados

Java

É possível utilizar o plug-in do gerenciador de token seguro para ativar a autenticação servidor-para-servidor, que requer que você implemente a interface SecureTokenManager.

O método generateToken(Object) obtém uma proteção de objeto, e depois gera um token que não pode ser compreendido pelos outros. O método verifyTokens(byte[]) faz o processo inverso: converte o token de volta ao objeto original.

Uma implementação SecureTokenManager simples usa um algoritmo de codificação simples, como um algoritmo XOR, para codificar o objeto na forma serializada e depois usa o algoritmo de codificação correspondente para decodificar o token. Esta implementação não é segura e é fácil de ser interrompida.

Implementação padrão do **WebSphere eXtreme Scale**

O WebSphere eXtreme Scale fornece uma implementação imediatamente disponível para esta interface. Esta implementação padrão utiliza um par de chaves para assinar e verificar a assinatura e utiliza uma chave secreta para criptografar o conteúdo. Cada servidor tem um armazenamento de chaves de tipo JCKES para armazenar o par de chaves, uma chave privada e uma chave pública e uma chave secreta. O armazenamento de chaves tem que ser do tipo JCKES para armazenar as chaves secretas. Estas chaves são utilizadas para criptografar e assinar ou verificar a cadeia de segredo na extremidade de envio. Além disso, o token está associado ao tempo de expiração. Na extremidade de recebimento, os dados são verificados, decriptografados e comparados com a cadeia de segredo do receptor. Os protocolos de comunicação Secure Sockets Layer (SSL) não são necessários entre um par de servidores para autenticação, porque as chaves privadas e as chaves públicas servem para a mesma finalidade. No entanto, se a comunicação do servidor não for criptografada, os dados poderão ser roubados por violação na comunicação. Como o token expira em breve, a ameaça de ataque à reprodução é minimizada. Esta possibilidade é significativamente reduzida se todos os servidores forem implementados atrás de um firewall.

A desvantagem desta abordagem é que os administradores do WebSphere eXtreme Scale precisam gerar chaves e transportá-las para todos os servidores, o que pode causar violação de segurança durante o transporte.

Tarefas relacionadas:

8.6+ "Ativando Autenticação LDAP nos Servidores de Catálogos e de Contêineres do eXtreme Scale" na página 780
Ative seus servidores WebSphere eXtreme Scale e servidores de catálogos para autenticação Lightweight Directory Access Protocol (LDAP) com um arquivo de políticas Java Authentication and Authorization Service (JAAS) utilizado para autorização.

"Autenticando e Autorizando Clientes" na página 771
É possível ativar a segurança e a autenticação de credencial para autenticar clientes. Além disso, é possível autorizar clientes administrativos para acessar a grade de dados.

"Autenticando Aplicativos Clientes" na página 772
A autenticação de cliente do aplicativo consiste em ativar a autenticação de credencial e de segurança cliente/servidor e de configurar um autenticador e um gerador de credencial de sistema.

"Autorizando Aplicativos Clientes" na página 774
A autorização do cliente do aplicativo consiste de classes de permissão do ObjectGrid, de mecanismos de autorização, de um período de verificação de permissão e de autorização de acesso apenas pelo criador.

8.6+ "Autorizando Clientes Administrativos" na página 778
Por meio da segurança administrativa, você pode autorizar os usuários a acessar a grade de dados. Algumas condições são necessárias, dependendo de seu ambiente de instalação do WebSphere eXtreme Scale e dos usuários que você deseja que tenham acesso.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Classe ClientSecurityConfigurationFactory

Segurança da Grade de Dados

A segurança da grade de dados garante que um servidor que está se juntando tenha as credenciais certas, de modo que um servidor malicioso não possa juntar-se à grade de dados. A segurança da grade de dados usa um mecanismo de sequência de segredo compartilhado.

Todos os servidores WebSphere eXtreme Scale, incluindo servidores de catálogo, concordam quanto a uma cadeia de segredo compartilhado. Quando um servidor junta a grade de dados, ele é desafiado a apresentar a sequência secreta. Se a cadeia secreta do servidor que está se juntando corresponder à cadeia no servidor presidente ou servidor de catálogo, o servidor que está se juntando é aceito. Se a cadeia não corresponder, o pedido de junção é rejeitado.

Não é seguro enviar um segredo em texto não-criptografado. A infraestrutura de segurança do WebSphere eXtreme Scale fornece um plug-in do gerenciador de token seguro para permitir que o servidor proteja este segredo antes de enviar. Você deve decidir como implementar a operação de proteção. O WebSphere eXtreme Scale fornece uma implementação pronta para usar, na qual a operação segura é implementada para criptografar e assinar o segredo.

A cadeia do segredo é configurada no arquivo `server.properties`. Consulte o Arquivo de Propriedades do Servidor para obter mais informações sobre a propriedade authenticationSecret.

Plug-in SecureTokenManager

Um plug-in do gerenciador de token de segurança é representado pela interface com.ibm.websphere.objectgrid.security.plugins.SecureTokenManager.

Para obter mais informações sobre o plug-in SecureTokenManager, consulte aDocumentação da API SecureTokenManager.

O método generateToken(Object) obtém um objeto, e depois gera um token que não pode ser compreendido pelos outros. O método verifyTokens(byte[]) faz o processo inverso: o método converte o token de volta ao objeto original.

Uma implementação SecureTokenManager simples usa um algoritmo de codificação simples, como um algoritmo exclusivo ou (XOR), para codificar o objeto na forma serializada e depois usa o algoritmo de codificação correspondente para codificar o token. Essa implementação não é segura.

O WebSphere eXtreme Scale fornece uma implementação imediatamente disponível para esta interface.

A implementação padrão utiliza um par de chaves para assinar e verificar a assinatura e utiliza uma chave secreta para criptografar o conteúdo. Cada servidor tem um armazenamento de chaves de tipo JCKES para armazenar o par de chaves, uma chave privada e uma chave pública e uma chave secreta. O armazenamento de chaves tem que ser do tipo JCKES para armazenar as chaves secretas.

Estas chaves são utilizadas para criptografar e assinar ou verificar a cadeia de segredo na extremidade de envio. Além disso, o token está associado ao tempo de expiração. Na extremidade de recebimento, os dados são verificados, decriptografados e comparados com a cadeia de segredo do receptor. Os protocolos de comunicação Secure Sockets Layer (SSL) não são necessários entre um par de servidores para autenticação, porque as chaves privadas e as chaves públicas servem para a mesma finalidade. No entanto, se a comunicação do servidor não for criptografada, os dados poderão ser roubados por violação na comunicação. Como o token expira em breve, a ameaça de ataque à reprodução é minimizada. Esta possibilidade é significativamente reduzida se todos os servidores forem implementados atrás de um firewall.

A desvantagem desta abordagem é que os administradores do WebSphere eXtreme Scale precisam gerar chaves e transportá-las para todos os servidores, o que pode causar violação de segurança durante o transporte.

Scripts de Amostra para Criar Propriedades do Gerenciador de Token Seguro

Conforme observado na seção anterior, é possível criar um keystore contendo um par de chaves para assinar e verificar a assinatura e uma chave secreta para criptografar o conteúdo.

Por exemplo, é possível utilizar o comando JDK 6 keytool para criar a chave da seguinte forma:

```
keytool -genkeypair -alias keypair1 -keystore key1.jck -storetype
JCEKS -keyalg
rsa -dname "CN=sample.ibm.com, OU=WebSphere eXtreme Scale" -storepass
key111 -keypass
keypair1 -validity 10000
```

```
keytool -genseckey -alias seckey1 -keystore key1.jck -storetype JCEKS
-keyalg
DES  -storepass key111 -keypass seckey1 -validity 1000
```

Esses dois comandos criam um par de chaves "keypair1" e uma chave secreta "seckey1". É possível então configurar o seguinte no arquivo de propriedades do servidor:

```
secureTokenKeyStore=key1.jck
secureTokenKeyStorePassword=key111
secureTokenKeyStoreType=JCEKS
secureTokenKeyPairAlias=keypair1
secureTokenKeyPairPassword=keypair1
secureTokenSecretKeyAlias=seckey1
secureTokenSecretKeyPassword=seckey1
secureTokenCipherAlgorithm=DES
secureTokenSignAlgorithm=RSA
```

Configuração

Consulte Propriedades do servidor para obter mais informações sobre as propriedades que você usa para configurar o gerenciador de token seguro.

Tarefas relacionadas:

8.6+ “Ativando Autenticação LDAP nos Servidores de Catálogos e de Contêineres do eXtreme Scale” na página 780
Ative seus servidores WebSphere eXtreme Scale e servidores de catálogos para autenticação Lightweight Directory Access Protocol (LDAP) com um arquivo de políticas Java Authentication and Authorization Service (JAAS) utilizado para autorização.

“Autenticando e Autorizando Clientes”
É possível ativar a segurança e a autenticação de credencial para autenticar clientes. Além disso, é possível autorizar clientes administrativos para acessar a grade de dados.

“Autenticando Aplicativos Clientes” na página 772
A autenticação de cliente do aplicativo consiste em ativar a autenticação de credencial e de segurança cliente/servidor e de configurar um autenticador e um gerador de credencial de sistema.

“Autorizando Aplicativos Clientes” na página 774
A autorização do cliente do aplicativo consiste de classes de permissão do ObjectGrid, de mecanismos de autorização, de um período de verificação de permissão e de autorização de acesso apenas pelo criador.

8.6+ “Autorizando Clientes Administrativos” na página 778
Por meio da segurança administrativa, você pode autorizar os usuários a acessar a grade de dados. Algumas condições são necessárias, dependendo de seu ambiente de instalação do WebSphere eXtreme Scale e dos usuários que você deseja que tenham acesso.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Classe ClientSecurityConfigurationFactory

Autenticando e Autorizando Clientes

É possível ativar a segurança e a autenticação de credencial para autenticar clientes. Além disso, é possível autorizar clientes administrativos para acessar a grade de dados.

Conceitos relacionados:

"Autenticação da Grade de Dados" na página 768
É possível utilizar o plug-in do gerenciador de token seguro para ativar a autenticação servidor-para-servidor, que requer que você implemente a interface SecureTokenManager.

"Segurança da Grade de Dados" na página 769
A segurança da grade de dados garante que um servidor que está se juntando tenha as credenciais certas, de modo que um servidor malicioso não possa juntar-se à grade de dados. A segurança da grade de dados usa um mecanismo de sequência de segredo compartilhado.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Classe ClientSecurityConfigurationFactory

Autenticando Aplicativos Clientes

A autenticação de cliente do aplicativo consiste em ativar a autenticação de credencial e de segurança cliente/servidor e de configurar um autenticador e um gerador de credencial de sistema.

Procedimento

- Ative a segurança de cliente/servidor

  A segurança deve ser ativada no cliente e no servidor para poder autenticar-se com êxito com o ObjectGrid.

  1. Ative a segurança de cliente.

     O WebSphere eXtreme Scale fornece um arquivo de amostra de propriedade do cliente, o arquivo `sampleClient.properties`, no diretório de instalação *was_root*`/optionalLibraries/ObjectGrid/properties` do WebSphere Application Server ou no diretório `/ObjectGrid/properties` em uma instalação do servidor combinada. É possível modificar este arquivo de gabarito com valores apropriados. Configure a propriedade **`securityEnabled`** no arquivo `objectgridClient.properties` para `true`. A propriedade **`securityEnabled`** indica se a segurança está ativada. Quando um cliente se conecta a um servidor, os valores no lado do cliente e do servidor devem ser ambos `true` ou ambos `false`. Por exemplo, se a segurança do servidor conectado estiver ativada, o valor da propriedade deverá ser configurado como `true` na lado do cliente para que o cliente se conecte ao servidor.

     A interface com.ibm.websphere.objectgrid.security.config.ClientSecurityConfiguration representa o arquivo `security.ogclient.props`. É possível usar a API pública com.ibm.websphere.objectgrid.security.config.ClientSecurityConfigurationFactory para criar uma instância desta interface com valores padrão ou criar uma instância passando o perfil de propriedade de segurança do cliente do ObjectGrid. O arquivo `security.ogclient.props` contém outras propriedades. Consulte a Documentação da API ClientSecurityConfiguration e a Documentação da API ClientSecurityConfigurationFactory para obter mais detalhes.

  2. Ative a segurança do servidor.

     Para ativar a segurança no lado do servidor, é possível configurar a propriedade **`securityEnabled`** no arquivo `security.xml` para `true`. Use um arquivo XML do descritor de segurança para especificar a configuração de

segurança da grade de dados para isolar a configuração de segurança de toda a grade da configuração sem segurança.

- Ative a autenticação de credencial.

  Após o cliente do eXtreme Scale recuperar o objeto Credential usando o objeto CredentialGenerator, o objeto Credential é enviado juntamente com o pedido do cliente para o servidor eXtreme Scale. O servidor autentica o objeto Credential antes de processar o pedido. Se o objeto Credential for autenticado com êxito, um objeto Subject será retornado para representar este objeto Credential. Este objeto Subject é, então, usado para autorizar o pedido.

  Configure a propriedade **credentialAuthentication** nos arquivos de propriedades do cliente e do servidor para ativar a autenticação de credencial. Para obter mais informações, consulte Arquivo de Propriedades do Cliente e Arquivo de Propriedades do Servidor.

  As tabelas a seguir exibem qual mecanismo de autenticação será utilizado em diferentes configurações.

Tabela 27. Autenticação de credencial nas configurações do cliente e do servidor

Autenticação de Credencial do Cliente	Autenticação de Credencial do Servidor	Resultado
Não	Nunca	Desativado
Não	Suportado	Desativado
Não	Necessário	Error case
Suportado	Nunca	Desativado
Suportado	Suportado	Ativada
Suportado	Necessário	Ativada
Necessário	Nunca	Error case
Necessário	Suportado	Ativada
Necessário	Necessário	Ativada

- Configure um autenticador.

  O servidor eXtreme Scale usa o plug-in do Autenticador para autenticar o objeto Credential. Uma implementação da interface do Autenticador obtém o objeto Credential e, em seguida, autentica-o para um registro do usuário, por exemplo, um servidor Lightweight Directory Access Protocol (LDAP) e assim por diante. O eXtreme Scale não fornece uma configuração de registro. A conexão com um registro do usuário e a autenticação nele devem ser implementadas neste plug-in.

  Por exemplo, uma implementação do Autenticador extrai o ID do usuário e a senha da credencial, usa-os para conectar e validar um servidor LDAP e cria um objeto Subject como resultado da autenticação. A implementação pode utilizar os módulos de login do Java Authentication and Authorization Service (JAAS). Um objeto Subject é retornado como resultado da autenticação.

  É possível configurar o autenticador no arquivo XML descritor de segurança, como mostra o seguinte exemplo:

```
<?xml version="1.0" encoding="UTF-8"?>
<securityConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config/security
../objectGridSecurity.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config/security">

 <security securityEnabled="true" loginSessionExpirationTime="300" >

  <authenticator className ="com.ibm.websphere.objectgrid.security.plugins.
builtins.KeyStoreLoginAuthenticator">
```

```
        </authenticator>

 </security>

</securityConfig>
```

Use a opção **-clusterSecurityFile** ao iniciar um servidor seguro para configurar o arquivo XML de segurança. Consulte o "Tutorial de Segurança do Java SE - Etapa 2" na página 22 para obter amostras sobre como iniciar um servidor seguro.

- Configure um gerador de credencial do sistema.

  O gerador de credenciais do sistema é utilizado para representar um factory para a credencial do sistema. Uma credencial de sistema é semelhante para uma credencial de administrador. É possível configurar o elemento SystemCredentialGenerator no arquivo XML de segurança de catálogo, conforme mostrado no seguinte exemplo:

  ```
  <systemCredentialGenerator className ="com.ibm.websphere.objectgrid.security.plugins.
   builtins.UserPasswordCredentialGenerator">
            <property name="properties"
  type="java.lang.String" value="manager manager1"
        description="username password" />
   </systemCredentialGenerator>
  ```

  Para demonstração, o nome de usuário e senha são armazenados em texto limpo. Não armazene o nome de usuário e senha em texto limpo em um ambiente de produção.

  O WebSphere eXtreme Scale fornece um gerador de credencial de sistema padrão, que usa as credenciais do servidor. Se você não especificar explicitamente o gerador de credencial de sistema, este gerador de credencial de sistema padrão é usado.

Conceitos relacionados:

"Autenticação da Grade de Dados" na página 768
É possível utilizar o plug-in do gerenciador de token seguro para ativar a autenticação servidor-para-servidor, que requer que você implemente a interface SecureTokenManager.

"Segurança da Grade de Dados" na página 769
A segurança da grade de dados garante que um servidor que está se juntando tenha as credenciais certas, de modo que um servidor malicioso não possa juntar-se à grade de dados. A segurança da grade de dados usa um mecanismo de sequência de segredo compartilhado.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Classe ClientSecurityConfigurationFactory

Autorizando Aplicativos Clientes

A autorização do cliente do aplicativo consiste de classes de permissão do ObjectGrid, de mecanismos de autorização, de um período de verificação de permissão e de autorização de acesso apenas pelo criador.

Sobre Esta Tarefa

Para o eXtreme Scale, a autorização se baseia no objeto Subject e nas permissões. O produto suporta dois tipos de mecanismos de autorização: Java Authentication and Authorization Service (JAAS) e autorização customizada.

A seguir há quatro tipos diferentes de classes de permissão.

- A classe MapPermission representa permissões para acessar os dados nos mapas de ObjectGrid.
- A classe ObjectGridPermission representa permissões para acessar o ObjectGrid.
- A classe ServerMapPermission representa permissões para acessar mapas de ObjectGrid no lado do servidor a partir de um cliente.
- A classe AgentPermission representa permissões para iniciar um agente no lado do servidor.

Para obter mais informações,consulte "Programação de Autorização de Cliente" na página 827.

Procedimento

1. Configure o período de verificação da permissão.

   O eXtreme Scale suporta armazenamento em cache dos resultados da verificação de permissão de mapa por motivo de desempenho. Sem este mecanismo, quando um método que está na lista de métodos para sua classe de permissão específica é chamado, o tempo de execução chama o mecanismo de autorização configurado para autorizar o acesso. Com este período de verificação de permissão configurado, o mecanismo de autorização é chamado periodicamente com base no período de verificação de permissão. Para obter uma lista de métodos para cada classe de permissão, consulte o "Programação de Autorização de Cliente" na página 827.

   As informações de autorização da permissão são baseadas no objeto Subject. Quando um cliente tenta acessar os métodos, o tempo de execução do eXtreme Scale consulta o cache com base no objeto Subject. Se o objeto não puder ser localizado no cache, o tempo de execução verifica as permissões concedidas para este objeto Subject, e, então, armazena as permissões em um cache.

   O período de verificação de permissão deve ser definido antes da inicialização do ObjectGrid. O período de verificação de permissão pode ser configurado de duas maneiras:

   É possível utilizar o arquivo XML do ObjectGrid para definir um ObjectGrid e configurar o período de verificação de permissão. No exemplo a seguir, o período de verificação de permissão é configurado para 45 segundos:

```
<objectGrids>
 <objectGrid name="secureClusterObjectGrid" securityEnabled="true"
 authorizationMechanism="AUTHORIZATION_MECHANISM_JAAS"
 permissionCheckPeriod="45">
  <bean id="bean id="TransactionCallback"
className="com.ibm.websphere.samples.objectgrid.HeapTransactionCallback" />
...
</objectGrids>
```

   Se desejar criar um ObjectGrid com APIs, chame o seguinte método para configurar o período de verificação de permissão. Este método pode ser chamado apenas antes da inicialização da instância do ObjectGrid. Este método se aplica apenas ao modelo de programação do eXtreme Scale local quando você utiliza a instância do ObjectGrid diretamente.

```
/**
 * This method takes a single parameter indicating how often you
 * want to check the permission used to allow a client access. If the
 * parameter is 0 then every single get/put/update/remove/evict call
 * asks the authorization mechanism, either JAAS authorization or custom
 * authorization, to check if the current subject has permission. This might be
 * prohibitively expensive from a performance point of view depending on
 * the authorization implementation, but if you need to have ever call check the
 * authorization mechanism, then set the parameter to 0.
 * Alternatively, if the parameter is > 0 then it indicates the number
 * of seconds to cache a set of permissions before returning to
 * the authorization mechanism to refresh them. This value provides much
 * better performance, but if the back-end
 * permissions are changed during this time then the ObjectGrid can
 * allow or prevent access even though the back-end security
 * provider was modified.
```

```
     *
     * @param period the permission check period in seconds.
     */
    void setPermissionCheckPeriod(int period);
```

2. Configure a autorização de acesso apenas pelo criador.

   A autorização de acesso apenas pelo criador garante que apenas o usuário (representado pelos objetos Principal associados a ele) que insere a entidade no mapa ObjectGrid possa acessar (ler, atualizar, invalidar e remover tal entrada.

   O modelo existente de autorização do mapa do ObjectGrid é baseado no tipo de acesso mas não em entradas de dados. Em outras palavras, um usuário possui um tipo de acesso específico, tal como read, write, insert, delete ou invalidate, para todo os dados no mapa ou em nenhum dos dados. Entretanto, o eXtreme Scale não autoriza usuários para a entrada de dados individual. Este recurso oferece uma nova maneira de autorizar usuários para entradas de dados.

   Em um cenário onde usuários diferentes acessam diferentes conjuntos de dados, este modelo pode ser útil. Quando o usuário carrega dados do armazenamento persistente nos mapas do ObjectGrid, o acesso pode ser autorizado pelo armazenamento persistente. Neste caso, não há necessidade de outra autorização na camada do mapa do ObjectGrid. É necessário apenas garantir que a pessoa que carrega os dados no mapa possa acessá-lo, permitindo o recurso de acesso apenas pelo criador.

   Valores de atributos do modo apenas do criador:

   desativada
   O recurso de acesso apenas pelo criador é desativado.

   complement
   O recurso de acesso apenas pelo criador é ativado para complementar a autorização do mapa. Em outras palavras, a autorização de mapa e o recurso de acesso apenas pelo criador serão efetivados. Portanto, é possível limitar ainda mais as operações nos dados. Por exemplo, o criador não pode invalidar os dados.

   supersede
   O recurso de acesso apenas pelo criador é ativado para substituir a autorização do mapa. Em outras palavras, o recurso de acesso apenas pelo criador substituirá a autorização do mapa e nenhuma autorização de mapa será feita.

   a. Configure o modo de acesso apenas pelo criador com um arquivo XML.

      É possível utilizar o arquivo XML do ObjectGrid para definir um ObjectGrid e configurar o acesso de modo apenas pelo criador para `disabled`, `complement` ou `supersede`, como mostra o seguinte exemplo:

```
<objectGrids>
    <objectGrid name="secureClusterObjectGrid" securityEnabled="true"
        accessByCreatorOnlyMode="supersede"
        <bean id="TransactionCallback"
              classname="com.ibm.websphere.samples.objectgrid.HeapTransactionCallback" />
    ...
</objectGrids>
```

   b. Configure o modo de acesso apenas pelo criador programaticamente.

      Se desejar criar um ObjectGrid programaticamente, é possível chamar o método a seguir para configurar o modo de acesso apenas pelo criador. A chamada deste método aplica-se somente ao modelo de programação local do eXtreme Scale quando você instancia diretamente a instância do ObjectGrid:

```
/**
 * Set the "access by creator only" mode.
 * Enabling "access by creator only" mode ensures that only the user (represented
 * by the Principals associated with it), who inserts the record into the map,
 * can access (read, update, invalidate, and remove) the record.
```

```
 * The "access by creator only" mode can be disabled, or can complement the
 * ObjectGrid authorization model, or it can supersede the ObjectGrid
 * authorization model. The default value is disabled:
 * {@link SecurityConstants#ACCESS_BY_CREATOR_ONLY_DISABLED}.
 * @see SecurityConstants#ACCESS_BY_CREATOR_ONLY_DISABLED
 * @see SecurityConstants#ACCESS_BY_CREATOR_ONLY_COMPLEMENT
 * @see SecurityConstants#ACCESS_BY_CREATOR_ONLY_SUPERSEDE
 *
 * @param accessByCreatorOnlyMode the access by creator mode.
 *
 * @since WAS XD 6.1 FIX3
*/
void setAccessByCreatorOnlyMode(int accessByCreatorOnlyMode);
```

Para ilustrar ainda mais, considere um cenário no qual uma conta de mapa do ObjectGrid está em uma grade financeira e Manager1 e o Employee1 são os dois usuários. A política de autorização do eXtreme Scale concede todas as permissões de acesso para o Manager1 e apenas a permissão de acesso de leitura para o Employee1. A política do JAAS para a autorização do mapa do ObjectGrid é mostrada no seguinte exemplo:

```
grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
    Principal com.acme.PrincipalImpl "Manager1" {
    permission com.ibm.websphere.objectgrid.security.MapPermission
        "banking.account", "all"
};
grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
    Principal com.acme.PrincipalImpl "Employee1" {
    permission com.ibm.websphere.objectgrid.security.MapPermission
        "banking.account", "read, insert"
};
```

Lembre-se: Considere como o recurso de acesso apenas pelo criador afeta a autorização:

- **`disabled`** Se o recurso de acesso apenas pelo criador estiver desativado, a autorização de mapa não é diferente. O usuário "Manager1" pode acessar todos os dados no mapa "account". O usuário "Employee1" pode ler e inserir todos os dados no mapa, mas não pode atualizar, invalidar e remover nenhum dado no mapa.
- **`complement`** Se o recurso de acesso apenas pelo criador estiver ativado com a opção "complement", a autorização de mapa e a autorização de acesso apenas pelo criador estarão em vigor. O usuário "Manager1" pode acessar os dados no mapa "account", mas apenas se o usuário sozinho os carregou no mapa. O usuário "Employee1" pode ler os dados no mapa "account", mas apenas se tal usuário sozinho os carregou no mapa. (Entretanto, este usuário não pode atualizar, invalidar ou remover dados no mapa).
- **`supersede`** Se o recurso de acesso apenas pelo criador estiver ativado com a opção "supersede", a autorização do mapa não será imposta. A autorização de acesso apenas pelo criador será a política apenas de autorização. O usuário "Manager1" possui o mesmo privilégio que no modo "complement": este usuário pode acessar os dados no mapa "account" apenas se o mesmo usuário carregou os dados no mapa. Entretanto, o usuário "Employee1" agora possui acesso total aos dados no mapa "account" se este usuários os carregou no mapa. Em outras palavras, a política de autorização definida na política do Java Authentication and Authorization Service (JAAS) não será imposta.

Conceitos relacionados:

"Autenticação da Grade de Dados" na página 768
É possível utilizar o plug-in do gerenciador de token seguro para ativar a autenticação servidor-para-servidor, que requer que você implemente a interface SecureTokenManager.

"Segurança da Grade de Dados" na página 769
A segurança da grade de dados garante que um servidor que está se juntando tenha as credenciais certas, de modo que um servidor malicioso não possa juntar-se à grade de dados. A segurança da grade de dados usa um mecanismo de sequência de segredo compartilhado.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Classe ClientSecurityConfigurationFactory

Autorizando Clientes Administrativos

Por meio da segurança administrativa, você pode autorizar os usuários a acessar a grade de dados. Algumas condições são necessárias, dependendo de seu ambiente de instalação do WebSphere eXtreme Scale e dos usuários que você deseja que tenham acesso.

Sobre Esta Tarefa

Quando usuários estão autorizados a acessar uma grade de dados do WebSphere eXtreme Scale, esses usuários também podem ser autorizados a executar operações de gerenciamento usando o comando **xscmd** ou o comando **stopOgServer**. A maioria dos implementadores de grade de dados restringem o acesso administrativo apenas a um subconjunto dos usuários que podem acessar os dados da grade.

Procedimento

1. Configure autorização para operações **xscmd** e o comando **stopOgServer**.

   Se você usar o comando a seguir para acessar a grade de dados, também poderá ser autorizado a executar as ações administrativas, como executar o comando **listAllJMXAddresses**:

   ```
   ./xscmd.sh -user <user> -password <password> <other_parameters>
   ```

   Se o usuário puder executar o comando anterior, então, qualquer operação **xscmd** ou o comando **stopOgServer** também poderão ser executados pelo mesmo usuário.

   Quando componentes eXtreme Scale são executados com o WebSphere Application Server, use o console administrativo do WebSphere Application Server para ativar o gerenciador de segurança. Para restringir acesso do aplicativo a recursos locais, clique em **Segurança** > **Segurança Global** e selecione as caixas de seleção **Ativar Segurança Administrativa** e **Usar Java 2 Security** para restringir o acesso do aplicativo a recursos locais.

   O acesso às operações de gerenciamento é controlado pelo gerenciador de segurança do WebSphere Application Server e é concedido apenas aos usuários que pertencem à função de Administrador do WebSphere. Você deve executar o comando **xscmd** e o comando **stopOgServer** a partir do diretório do WebSphere Application Server.
2. Configure a autorização administrativa em instalações independentes.

Quando componentes do eXtreme Scale são executados em um ambiente independente, etapas adicionais são necessárias para implementar a segurança administrativa. Você deve executar os servidores de catálogos e servidores de contêiner usando o gerenciador de segurança Java, o que requer um arquivo de políticas.

O arquivo de políticas é semelhante ao exemplo a seguir:

Lembre-se: O arquivo de política geralmente também contém entradas MapPermission, conforme documentado em "Tutorial de Segurança do Java SE - Etapa 5" na página 30.

```
grant codeBase "file:${objectgrid.home}/lib/*" {
permission java.security.AllPermission;
};

grant principal javax.security.auth.x500.X500Principal "CN=manager,O=acme,OU=OGSample" {
permission javax.management.MBeanPermission "*", "getAttribute,setAttribute,invoke,queryNames";
};
```

Se o cliente for um aplicativo Java Spring, a entrada `AgentPermission` a seguir é necessária no arquivo de políticas para permitir que a conta `CN=manager` acesse a grade de dados a partir do cliente do Spring.

```
grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
principal javax.security.auth.x500.X500Principal "CN=manager,O=acme,OU=OGSample" {
permission com.ibm.websphere.objectgrid.security.AgentPermission "*",
"com.ibm.ws.objectgrid.spring.PutAgent";
};
```

Neste exemplo, somente o gerente principal está autorizado para operações administrativas com o comando **xscmd** ou o comando **stopOgServer**. É possível incluir outras linhas conforme necessário para fornecer mais permissões de MBean principais. Um tipo diferente de principal é necessário se você usa autenticação LDAP.

Digite o seguinte comando: UNIX Linux

```
startOgServer.sh <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
-Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=$OBJECTGRID_HOME
```

UNIX Linux 8.6+

```
startXsServer.sh <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
-Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=$OBJECTGRID_HOME
```

Windows

```
startOgServer.bat <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
-Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=%OBJCTGRID_HOME%
```

Windows 8.6+

```
startXsServer.bat <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
 -Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=%OBJCTGRID_HOME%
```

Conceitos relacionados:

"Autenticação da Grade de Dados" na página 768
É possível utilizar o plug-in do gerenciador de token seguro para ativar a autenticação servidor-para-servidor, que requer que você implemente a interface SecureTokenManager.

"Segurança da Grade de Dados" na página 769
A segurança da grade de dados garante que um servidor que está se juntando tenha as credenciais certas, de modo que um servidor malicioso não possa juntar-se à grade de dados. A segurança da grade de dados usa um mecanismo de sequência de segredo compartilhado.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Classe ClientSecurityConfigurationFactory

Ativando Autenticação LDAP nos Servidores de Catálogos e de Contêineres do eXtreme Scale

Ative seus servidores WebSphere eXtreme Scale e servidores de catálogos para autenticação Lightweight Directory Access Protocol (LDAP) com um arquivo de políticas Java Authentication and Authorization Service (JAAS) utilizado para autorização.

Sobre Esta Tarefa

Nesta tarefa, você utiliza LDAP como um mecanismo de autenticação que fornece acesso à grade de dados, de acordo com as permissões que você configura no arquivo de configuração da política de autorização JAAS.

Procedimento

1. Crie um arquivo `wxs_ldap.config`; por exemplo:

```
LDAPLogin {
 com.ibm.websphere.objectgrid.security.plugins.builtins.SimpleLDAPLoginModule required
 providerURL="ldap://yourldapserver.yourcompany.com:389/"
 factoryClass="com.sun.jndi.ldap.LdapCtxFactory"
};
```

2. Crie um arquivo `wxs_ldap.auth.config`. Substitua o proprietário pelo usuário que efetua login na grade de dados. Além disso, substitua `YourGridName` pelo nome de sua grade de dados. Repita esta etapa conforme necessário para usuários e grades de dados adicionais. Consulte o seguinte exemplo:

```
grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
    principal javax.security.auth.x500.X500Principal "CN=manager,O=acme,OU=sample" {
    permission com.ibm.websphere.objectgrid.security.MapPermission "*.*", "all";

    permission com.ibm.websphere.objectgrid.security.ObjectGridPermission "*.*", "all";
};
```

   Alternativamente, você pode conceder permissão para todas as grades de dados; por exemplo:

```
grant codebase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
    principal javax.security.auth.x500.X500Principal "CN=manager,O=acme,OU=sample" {
    permission com.ibm.websphere.objectgrid.security.MapPermission "*", "all";

    permission com.ibm.websphere.objectgrid.security.ObjectGridPermission "*", "all";
};
```

3. Crie um arquivo `security.xml` do lado do servidor; por exemplo:

```
<?xml version="1.0" encoding="UTF-8"?>
<securityConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config/security
../objectGridSecurity.xsd"
xmlns="http://ibm.com/ws/objectgrid/config/security">
<security securityEnabled="true" loginSessionExpirationTime="300" >
        <authenticator className ="com.ibm.websphere
.plugins.builtins.LDAPAuthenticator">
        </authenticator>
    </security>
</securityConfig>
```

4. Edite seu arquivo `objectGridServer.properties` com as propriedades a seguir. Se você não tiver um arquivo `objectGridServer.properties`, poderá usar o arquivo `sampleServer.properties` que está no diretório *wxs_home*`/properties` para criar seu arquivo de propriedades.

```
securityEnabled=true

credentialAuthentication=Required
```

5. Inicie seus servidores de catálogos.

   Reprovado: 8.6+ Os comandos **startOgServer** e **stopOgServer** iniciam servidores que usam o mecanismo de transporte do Object Request Broker (ORB). O ORB foi descontinuado, mas você pode continuar utilizando esses scripts se estava utilizando o ORB em uma liberação anterior. O mecanismo de transporte do IBM eXtremeIO (XIO) substitui o ORB. Use os scripts **startXsServer** e **stopXsServer** para iniciar e parar os servidores que utilizam o transporte XIO.

   ```
   -Dobjectgrid.cluster.security.url=file:///security/security.xml
   -Dobjectgrid.server.props="/security/objectGridServer.properties"
   -Djava.security.policy="/security/wxs_ldap_auth.config"
   ```

   Para iniciar seus servidores de catálogos no WebSphere Application Server, consulte “Ativando Autenticação LDAP nos Servidores de Catálogos e de Contêineres do eXtreme Scale” na página 780.

6. Inicie seus servidores de contêiner.

   ```
   Dobjectgrid.server.props="/security/objectGridServer.properties"
   -Djava.security.policy="/security/wxs_ldap_auth.config"
   ```

   Para iniciar seus servidores de contêineres no WebSphere Application Server, consulte “Ativando Autenticação LDAP nos Servidores de Catálogos e de Contêineres do eXtreme Scale” na página 780.

7. Edite seu arquivo `objectGridClient.properties` do lado do cliente. Se WebSphere Application Server é o cliente, o arquivo que você atualiza é *was_profile_dir*`/properties`.

   ```
   securityEnabled=true

   credentialAuthentication=Supported
   ```

8. Configure seu cliente para passar as credenciais de login de LDAP necessárias. Carregue um arquivo de propriedades do cliente. Esse arquivo pode conter o ID do usuário e a senha. Se o arquivo de propriedades não incluir o ID do usuário e a senha, inclua os mesmos na configuração do programa cliente. No exemplo a seguir, um arquivo de propriedades do cliente é carregado usando um parâmetro de programa. Em seguida, o ID do usuário e a senha são incluídos na configuração.

```
String userid = "CN=manager,O=acme,OU=sample";

String pw="password";

// Creates a ClientSecurityConfiguration object using the specified file
ClientSecurityConfiguration clientSC = ClientSecurityConfigurationFactory
.getClientSecurityConfiguration(args[0]);

//Creates a CredentialGenerator using the user and password.
CredentialGenerator credGen = new UserPasswordCredentialGenerator(userid,password);
clientSC.setCredentialGenerator(credGen);

// Create an ObjectGrid by connecting to the catalog server
ClientClusterContext ccContext =
ogManager.connect("cataloghostname:2809", clientSC, null);
ObjectGrid og = ogManager.getObjectGrid(ccContext, "YourGridName");'
```

Conceitos relacionados:

"Autenticação da Grade de Dados" na página 768
É possível utilizar o plug-in do gerenciador de token seguro para ativar a autenticação servidor-para-servidor, que requer que você implemente a interface SecureTokenManager.

"Segurança da Grade de Dados" na página 769
A segurança da grade de dados garante que um servidor que está se juntando tenha as credenciais certas, de modo que um servidor malicioso não possa juntar-se à grade de dados. A segurança da grade de dados usa um mecanismo de sequência de segredo compartilhado.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Classe ClientSecurityConfigurationFactory

Ativando Autenticação de Keystore nos Servidores de Contêineres e de Catálogos do eXtreme Scale

Ative seus servidores do WebSphere eXtreme Scale e servidores de catálogos para autenticação de keystore com um arquivo de políticas de Java Authentication and Authorization Service (JAAS) usado para autorização.

Sobre Esta Tarefa

Nesta tarefa, você usa um arquivo keystore como um mecanismo de autenticação que fornece acesso à grade de dados, de acordo com as permissões configuradas no arquivo de configuração de política de autorização JAAS.

Procedimento

1. Crie um keystore com aliases de login conforme descrito no "Tutorial de Segurança do Java SE - Etapa 4" na página 26.
2. Crie um arquivo `wxs_keystore.config`. Substitua o proprietário pelo usuário que efetua login na grade de dados. Além disso, substitua `YourGridName` pelo nome de sua grade de dados. Repita essa etapa conforme necessário para mais usuários e grades de dados. Consulte o seguinte exemplo:

```
KeyStoreLogin {
com.ibm.websphere.objectgrid.security.plugins.builtins.KeyStoreLoginModule required
keyStoreFile="/security/sampleKS.jks";

}
```

3. Crie um arquivo `security.xml` do lado do servidor; por exemplo:

```
<?xml version="1.0" encoding="UTF-8"?>
<securityConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://ibm.com/ws/objectgrid/config/security
../objectGridSecurity.xsd"
xmlns="http://ibm.com/ws/objectgrid/config/security">
<security securityEnabled="true" loginSessionExpirationTime="300" >
        <authenticator className="com.ibm.websphere.objectgrid.security.plugins.
builtins.KeyStoreLoginAuthenticator>
        </authenticator>
    </security>
</securityConfig>
```

4. Edite seu arquivo `objectGridServer.properties` com as propriedades a seguir. Se você não tiver um arquivo `objectGridServer.properties`, poderá usar o arquivo `sampleServer.properties` que está no diretório *wxs_home*`/properties` para criar seu arquivo de propriedades. Para obter informações adicionais, consulte Configurando o Mecanismo Quorum.

```
securityEnabled=true

credentialAuthentication=Required
```

5. Inicie seus servidores de catálogos.

Reprovado: 8.6+ Os comandos **startOgServer** e **stopOgServer** iniciam servidores que usam o mecanismo de transporte do Object Request Broker (ORB). O ORB foi descontinuado, mas você pode continuar utilizando esses scripts se estava utilizando o ORB em uma liberação anterior. O mecanismo de transporte do IBM eXtremeIO (XIO) substitui o ORB. Use os scripts **startXsServer** e **stopXsServer** para iniciar e parar os servidores que utilizam o transporte XIO.

```
startOgServer.sh catalogServer -clusterSecurityFile /security/security.xml
-serverProps /security/objectGridServer.properties -jvmArgs
-Djava.security.auth.login.config="/security/wxs_keystore.config"

-Djava.security.policy="/security/wxs_ldap_auth.config"
```

8.6+

```
startXsServer.sh catalogServer -clusterSecurityFile /security/security.xml
-serverProps /security/objectGridServer.properties -jvmArgs
-Djava.security.auth.login.config="/security/wxs_keystore.config"

-Djava.security.policy="/security/wxs_ldap_auth.config"
```

6. Inicie seus servidores de contêiner.

```
startOgServer.sh c0 -objectgridFile /xml/objectgrid.xml
-deploymentPolicyFile /xml/deployment.xml
-catalogServiceEndPoints cataloghostname:2809
-serverProps /security/objectGridServer.properties
-jvmArgs -Djava.security.auth.login.config="/security/wxs_keystore.config"

-Djava.security.policy="/security/wxs_ldap_auth.config"
```

8.6+

```
startXsServer.sh c0 -objectgridFile /xml/objectgrid.xml
-deploymentPolicyFile /xml/deployment.xml
-catalogServiceEndPoints cataloghostname:2809
-serverProps /security/objectGridServer.properties
-jvmArgs -Djava.security.auth.login.config="/security/wxs_keystore.config"

-Djava.security.policy="/security/wxs_ldap_auth.config"
```

7. Edite seu arquivo objectGridClient.properties do lado do cliente. Se WebSphere Application Server é o cliente, o arquivo que você atualiza é *was_profile_dir*/properties.

```
securityEnabled=true

credentialAuthentication=Supported

transportType=TCP/IP

singleSignOnEnabled=false
```

8. Modifique o aplicativo cliente para transmitir as credenciais de login do keystore necessárias.

```
String userid = "CN=manager,O=acme,OU=sample";

String pw="password";
// Creates a ClientSecurityConfiguration object using the specified file
ClientSecurityConfiguration clientSC = ClientSecurityConfigurationFactory
.getClientSecurityConfiguration(args[0]);

// Creates a CredentialGenerator using the passed-in user and password.
CredentialGenerator credGen = new UserPasswordCredentialGenerator(userid,password);
clientSC.setCredentialGenerator(credGen);

// Create an ObjectGrid by connecting to the catalog server
ClientClusterContext ccContext =
ogManager.connect("cataloghostname:2809", clientSC, null);
ObjectGrid og = ogManager.getObjectGrid(ccContext, "YourGridName");'
```

Configurando Tipos de Transportes Seguros

A Segurança da Camada de Transporte (TLS) fornece comunicação segura entre o cliente e o servidor. O mecanismo de comunicação que é usado depende do valor do parâmetro **transportType** que é especificado nos arquivos de configuração do cliente e do servidor.

Sobre Esta Tarefa

Quando o Secure Sockets Layer (SSL) é usado, os parâmetros de configuração SSL devem ser fornecidos para o lado do cliente e também para o lado do servidor. Em um ambiente Java SE, a configuração SSL é configurada nos arquivos de propriedades do cliente ou servidor. Se o cliente ou servidor estiver no WebSphere Application Server, será possível usar as configurações de transporte do WebSphere Application Server CSIV2 existentes para os servidores de contêiner e clientes. Consulte o “Integração de Segurança com o WebSphere Application Server” na página 794 para obter informações adicionais.

Tabela 28. Protocolo de Transporte a Ser Utilizado nas Configurações de Transporte do Cliente e Transporte do Servidor.

Se as configurações transportType forem diferentes entre o cliente e o servidor, o protocolo resultante pode variar ou resultar em um erro.

Propriedade transportType do cliente	Propriedade transportType do servidor	Protocolo resultante
TCP/IP	TCP/IP	TCP/IP
TCP/IP	Suportado pelo SSL	TCP/IP
TCP/IP	Requerido pelo SSL	Erro
Suportado pelo SSL	TCP/IP	TCP/IP
Suportado pelo SSL	Suportado pelo SSL	SSL (se o SSL falhar, TCP/IP)
Suportado pelo SSL	Requerido pelo SSL	SSL

Tabela 28. Protocolo de Transporte a Ser Utilizado nas Configurações de Transporte do Cliente e Transporte do Servidor (continuação).

Se as configurações transportType forem diferentes entre o cliente e o servidor, o protocolo resultante pode variar ou resultar em um erro.

Propriedade transportType do cliente	Propriedade transportType do servidor	Protocolo resultante
Requerido pelo SSL	TCP/IP	Erro
Requerido pelo SSL	Suportado pelo SSL	SSL
Requerido pelo SSL	Requerido pelo SSL	SSL

Procedimento

1. Para configurar a propriedade **transportType** na configuração de segurança do cliente, consulte Arquivo de Propriedades do Cliente.
2. Para configurar a propriedade **transportType** na configuração de segurança do contêiner e do servidor de catálogos, consulte Arquivo de Propriedades do Servidor.

Transport Layer Security e Secure Sockets Layer

O WebSphere eXtreme Scale suporta TCP/IP e Transport Layer Security/Secure Sockets Layer (TLS/SSL) para a comunicação segura entre clientes e servidores.

Ativar TLS/SSL em Ambas as Direções

O TLS/SSL às vezes é ativado em uma direção. Por exemplo, apenas o certificado público do servidor é importado no armazenamento confiável do cliente, porém o certificado público do cliente não é importado no armazenamento confiável do servidor. Entretanto, o WebSphere eXtreme Scale usa amplamente os agentes da grade de dados. Uma característica de um agente da grade de dados é que quando o servidor envia respostas de volta para o cliente, uma nova conexão é criada. O servidor eXtreme Scale, em seguida, atua como um cliente. Portanto, você deve importar o certificado público do cliente no armazenamento confiável do servidor.

Ativar Segurança de Transporte para Oracle JDK

WebSphere eXtreme Scale requer o ExtensionJava Secure Sockets IBM (IBMJSSE) ou o IBM Java Secure Sockets Extension 2 (IBMJSSE2). Os provedores IBMJSSE e IBMJSSE2 contêm uma implementação de referência que suporta os protocolos SSL e TLS (Transport Layer Security) e uma estrutura de API (Application Programming Interface).

O Oracle JDK não envia provedores IBM JSSE e IBM JSSE2; portanto, a segurança de transporte não pode ser ativada com um Oracle JDK. Para fazer esse trabalho, é necessário um Oracle JDK enviado com WebSphere Application Server. O Oracle JDK enviado pelo WebSphere Application Server contém os provedores IBM JSSE e IBM JSSE2.

Consulte o Configurando um Object Request Broker Customizado para obter informações sobre o uso de um não IBM JDK para WebSphere eXtreme Scale. Se `-Djava.endorsed.dirs` estiver configurado, ele apontará para os diretórios `objectgridRoot/lib/endorsed` e `JRE/lib/endorsed`. O diretório `objectgridRoot/lib/endorsed` é necessário de modo que o IBM ORB seja utilizado e o diretório `JRE/lib/endorsed` é necessário para carregar os provedores IBM JSSE e IBM JSSE2.

Use o “Tutorial de Segurança do Java SE - Etapa 4” na página 26 para configurar as propriedades SSL necessárias, para criar os keystores e os armazenamentos confiáveis e para iniciar os servidores seguros no WebSphere eXtreme Scale.

Configurando os Parâmetros do Secure Sockets Layer (SSL) para Clientes ou Servidores

O modo com que os parâmetros SSL são configurados varia entre clientes e servidores.

Sobre Esta Tarefa

O TLS/SSL às vezes é ativado em uma direção. Por exemplo, o certificado público do servidor é importado no armazenamento confiável do cliente, mas o certificado público do cliente não é importado para o armazenamento confiável do servidor. Entretanto, o WebSphere eXtreme Scale usa amplamente os agentes da grade de dados. Uma característica de um agente de grade de dados é que quando o servidor envia resposta de volta para o cliente, ele cria uma conexão. O servidor eXtreme Scale, em seguida, atua como um cliente. Portanto, você deve importar o certificado público do cliente no armazenamento confiável do servidor.

Procedimento

- Configure os parâmetros SSL do cliente.

  Use uma das opções a seguir para configurar os parâmetros SSL no cliente:
  - Crie um objeto com.ibm.websphere.objectgrid.security.config.SSLConfiguration usando o com.ibm.websphere.objectgrid.security.config.ClientSecurityConfigurationFactory.
  - Configure os parâmetros no arquivo `client.properties`. Em seguida, é possível configurar o valor da propriedade como uma propriedade do cliente JVM ou usar as APIs do WebSphere eXtreme Scale. Passe o arquivo de propriedades no método ClientSecurityConfigurationFactory.getClientSecurityConfiguration(String) para o cliente e use o objeto retornado como um parâmetro para o método ObjectGridManager.connect(String, ClientSecurityConfiguration, URL).
- Configure os parâmetros SSL do servidor.

  Os parâmetros SSL são configurados para servidores usando o arquivo `server.properties`. Para iniciar um servidor de contêineres ou catálogos com um arquivo de propriedades específico, use o parâmetro **`-serverProps`** no script **`startOgServer`** ou **`startXsServer`**. Para obter mais informações sobre os parâmetros SSL, é possível configurar os servidores do eXtreme Scale, consulte Propriedades do Servidor de Segurança.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Segurança do Java Management Extensions (JMX)

É possível proteger chamadas de beans gerenciados (MBean) em um ambiente distribuído.

Para obter informações adicionais sobre os MBeans que estão disponíveis, consulte Administrando com Beans Gerenciados (MBeans).

Na topologia de implementação distribuída, MBeans são hospedados diretamente nos servidores de catálogos e nos servidores de contêiner. Em geral, a segurança de JMX em uma topologia distribuída segue a especificação de segurança do JMX conforme especificado na Especificação da Java Management Extensions (JMX). Ela consiste nas três partes a seguir:

1. Autenticação: O cliente remoto precisa ser autenticado no servidor do conector.
2. Controle de acesso: O controle de acesso do MBean limita quem pode acessar as informações do MBean e quem pode executar as operações do MBean.
3. Transporte seguro: O transporte entre o cliente JMX e o servidor pode ser protegido com TLS/SSL.

Autenticação

O JMX fornece métodos para os servidores conectores para autenticar os clientes remotos. Para o conector RMI, a autenticação é concluída ao fornecer um objeto que implementa a interface JMXAuthenticator quando o servidor conector é criado. Assim, o eXtreme Scale implementa essa interface JMXAuthenticator para usar o plug-in do Autenticador do ObjectGrid para autenticar os clientes remotos. Consulte “Tutorial de Segurança do Java SE - Etapa 2” na página 22 para obter detalhes sobre como o eXtreme Scale autentica um cliente.

O cliente JMX segue as APIs do JMX para fornecer credenciais para conectar-se com o servidor conector. . A estrutura JMX passa a credencial para o servidor do conector e, em seguida, chama a implementação do JMXAuthenticator para autenticação. Conforme descrito anteriormente, a implementação do JMXAuthenticator então delega a autenticação para a implementação do Autenticador do ObjectGrid.

Revise o exemplo a seguir que descreve como conectar-se a um servidor conector com uma credencial:

```
javax.management.remote.JMXServiceURL jmxUrl = new JMXServiceURL(
        "service:jmx:rmi:///jndi/rmi://localhost:1099/objectgrid/MBeanServer");

    environment.put(JMXConnector.CREDENTIALS, new UserPasswordCredential("admin", "xxxxxx"));

    // Create the JMXCconnectorServer
    JMXConnector cntor = JMXConnectorFactory.newJMXConnector(jmxUrl, null);

    // Connect and invoke an operation on the remote MBeanServer
    cntor.connect(environment);
```

No exemplo anterior, um objeto UserPasswordCredential é fornecido com o ID do usuário configurado para `admin` e a senha configurada para `xxxxx`. Este objeto UserPasswordCredential é configurado no mapa do ambiente, que é usado no método JMXConnector.connect(Map). Este objeto UserPasswordCredential é então passado para o servidor pela estrutura JMX e finalmente passado para a estrutura de autenticação do ObjectGrid para a autenticação.

O modelo de programação do cliente segue estritamente a especificação JMX.

Controle de Acesso

Um servidor MBean JMX pode ter acesso a informações sensitivas e pode executar operações sensitivas. O JMX fornece o controle de acesso necessário que identifica quais clientes podem acessar tais informações e quem pode executar tais operações. o controle de acesso é integrado no modelo de segurança Java padrão por meio da definição de permissões que controlam o acesso ao servidor MBean e às suas operações.

Para controle de acesso de operação ou autorização do JMX, oeXtreme Scale conta com o suporte de JAAS fornecido pela implementação JMX. Em qualquer ponto na execução de um programa, há um conjunto atual de permissões que um encadeamento de execuções retém. Quando um destes encadeamentos chama uma operação de especificação JMX, estas permissões são conhecidas como permissões retidas. Quando uma operação JMX é executada, uma verificação de segurança é feita para verificar se a permissão necessária é incluída pela permissão contida.

A definição de política do MBean segue o formato da política Java. Por exemplo, a política a seguir concede a todos os assinantes e a todas as bases de código o direito de recuperar o endereço JMX do servidor para o PlacementServiceMBean. Entretanto, os assinantes e as bases de código ficam restritos ao domínio com.ibm.websphere.objectgrid.

```
grant {
    permission javax.management.MBeanPermission
        "com.ibm.websphere.objectgrid.management.PlacementServiceMBean#ServerJMXAddress
 [com.ibm.websphere.objectgrid:*,type=PlacementService]",
        "invoke";
}
```

O exemplo de política a seguir pode ser utilizado para concluir a autorização baseada na identidade do cliente remoto. A política concede a mesma permissão MBean, conforme mostrado no exemplo anterior, exceto apenas para usuários com o nome X500Principal como:
`CN=Administrator,OU=software,O=IBM,L=Rochester,ST=MN,C=US`.

```
grant principal javax.security.auth.x500.X500Principal "CN=Administrator,OU=software,O=IBM,
    L=Rochester,ST=MN,C=US" {permission javax.management.MBeanPermission
        "com.ibm.websphere.objectgrid.management.PlacementServiceMBean#ServerJMXAddress
    [com.ibm.websphere.objectgrid:*,type=PlacementService]",
        "invoke";
}
```

As políticas do Java são verificadas somente se o gerenciador de segurança estiver ativado. Inicie os servidores de catálogos e servidores de contêineres com o argumento JVM -Djava.security.manager para forçar o controle de acesso da operação MBean.

Transporte Seguro

O transporte entre o cliente e o servidor JMX pode ser assegurado com o TLS/SSL. Se o transportType do servidor de catálogos ou servidor de contêiner for configurado como SSL_Required ou SSL_Supported, você deverá usar o SSL para conectar-se ao servidor JMX.

Para usar o SSL, você deve configurar o armazenamento confiável, o tipo de armazenamento confiável e a senha do armazenamento confiável no cliente MBean com as propriedades do sistema -D:

1. `-Djavax.net.ssl.trustStore=TRUST_STORE_LOCATION`
2. `-Djavax.net.ssl.trustStorePassword=TRUST_STORE_PASSWORD`
3. `-Djavax.net.ssl.trustStoreType=TRUST_STORE_TYPE`

Se com.ibm.websphere.ssl.protocol.SSLSocketFactory for usado como seu factory de soquete SSL em seu arquivo *java_home*`/jre/lib/security/java.security`, use as seguintes propriedades:

1. `-Dcom.ibm.ssl.trustStore=TRUST_STORE_LOCATION`
2. `-Dcom.ibm.ssl.trustStorePassword=TRUST_STORE_PASSWORD`
3. `-Dcom.ibm.ssl.trustStoreType=TRUST_STORE_TYPE`

Para obter essas informações quando o protocolo Segurança da Camada de Transporte/Secure Sockets Layer (TLS/SSL) estiver ativado nas configurações independentes, você deve iniciar os servidores de catálogos e de contêiner com o conjunto de portas de serviço JMX. Use um dos seguintes métodos para configurar a porta de serviço JMX:

- Use a opção **-JMXServicePort** no script **startOgServer** ou **startXsServer**.
- Se você estiver usando um servidor integrado, chame o método setJMXServicePort na interface ServerProperties para configurar a porta de serviço JMX.

O valor padrão para a porta de serviço JMX nos servidores de catálogos é `1099`. Você deve usar um número da porta diferente para cada JVM na configuração. Se desejar usar o JMX/RMI, especifique explicitamente a opção **-JMXServicePort** e o número da porta, mesmo se desejar usar o valor da porta padrão.

A configuração da porta de serviço JMX é requerida quando você deseja exibir informações do servidor de contêiner a partir do servidor de catálogos. Por exemplo, a porta é necessária quando estiver usando o comando **xscmd -c showMapSizes**.

Configure a porta do conector JMX para evitar a criação de porta efêmera. Use um dos métodos a seguir para configurar a porta do conector JMX.

- Use a opção **-JMXConnectorPort** no script **startOgServer** ou **startXsServer**.
- Se estiver usando um servidor integrado, chame o método setJMVConnectorPort na interface ServerProperties.

Integração de Segurança com Provedores Externos

Para proteger seus dados, o produto pode se integrar com vários provedores de segurança.

O WebSphere eXtreme Scale pode integrar-se a uma implementação de segurança externa. Esta implementação externa deve fornecer serviços de autenticação e autorização para o WebSphere eXtreme Scale. O WebSphere eXtreme Scale possui pontos de plug-in para integrar em uma implementação de segurança. O WebSphere eXtreme Scale foi integrado com sucesso nos seguintes componentes:

- LDAP (Lightweight Directory Access Protocol)
- Kerberos
- Segurança do ObjectGrid
- Tivoli Access Manager
- JAAS (Java Authentication and Authorization Service)

O eXtreme Scale utiliza o provedor de segurança para as seguintes tarefas:

- Autenticar clientes para servidores.
- Autorizar clientes para acessar determinados artefatos do eXtreme Scale ou para especificar o que pode ser feito com os artefatos do eXtreme Scale.

O eXtreme Scale possui os seguintes tipos de autorizações:

Autorização de mapa
Clientes ou grupos podem ser autorizados a executar operações de inserção, leitura, atualização, despejo ou exclusão nos mapas.

Autorização do ObjectGrid
Clientes ou grupos podem ser autorizados a executar consultas de objetos ou de entidades nos objectGrids.

Autorização do agente do DataGrid
Clientes ou grupos podem ser autorizados a permitir que os agentes DataGrid sejam implementados a um ObjectGrid.

Autorização de Mapa do Lado do Servidor
Clientes ou grupos podem ser autorizados a replicar um mapa do servidor no lado do cliente ou criar um índice dinâmico para o mapa do servidor.

Autorização de administração
Clientes ou grupos podem ser autorizados a executar tarefas de administração.

Nota: Se você já tiver a segurança ativada para seu backend, lembre-se de que estas configurações de segurança não são mais suficientes para proteger seus dados. As configurações de segurança do seu banco de dados ou outro datastore não são, de forma alguma, transferidas para o seu cache. É necessário proteger separadamente os dados que agora são armazenados em cache utilizando o mecanismo de segurança do eXtreme Scale, incluindo segurança no nível de autenticação, autorização e transporte.

Importante: Use um Development Kit ou Runtime Environment na Versão 1.6 e posterior para suportar a segurança do Transporte SSL com o WebSphere eXtreme Scale Versão 7.1.1 e posterior.

Protegendo o Serviço de Dados REST

Proteja vários aspectos do serviço de dados REST. O acesso ao serviço de dados REST do eXtreme Scale pode ser protegido por meio da autenticação e autorização. O acesso também pode ser controlado por regras de configuração com escopo definido de serviço, conhecidas como regras de acesso. A segurança de transporte é a terceira consideração.

Sobre Esta Tarefa

O acesso ao serviço de dados REST do eXtreme Scale pode ser protegido por meio da autenticação e autorização. A autenticação e a autorização são realizadas fazendo a integração com a segurança do eXtreme Scale.

O acesso também pode ser controlado por regras de configuração com escopo definido de serviço, conhecidas como regras de acesso. Existem dois tipos de regras de acesso: direitos de operação de serviço, que controlam as operações CRUD que são permitidas pelo serviço, e direitos de acesso de entidade, que controlam as operações CRUD que são permitidas para um tipo de entidade particular.

A segurança de transporte é fornecida pela configuração de contêiner hosting para conexões entre o cliente da web e o serviço REST. E a segurança de transporte é fornecida pela configuração de cliente eXtreme Scale (para serviço REST para conexões de grade de dados eXtreme Scale).

Procedimento

- Autenticação e autorização de controle.

O acesso ao serviço de dados REST do eXtreme Scale pode ser protegido por meio da autenticação e autorização. A autenticação e a autorização são realizadas pela integração com a segurança do eXtreme Scale.

O serviço de dados REST do eXtreme Scale usa a segurança do eXtreme Scale para autenticação e autorização, a fim de controlar quais usuários podem acessar o serviço e as operações que um usuário tem permissão para executar por meio do serviço. O serviço de dados REST do eXtreme Scale usa uma credencial global configurada, com usuário e senha, ou uma credencial derivada de um desafio HTTP BASIC que é enviado com cada transação para a grade do eXtreme Scale na qual a autenticação e a autorização são executadas.

1. Configure a autenticação e a autorização do cliente do eXtreme Scale na grade Consulte “Integração de Segurança com Provedores Externos” na página 789 para obter detalhes sobre como configurar a autenticação e a autorização do cliente do eXtreme Scale.
2. Configure o cliente do eXtreme Scale usado pelo serviço REST para segurança.

   O serviço de dados REST do eXtreme Scale chama a biblioteca do cliente do eXtreme Scale ao se comunicar com a grade do eXtreme Scale. Portanto, o cliente do eXtreme Scale deve ser configurado para a segurança do eXtreme Scale.

   A autenticação de cliente do eXtreme Scale é ativada por meio de propriedades no arquivo de propriedades do cliente objectgrid. No mínimo, os seguintes atributos devem ser ativados ao usar a segurança do cliente com o serviço REST:

   ```
   securityEnabled=true
   credentialAuthentication=Supported [-or-] Required
   credentialGeneratorProps=user:pass [-or-] {xor encoded user:pass}
   ```

   Lembre-se: O usuário e a senha especificados na propriedade credentialGeneratorProps devem ser mapeados para um ID no registro de autenticação e ter direitos de políticas do ObjectGrid suficientes para se conectar com, e criar, osObjectGrids.

   Um arquivo de política do cliente de objectgrid de amostra está localizado em *restservice_home*`/security/security.ogclient.properties`. Consulte também Arquivo de Propriedades do Cliente.
3. Configure o serviço de dados REST do eXtreme Scale para segurança.

   O arquivo de propriedades de configuração do serviço de dados REST do eXtreme Scale precisa conter as seguintes entradas para ser integrado com a segurança do eXtreme Scale:

   ```
   ogClientPropertyFile=file_name
   ```

   O ogClientPropertyFile é o local do arquivo de propriedades que contém propriedades do cliente de ObjectGrid mencionadas na etapa anterior. O serviço REST usa este arquivo para inicializar o cliente do eXtreme Scale para falar com a grade quando a segurança estiver ativada.

   ```
   loginType=basic [-or-] none
   ```

   A propriedade loginType configura o serviço REST para o tipo de login. Se um valor de `nenhum` for especificado, o ID do usuário e senha "globais " definidos por credentialGeneratorProps serão enviados para a grade para cada transação. Se um valor de `básico` for especificado, o serviço REST apresentará um desafio HTTP BASIC para o cliente solicitando credenciais que ele enviará em cada transação ao se comunicar com a grade.

   Para obter mais informações sobre as propriedades ogClientPropertyFile e loginType, consulte o Arquivo de Propriedades do Serviço de Dados REST.

- Aplique as regras de acesso.

  O acesso também pode ser controlado por regras de configuração com escopo definido de serviço, conhecidas como regras de acesso. Existem dois tipos de regras de acesso: direitos de operação de serviço, que controla as operações CRUD que são permitidas pelo serviço; e direitos de acesso de entidade, que controlam as operações CRUD que são permitidas para um tipo de entidade particular.

  O serviço de dados REST do eXtreme Scale permite, opcionalmente, regras de acesso que podem ser configuradas para restringir o acesso ao serviço e a entidades no serviço. Essas regras de acesso são especificadas no arquivo de propriedades de direitos de acesso do serviço REST. O nome deste arquivo é especificado no arquivo de propriedades do serviço de dados REST pela propriedade wxsRestAccessRightsFile. Para obter mais informações sobre essa propriedade, consulte Arquivo de Propriedades do Serviço de Dados REST. Este arquivo é um arquivo de propriedades Java típico com pares de chave e valor. Existem dois tipos de regras de acesso: direitos de operação de serviço, que controlam as operações CRUD que são permitidas pelo serviço; e direitos de acesso de entidade, que controlam as operações CRUD que são permitidas para um tipo de entidade particular.

  1. Configure os direitos de operação de serviço.

     Os direitos de operações de serviço especificam direitos de acesso que se aplicam a todos os ObjectGrids expostos por meio do serviço REST ou a todas as entidades de um ObjectGrid individual, conforme especificado.

     Use a seguinte sintaxe.

     ```
     serviceOperationRights=service_operation_right
     serviceOperationRights.grid_name -OR- *=service_operation_right
     ```

     em que

     – serviceOperationRights pode ser uma das opções a seguir: [NONE, READSINGLE, READMULTIPLE, ALLREAD, ALL]
     – serviceOperationRights.*grid_name -OR-* * implica que o direito de acesso se aplica a todos os ObjectGrids, também o nome de um ObjectGrid específico pode ser fornecido.

     Por exemplo:

     ```
     serviceOperationsRights=ALL
     serviceOperationsRights.*=NONE
     serviceOperationsRights.EMPLOYEEGRID=READSINGLE
     ```

     O primeiro exemplo especifica que todas as operações de serviço são permitidas para todos os ObjectGrids expostos por este Serviço REST. O segundo exemplo é semelhante ao primeiro, uma vez que também se aplica a todos os ObjectGrids expostos pelo serviço REST; no entanto, ele especifica o direito de acesso como NONE, o que significa que nenhuma das operações de serviço são permitidas nos ObjectGrids. O último exemplo especifica como controlar as operações de serviço para uma grade específica, aqui apenas Reads, que resultam em um único registro, são permitidas para todas as entidades do EMPLOYEEGRID.

     O padrão assumido pelo serviço REST é `serviceOperationsRights` que significa que todas as operações são permitidas para todos os ObjectGrids expostos por este serviço. Isto é diferente da implementação Microsoft para a qual o padrão é `NONE`, portanto, nenhuma operação é permitida no Serviço REST.

Importante: Os direitos de operações de serviço são avaliados na ordem em que são especificados neste arquivo, portanto, o último direito especificado substituirá os direitos que o precedem.

2. Configure os direitos de acesso da entidade.

   Os direitos do conjunto de entidades especifica os direitos de acesso que se aplicam a entidades do ObjectGrid específicas expostas por meio do serviço REST. Esses direitos fornecem uma maneira de impor um controle de acesso melhor e mais refinado sobre entidades do ObjectGrid individuais que o comparado aos direitos de Operações de Serviço.

   Use a seguinte sintaxe.

   ```
   entitySetRights.grid_name.entity_name=entity_set_right
   ```

   em que

   – *entity_set_right* pode ser um dos direitos a seguir.

Tabela 29. Direitos de Acesso de Entidade. Valores suportados.

Direito de acesso	Descrição
NENHUM	Nega todos os direitos para acessar dados
READSINGLE	Permite a leitura de itens de dados únicos
READMULTIPLE	Permite a leitura de conjuntos de dados
ALLREAD	Permite a leitura de um único ou de vários conjuntos de dados
WRITEAPPEND	Permite a criação de novos itens de dados em conjuntos de dados
WRITEREPLACE	Permite a substituição de dados
WRITEDELETE	Permite a exclusão de itens de dados dos conjuntos de dados
WRITEMERGE	Permite a mesclagem de dados
ALLWRITE	Permite a gravação (isto é, criação, substituição, mesclagem ou exclusão) de dados
ALL	Permite a criação, leitura, atualização e exclusão de dados

   – *entity_name* é o nome de um ObjectGrid específico dentro do serviço REST.

   – *grid_name* é o nome de uma entidade específica dentro do ObjectGrid especificado.

   Nota: Se os direitos de operação de serviço e os direitos do conjunto de entidades forem especificados para um ObjectGrid respectivo e suas entidades, o mais restritivo desses direitos será reforçado, conforme ilustrado nos exemplos a seguir. Observe também que os direitos do conjunto de entidades são avaliados na ordem em que são especificados no arquivo. O último direito especificado substituirá os direitos que o precedem.

   Exemplo 1: Se serviceOperationsRights.NorthwindGrid=READSINGLE e entitySetRights.NorthwindGrid.Customer=ALL forem especificados. READSINGLE será reforçado para a entidade Cliente.

   Exemplo 2: Se serviceOperationsRights.NorthwindGrid=ALLREAD for especificado e entitySetRights.NorthwindGrid.Customer=ALLWRITE for especificado, apenas Reads será permitido para todas as entidades de NorthwindGrid. No entanto, para Cliente, seus direitos do conjunto de entidades impedirão quaisquer Reads (uma vez que especificou ALLWRITE) e, consequentemente, com efeito, a entidade Cliente terá o direito de acesso como NONE.

- Transportes seguros.

A segurança de transporte é fornecida pela configuração de contêiner hosting para conexões entre o cliente da web e o serviço REST. A segurança de transporte é fornecida pela configuração do cliente do eXtreme Scale para conexões entre o serviço REST e a grade do eXtreme Scale .

1. Proteja a conexão do cliente e do serviço REST. A segurança de transporte para esta conexão é fornecida pelo ambiente de contêiner do hosting, não no eXtreme Scale.
2. Proteja a conexão do serviço REST e da grade do eXtreme Scale. A segurança de transporte para esta conexão é configurada no eXtreme Scale. Consulte "Transport Layer Security e Secure Sockets Layer" na página 785.

Integração de Segurança com o WebSphere Application Server

Quando o WebSphere eXtreme Scale é implementada em um ambiente do WebSphere Application Server, é possível simplificar a configuração de segurança do fluxo de autenticação e da camada de transporte a partir do WebSphere Application Server.

Fluxo de Autenticação Simplificada

Quando os clientes e servidores do eXtreme Scale estão em execução no WebSphere Application Server e no mesmo domínio de segurança, é possível usar a infraestrutura de segurança do WebSphere Application Server para propagar as credenciais de autenticação do cliente para o servidor do eXtreme Scale. Por exemplo, se um servlet atuar como um cliente do eXtreme Scale para se conectar a um servidor do eXtreme Scale no mesmo domínio de segurança, e o servlet já estiver autenticado, é possível propagar o token de autenticação do cliente (servlet) para o servidor e, em seguida, usar a infraestrutura de segurança do WebSphere Application Server para converter o token de autenticação de volta para as credenciais do cliente.

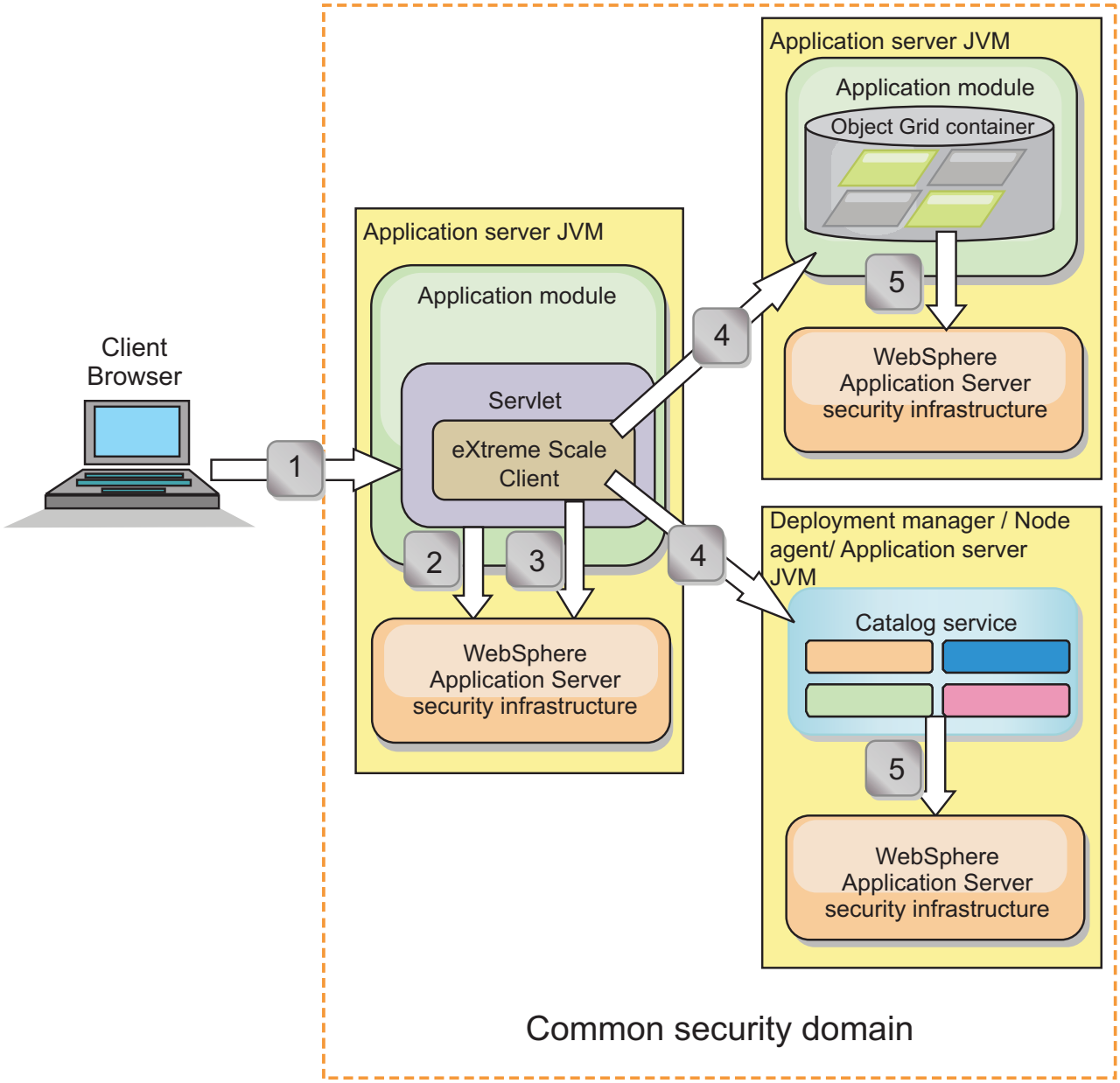


Figura 47. Fluxo de Autenticação para Servidores Dentro do Mesmo Domínio de Segurança

No diagrama anterior, os servidores de aplicativos estão no mesmo domínio de segurança. Um servidor de aplicativos hospeda o aplicativo da web, que também é um cliente do eXtreme Scale. O outro servidor de aplicativos hospeda o servidor de contêiner. A Java Virtual Machine (JVM) do gerenciador de implementação ou do agente do nó hospeda o serviço de catálogo.

Nota: Use esse tipo de configuração nos ambientes de desenvolvimento. No entanto, para ambientes de produção, execute os servidores de catálogos em processos separados e, se possível, execute os servidores de catálogos em um sistema diferente de onde os servidores de contêineres estão em execução.
As setas no diagrama indicam como o processo de autenticação flui:

1. Um usuário do aplicativo corporativo usa um navegador da web para efetuar login no primeiro servidor de aplicativos com um nome de usuário e senha.

2. O primeiro servidor de aplicativos envia o nome de usuário e a senha do cliente para a infraestrutura de segurança do WebSphere Application Server para autenticar-se com o registro do usuário. Por exemplo, este registro do usuário pode ser um servidor LDAP. Como resultado, as informações de segurança são armazenadas no encadeamento do servidor de aplicativos.
3. O arquivo JavaServer Pages (JSP) age como um cliente do eXtreme Scale para recuperar as informações de segurança a partir do encadeamento do servidor. O arquivo JSP chama a infraestrutura de segurança do WebSphere Application Server para obter os tokens de segurança que representam o usuário do aplicativo corporativo.
4. O cliente ou o arquivo JSP do eXtreme Scale envia os tokens de segurança com a solicitação para o servidor de contêiner e para o serviço de catálogo hospedados nas outras JVMs. O servidor de catálogos e o servidor de contêiner usam os tokens de segurança do WebSphere Application Server como uma credencial de cliente do eXtreme Scale.
5. Os servidores de catálogos e contêiner enviam os tokens de segurança para a infraestrutura de segurança do WebSphere Application Server para converter os tokens de segurança em informações de segurança do usuário. Essas informações de segurança do usuário são representadas por um objeto Subject, que contém os principais, as credenciais públicas e credenciais privadas. Essa conversão pode ocorrer porque os servidores de aplicativos que hospedam o cliente, um servidor de catálogos e um servidor de contêiner do eXtreme Scale compartilham os mesmos tokens WebSphere Application Server Lightweight Third-Party Authentication (LTPA).

Integração de Autenticação

Integração de segurança distribuída com o WebSphere Application Server:

Para o modelo distribuído, use as seguintes classes:

- com.ibm.websphere.objectgrid.ssecurity.plugins.builtins.WSTokenCredentialGenerator
- com.ibm.websphere.objectgrid.security.plugins.builtins.WSTokenAuthenticator
- com.ibm.websphere.objectgrid.security.plugins.builtins.WSTokenCredential

Para obter exemplos sobre como usar essas classes, consulte “Tutorial: Integrar a Segurança do WebSphere eXtreme Scale com o WebSphere Application Server” na página 47.

No lado do servidor, o WSTokenAuthentication pode ser utilizado como o autenticador para autenticar o objeto WSTokenCredential.

Integração de segurança local com o WebSphere Application Server:

Para o modelo de ObjectGrid local, use as seguintes classes:

- com.ibm.websphere.objectgrid.security.plugins.builtins.WSSubjectSourceImpl
- com.ibm.websphere.objectgrid.security.plugins.builtins.WSSubjectValidationImpl

Para obter mais informações sobre essas classes, consulte “Programação de Segurança Local” na página 836. É possível configurar a classe WSSubjectSourceImpl como o plug-in SubjectSource e a classe WSSubjectValidationImpl como o plug-in SubjectValidation.

Suporte à Segurança da Camada de Transporte no WebSphere Application Server

Quando um cliente, um servidor de contêiner ou servidor de catálogos do eXtreme Scale está em execução em um processo do WebSphere Application Server, a segurança de transporte do eXtreme Scale é gerenciada pelas configurações de transporte do WebSphere Application Server CSIV2. Para o cliente ou servidor de contêiner do eXtreme Scale,as propriedades do cliente ou de servidor do eXtreme Scale não devem ser usadas para definir as configurações SSL. Todas as configurações SSL devem ser especificadas na configuração do WebSphere Application Server.

Entretanto, o servidor de catálogos é um pouco diferente. O servidor de catálogos tem seus próprios caminhos de transporte proprietários que não podem ser gerenciados pelas configurações de transporte do WebSphere Application Server CSIV2. Portanto, as propriedades de SSL ainda precisam ser configuradas no arquivo de propriedades do servidor para o servidor de catálogos. Consulte o "Tutorial: Integrar a Segurança do WebSphere eXtreme Scale com o WebSphere Application Server" na página 47 para obter informações adicionais.

Configurando a Segurança do Cliente em um Domínio de Serviço de Catálogo

Ao configurar a segurança do cliente em um domínio do serviço de catálogo, é possível definir as propriedades de configuração de autenticação de cliente padrão. Essas propriedades são usadas quando um arquivo de propriedades do cliente não estiver localizado na Java virtual machine (JVM) que está hospedando o cliente ou quando o cliente não especificar programaticamente as propriedades de segurança. Se um arquivo de propriedades do cliente existir, as propriedades que especificas no console substituirão os valores no arquivo. É possível substituir essas propriedades ao especificar um arquivo `splicer.properties` com a propriedade customizada com.ibm.websphere.xs.sessionFilterProps ou ao unir o arquivo EAR do aplicativo.

Antes de Iniciar

- Você deve saber a implementação CredentialGenerator que está usando para autenticar os clientes com a grade de dados remota. É possível usar uma das implementações que são fornecidas pelo WebSphere eXtreme Scale: UserPasswordCredentialGenerator ou WSTokenCredentialGenerator.

  Também é possível usar uma implementação customizada da interface CredentialGenerator. A implementação customizada deve estar no caminho de classe do cliente de tempo de execução e do servidor. Se estiver configurando um cenário de sessão HTTP com WebSphere Application Server, você deverá colocar a implementação no caminho de classe do gerenciador de implementação e no caminho de classe do servidor de aplicativos no qual o cliente está em execução.
- Um domínio de serviço de catálogo deve ser definido. Consulte Criando Domínios do Serviço de Catálogo no WebSphere Application Server para obter mais informações.

Sobre Esta Tarefa

A segurança do cliente deve ser configurada no domínio de serviço de catálogo, quando a autenticação de credencial no lado do servidor foi ativada, ao configurar um dos seguintes cenários:

- A política de segurança no lado do servidor tem a propriedade **credentialAuthentication** configurada para `Obrigatório`.
- A política de segurança do lado do servidor possui a propriedade **credentialAuthentication** configurada para `Suportado` e (AND) um **authorizationMechanism** foi especificado no arquivo XML do ObjectGrid.

Nesses cenários, uma credencial deve ser passada a partir do cliente. A credencial que é passada do cliente é recuperada a partir do método getCredential em uma classe que implementa a interface CredentialGenerator. Em um cenário de configuração de sessão HTTP, o tempo de execução deve conhecer a implementação CredentialGenerator a ser usada para gerar uma credencial que é transmitida para uma grade de dados remota. Se a classe de implementação CredentialGenerator não for especificadapara uso, a grade de dados remota rejeitará solicitações do cliente porque o cliente não pode ser autenticado.

Procedimento

Defina as propriedades de segurança do cliente. No console administrativo do WebSphere Application Server , clique em **Administração do sistema** > **WebSphere eXtreme Scale** > **Domínios do serviço de catálogo** > *catalog_service_domain_name* > **Propriedades de segurança do cliente**. Especifique as propriedades de segurança do cliente na página e salve suas mudanças. Consulte Propriedades de Segurança do Cliente para obter uma lista de propriedades que podem ser configuradas.

Resultados

As propriedades de segurança do cliente configuradas no domínio de serviço de catálogo são usadas como valores padrão. Os valores especificados substituem quaisquer propriedades que forem definidas nos arquivos `client.properties`.

O que Fazer Depois

Configure seus aplicativos para usar o WebSphere eXtreme Scale para gerenciamento de sessão. Consulte Unindo Automaticamente Aplicativos para Gerenciamento de Sessões HTTP no WebSphere Application Server para obter mais informações.

Configurando a Segurança da Grade de Dados e SSL para .NET

.NET

É possível configurar .NET e Java para comunicação por meio de Secure Sockets Layer (SSL) e para usar a lógica de autenticação UserPassword.

Antes de Iniciar

Você deve ter os arquivos `key.jks` e `trust.jks` para seu ambiente. Para obter informações adicionais sobre como criar arquivos de keystore e de armazenamento confiável, consulte “Tutorial de Segurança do Java SE - Etapa 6” na página 34.

Procedimento

1. Ative e configure a segurança em seus servidores. Se a segurança ainda não estiver configurada em seus servidores, use as etapas a seguir para configurar a segurança com a amostra do autenticador externo.

a. Obtenha os arquivos de segurança de amostra. Faça download dos arquivos de amostra no arquivo `security_extauth.zip` do wiki do WebSphere eXtreme Scale.
   - `xsjaas3.config` : Define a configuração de Java Authentication and Authorization Service (JAAS).
   - `sampleKS3.jks` Contém o keystore de valores de usuário e senha do JAAS.
   - `security3.xml` Define o autenticador para utilização para segurança.

b. Edite o arquivo `xsjaas3.config` e corrija o caminho para o arquivo `sampleKS3.jks`.

c. Se desejar gerar seu próprio keystore privado em vez de usar o arquivo `sampleKS3.jks` de amostra, utilize o utilitário **keytool** para gerar a chave privada.

```
keytool -genkey -alias myalias -keysize 2048 -keystore key.jks -keyalg rsa -dname
 "CN=www.mydomain.com" -storepass password -keypass password -validity 3650
```

d. Edite o `sampleServer.properties` para ativar a segurança. O arquivo `sampleServer.properties` está no diretório *wxs_install_root*\`properties`. Remova o comentário e edite os seguintes valores da propriedade:

```
securityEnabled=true
secureTokenManagerType=none
alias=ogsample
contextProvider=IBMJSSE2
protocol=SSL
keyStoreType=JKS
keyStore=../../../../xio.test/etc/test/security/key.jks
keyStorePassword=ogpass
trustStoreType=JKS
trustStore=../../../../xio.test/etc/test/security/trust.jks
trustStorePassword=ogpass
```

e. Inicie os servidores de catálogo e contêiner.

```
startXsServer.bat cs0 -catalogServiceEndPoints
cs0:localhost:6600:6601 -listenerPort 2809 -objectgridFile
gettingstarted\xml\objectgrid.xml
-deploymentPolicyFile gettingstarted\xml\deployment.xml
-serverProps ..\properties\sampleServer.properties
-clusterSecurityFile security3.xml -jvmArgs
-Djava.security.auth.login.config="xsjaas3.config"
```

```
startXsServer.bat c0 -catalogServiceEndPoints
localhost:2809 -objectgridFile gettingstarted\xml\objectgrid.xml
-deploymentPolicyFile gettingstarted\xml\deployment.xml
-serverProps ..\properties\sampleServer.properties
-clusterSecurityFile security3.xml -jvmArgs
-Djava.security.auth.login.config="xsjaas3.config"
```

2. Configure a segurança para o cliente .NET.

a. Opcional: Usando o utilitário keytool, extraia o certificado público do arquivo `key.jks` que você configurou para o servidor.

```
keytool -export -alias myalias -keystore key.jks -file public.cer -storepass password
```

   Importe essa chave pública para o armazenamento de certificados do Windows com o Certificate Management Tool, `certmgr.msc`, para importar a chave para a pasta de certificados 'Trusted Root Certification Authority' ou 'Trusted People'. (A propriedade **keyStore** no arquivo `client.properties` pode apontar para esse arquivo)

b. Edite o arquivo `Client.Net.properties` para incluir os valores de propriedades a seguir:

```
securityEnabled=true
credentialAuthentication=supported
authenticationRetryCount=3
credentialGeneratorAssembly=IBM.WebSphere.Caching.C
CredentialGenerator,Version=8.6.0.0,
Culture=neutral,PublicKeyToken=b439a24ee43b0816
credentialGeneratorProps=manager manager1
transportType=ssl-supported
publicKeyFile=<name>.cer
```

O valor da propriedade credentialGeneratorProps, `manager manager1` é usado como os valores de nome de usuário e senha que são fornecidos ao servidor no objeto de Credencial.

A propriedade **publicKeyFile** é configurada como um caminho relativo para o tempo de execução de .NET. Se a propriedade **publicKeyFile** não estiver configurada, no armazenamento de certificados do Windows 'a' é procurado o arquivo `public.cer`. Se a propriedade **publicKeyFile** for configurada, então, o arquivo especificado será usado para o arquivo de certificado público de SSL. Se o arquivo especificado não puder ser localizado, o cliente .NET tenta localizar um arquivo `public.cer` correspondente no armazenamento de certificados.

c. Copie *net_client_home*`\IBM.WebSphere.Caching.CredentialGenerator.dll` para o diretório *net_client_home*`\sample\SimpleClient\bin\`*`<ConfigurationName>`*.

d. Construa uma amostra com o contexto de projeto *ConfigurationName*. Execute a amostra em seu servidor.

Ativando Autorização da Grade de Dados

O WebSphere eXtreme Scale fornece vários terminais de segurança para integrar mecanismos customizados. No modelo de programação local, a principal função de segurança é a autorização e não possui suporte à autenticação. É necessário autenticar fora do WebSphere Application Server já existente. No entanto, é possível usar os plug-ins fornecidos para obter e validar objetos Subject.

Sobre Esta Tarefa

A segurança local pode ser ativada com o arquivo descritor XML do ObjectGrid ou programaticamente.

Procedimento

- Ative a segurança local com o arquivo descritor XML do ObjectGrid.

  O arquivo `secure-objectgrid-definition.xml`, que é utilizado na amostra do aplicativo corporativo ObjectGridSample, é mostrado no seguinte exemplo. Configure o atributo securityEnabled como `true` para ativar a segurança.

```
<objectGrids>
    <objectGrid name="secureClusterObjectGrid" securityEnabled="true"
        authorizationMechanism="AUTHORIZATION_MECHANISM_JAAS">
    ...
</objectGrids>
```

- Ative a segurança local programaticamente.

  Para criar um ObjectGrid usando o método ObjectGrid.setSecurityEnabled, chame o seguinte método na interface ObjectGrid:

```
/**
 * Enable the ObjectGrid security
 */
void setSecurityEnabled();
```

O que Fazer Depois

Inicie os servidores de contêiner e de catálogos com a segurança ativada.

Referências relacionadas:

Arquivo Descritor XML de Política de Implementação
Para configurar uma política de implementação, utilize um arquivo XML do descritor da política de implementação.

Iniciando e Parando Servidores Seguros

A segurança é ativada ao definir as configurações específicas de segurança quando você inicia e para servidores.

Iniciando Servidores Seguros em um Ambiente Independente

Para iniciar servidores independentes seguros, transmita os arquivos de configuração adequados, especificando os parâmetros no comando **startOgServer** ou **startXsServer**.

8.6+ Sobre Esta Tarefa

Reprovado: 8.6+ Os comandos **startOgServer** e **stopOgServer** iniciam servidores que usam o mecanismo de transporte do Object Request Broker (ORB). O ORB foi descontinuado, mas você pode continuar utilizando esses scripts se estava utilizando o ORB em uma liberação anterior. O mecanismo de transporte do IBM eXtremeIO (XIO) substitui o ORB. Use os scripts **startXsServer** e **stopXsServer** para iniciar e parar os servidores que utilizam o transporte XIO.

Procedimento

- Inicie seus servidores de contêiner seguros.

  Iniciar um servidor de contêiner seguro requer o seguinte arquivo de configuração de segurança:

  – **Arquivo de propriedades do servidor:** O arquivo de propriedades do servidor configura as propriedades de segurança específicas para o servidor. Consulte o Arquivo de Propriedades do Servidor para obter mais detalhes.

  Especifique o local deste arquivo de configuração fornecendo o argumento a seguir ao script **startOgServer** ou **startXsServer**:

  -serverProps
  Especifica o local do arquivo de propriedades do servidor, que contém as propriedades de segurança específicas do servidor. O nome do arquivo especificado para esta propriedade está em formato de caminho de arquivo simples, como `../security/server.properties`.

  Insira as linhas a seguir ao executar o comando **startOgServer** ou o comando **startXsServer**: UNIX Linux

```
startOgServer.sh <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
-Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=$OBJECTGRID_HOME
```

UNIX Linux 8.6+

```
startXsServer.sh <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
-Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=$OBJECTGRID_HOME
```

Windows

```
startOgServer.bat <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
-Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=%OBJECTGRID_HOME%
```

Windows 8.6+

```
startXsServer.bat <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config
 -Djava.security.manager -Djava.security.policy="auth.policy" -Dobjectgrid.home=%OBJECTGRID_HOME%
```

- Inicie os servidores de catálogos seguros.

  Para iniciar um serviço de catálogo seguro, você deve ter os seguintes arquivos de configuração:

  – **Arquivo descritor XML de segurança:** O arquivo descritor XML de segurança descreve as propriedades de segurança comuns para todos os servidores, incluindo servidores de catálogo e servidores de contêiner. Um exemplo de propriedade é a configuração do autenticador que representa o registro do usuário e o mecanismo de autenticação.

  – **Arquivo de propriedades do servidor:** O arquivo de propriedades do servidor configura as propriedades de segurança que são específicas para o servidor.

  Especifique o local destes arquivos de configuração fornecendo os argumentos a seguir ao script **startOgServer** ou **startXsServer**:

  -clusterSecurityFile e -clusterSecurityUrl
  Estes argumentos especificam o local do arquivo descritor XML de Segurança. Use o parâmetro **-clusterSecurityFile** para especificar um arquivo local ou o parâmetro **-clusterSecurityUrl** para especificar a URL do arquivo `objectGridSecurity.xml`.

  -serverProps
  Especifica o local do arquivo de propriedades do servidor, que contém as propriedades de segurança específicas do servidor. O nome do arquivo especificado para esta propriedade está em formato de caminho de arquivo simples, tal como `c:/tmp/og/catalogserver.props`.

Iniciando Servidores Seguros no WebSphere Application Server

Para iniciar servidores seguros no WebSphere Application Server, você deve especificar os arquivos de configuração de segurança nos argumentos genéricos da Java virtual machine (JVM).

Procedimento

- Associe os servidores de catálogos do WebSphere eXtreme Scale aos WebSphere Application Servers usando o console administrativo. No console administrativo, clique em **Administração do Sistema** > **WebSphere eXtreme Scale** > **Domínios do serviço de catálogo**.
- Associe os servidores de contêineres do WebSphere eXtreme Scale aos WebSphere Application Servers específicos implementando um arquivo archive corporativo (EAR) que contém os descritores XML necessários para a grade de dados. Para obter informações adicionais sobre esse procedimento, consulte “Tutorial: Integrar a Segurança do WebSphere eXtreme Scale com o WebSphere Application Server” na página 47.
- Especifique os argumentos da Java virtual machine (JVM) que aponta para arquivos de configuração para tornar os servidores de catálogos e de contêineres seguros. Para obter informações adicionais sobre esse procedimento. consulte Autenticando Solicitações de Clientes no WebSphere Application Server e “Autorizando Acesso à Grade de Dados no WebSphere Application Server” na página 145

página 145. Além disso, especifique `securityEnabled="true"` no arquivo `objectgrid xml` para cada grade de dados. Após especificar os argumentos JVM e ativar segurança em suas grades de dados, é possível iniciar os servidores ou clusters que agem como servidores de catálogos ou servidores de contêineres do eXtreme Scale.

- Inicie os servidores de catálogos e de contêineres com o console administrativo do WebSphere Application Server ou use a linha de comandos do WebSphere Application Server.

O que Fazer Depois

"Parando Servidores Seguros" na página 161

Parando Servidores Seguros

Parar servidores de catálogos ou servidores de contêiner seguros requer um arquivo de configuração de segurança.

Procedimento

- Pare um servidor de catálogos ou um servidor de contêiner seguro nas implementações independentes. Em ambientes independentes, pare os servidores de catálogos e de contêineres do WebSphere eXtreme Scale usando a função teardown do comando **xscmd** ou usando os comandos **stopXsServer** ou **stopOgServer**.

  Restrinja acesso a essas operações aos administradores autorizados somente, conforme descrito na seção "Autorizando Acesso para Operações Administrativas em Ambientes Independentes" na página 146. Quando autenticação ou SSL é usado, os comandos **stopXsServer** e **stopOgServer** requerem que um arquivo de propriedades do cliente seja passado como um parâmetro. O conteúdo do arquivo de propriedades do cliente está descrito em "Autenticando Solicitações de Clientes em Ambientes Independentes" na página 135 e "Protegendo Dados que Fluem entre Servidores eXtreme Scale em Ambientes Independentes com Criptografia SSL" na página 149.
- Use o console administrativo do WebSphere Application Server para parar o servidor do eXtreme Scale executado com o WebSphere Application Server. A segurança administrativa do WebSphere Application Server deve estar configurada para restringir acesso para iniciar e parar servidores a administradores autorizados, conforme descrito em "Autorizando Acesso para Operações Administrativas no WebSphere Application Server" na página 149.

Configurando o WebSphere eXtreme Scale para Utilizar o FIPS 140-2

Federal Information Processing Standard (FIPS) 140-2 especifica os níveis necessários de criptografia para Transport Layer Security/Secure Sockets Layer (TLS/SSL). Este padrão assegura alta protecção de dados conforme eles são enviados pela conexão.

Antes de Iniciar

- Você deve estar utilizando um IBM Runtime Environment. Para obter informações adicionais, consulte "Considerações sobre o Java SE" na página 310.
- Configure a segurança da camada de transporte e o Secure Sockets Layer em ambas as direções. Seu arquivo de armazenamento confiável do servidor de catálogo deve conter os certificados autoassinados para os servidores de contêiner. Os servidores de contêiner devem conter os certificados autoassinados

para o servidor de catálogos. Para obter informações adicionais, consulte "Transport Layer Security e Secure Sockets Layer" na página 785.

Sobre Esta Tarefa

É possível utilizar as etapas a seguir para configurar os servidores de catálogos e servidores de contêiner em sua instalação independente do WebSphere eXtreme Scale para utilizar o FIPS.

Se você estiver usando o WebSphere eXtreme Scale integrado ao WebSphere Application Server, os servidores de catálogo e servidores de contêiner herdarão as propriedades de segurança do servidor de aplicativos. Para obter mais informações sobre como configurar o FIPS com o WebSphere Application Server, consulte Configurando arquivos Java Secure Socket Extension do Federal Information Processing Standard. Quando um servidor de catálogo é executado no WebSphere Application Server, algumas das comunicações são controladas pelo arquivo `server.properties`. Atualize o arquivo `server.properties` para conter as mesmas propriedades que são necessárias para os servidores de catálogo independentes.

Procedimento

1. Edite o arquivo `java.security`. O local do `java.security` depende da configuração de sua Java virtual machine (JVM):
   - Se você estiver utilizando a JVM padrão que é fornecida com o produto, o arquivo está no diretório *wxs_install_root*`/java/jre/lib/security`.
   - Se você estiver utilizando uma JVM diferente, edite o arquivo no diretório *java_home*`/jre/lib/security`.

   O arquivo deve conter o seguinte texto:

   ```
   security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
   security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
   security.provider.3=com.ibm.crypto.provider.IBMJCE
   security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.5=com.ibm.security.cert.IBMCertPath
   security.provider.6=com.ibm.security.sasl.IBMSASL
   security.provider.7=com.ibm.xml.crypto.IBMXMLCryptoProvider
   security.provider.8=com.ibm.xml.enc.IBMXMLEncProvider
   security.provider.9=org.apache.harmony.security.provider.PolicyProvider
   security.provider.10=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
   ```

2. Edite os arquivos de propriedades do servidor para o servidor de catálogos e servidores de contêiner.

   Esses arquivos devem conter as propriedades e os valores a seguir:

   ```
   contextProvider=IBMJSSE2
   transportType=SSL-Required
   ```

   Para obter mais informações sobre propriedades de servidor, consulte Arquivo de Propriedades do Servidor.

3. Configure pares de chaves que usam o algoritmo de geração de chave RSA no conjunto de chaves para o servidor de catálogos e os servidores de contêineres. O comprimento da chave mínimo é 1024 bits.
4. Reinicie seus servidores de catálogo e de contêiner.

   Ao iniciar os servidores de catálogos, você deve especificar argumentos da Java virtual machine (JVM). Os argumentos que você utiliza dependem de qual versão do Java SE você está utilizando.

   - Para Java 5 e Java 6 até o SR 9, especifique o argumento **`-Dcom.ibm.jsse2.JSSEFIPS=true`** quando iniciar o servidor.

- Para Java 6 SR 10 e posterior, ou Java 7, especifique o argumento **-Dcom.ibm.jsse2.usefipsprovider=true** quando iniciar o servidor.

Para obter informações adicionais, consulte "Iniciando e Parando Servidores Seguros" na página 158.

Configurando Perfis de Segurança para o Utilitário xscmd

Criando um perfil de segurança, é possível usar parâmetros de segurança salvos para usar o utilitário **xscmd** com ambientes seguros.

Antes de Iniciar

Para obter informações adicionais sobre como configurar o utilitário **xscmd**, consulte Administrando com o Utilitário **xscmd**.

Sobre Esta Tarefa

É possível usar o parâmetro **-ssp** *profile_name* ou **--saveSecProfile** *profile_name* com o restante de seu comando **xscmd**. Para salvar um perfil de segurança. O perfil pode conter configurações para nomes de usuário e senhas, geradores de credencial, keystores, armazenamentos confiáveis e tipos de transporte.

O do grupo de comandos **ProfileManagement** no utilitário **xscmd** contém comandos para gerenciar seus perfis de segurança.

Procedimento

- Salve um perfil de segurança.

  Para salvar um perfil de segurança, use o parâmetro **-ssp** *profile_name* ou **--saveSecProfile** *profile_name* com o restante de seu comando. A inclusão deste parâmetro em seu comando salva os parâmetros a seguir:

  ```
  -al,--alias <alias>
  -arc,--authRetryCount <integer>
  -ca,--credAuth <support>
  -cgc,--credGenClass <className>
  -cgp,--credGenProps <property>
  -cxpv,--contextProvider <provider>
  -ks,--keyStore <filePath>
  -ksp,--keyStorePassword <password>
  -kst,--keyStoreType <type>
  -prot,--protocol <protocol>
  -pwd,--password <password>
  -ts,--trustStore <filePath>
  -tsp,--trustStorePassword <password>
  -tst,--trustStoreType <type>
  -tt,--transportType <type>
  -user,--username <username>
  ```

  Os perfis de segurança são salvos no diretório *user_home*`\.xscmd\profiles\security\<`*profile_name*`>.properties`.

  Importante: Não inclua a extensão do nome do arquivo `.properties` no parâmetro *profile_name*. Essa extensão é incluída automaticamente no nome do arquivo.

- Use um perfil de segurança salvo.

  Para usar um perfil de segurança salvo, inclua o parâmetro **-sp** *profile_name* ou **--securityProfile** *profile_name* no comando que você está executando. Exemplo de comando: `xscmd -c listHosts -cep myhost.mycompany.com -sp myprofile`

- Liste os comandos no grupo de comandos do **ProfileManagement**.
  Execute o comando a seguir: **xscmd -lc ProfileManagement**.
- Liste os perfis de segurança existentes.
  Execute o comando a seguir: **xscmd -c listProfiles -v**.
- Exiba as configurações que são salvas em um perfil de segurança.
  Execute o comando a seguir: **xscmd -c showProfile -pn** *profile_name*.
- Remova um perfil de segurança existente.
  Execute o comando a seguir: **xscmd -c RemoveProfile -pn** *profile_name*.

Referências relacionadas:

Ferramenta **xsadmin** para a Migração de Ferramenta **xscmd**
Em liberações anteriores, a ferramenta **xsadmin** é um utilitário de linha de comandos de amostra para monitorar o estado do ambiente. A ferramenta **xscmd** foi apresentada como uma ferramenta de linha de comandos administrativa e de monitoramento oficialmente suportada. Se a ferramenta **xsadmin** era usada anteriormente, considere migrar seus comandos para a nova ferramenta **xscmd**.

Protegendo as Conexões do Cliente J2C

Use a arquitetura Java 2 Connector (J2C) para proteger as conexões entre clientes WebSphere eXtreme Scale e seus aplicativos.

Sobre Esta Tarefa

Os aplicativos se referem ao connection factory, o que estabelece a conexão com a grade de dados remotos. Cada connection factory hospeda uma única conexão do cliente do eXtreme Scale que é reutilizada para todos os componentes de aplicativo.

Importante: Uma vez que a conexão do cliente do eXtreme Scale pode incluir um cache próximo, é importante que os aplicativos não compartilhem uma conexão. Um connection factory deve existir para uma instância única do aplicativo para evitar problemas ao compartilhar objetos entre os aplicativos.

É possível configurar o gerador de credenciais com a API ou no arquivo de propriedades do cliente. No arquivo de propriedades do cliente, as propriedades securityEnabled e credentialGenerator são usadas. O exemplo de código a seguir é exibido em diversas linhas para propósitos de publicação:

```
securityEnabled=true
credentialGeneratorClass=com.ibm.websphere.objectgrid.security.plugins.builtins.
     UserPasswordCredentialGenerator
credentialGeneratorProps=operator XXXXXX
```

O gerador de credenciais e a credencial no arquivo de propriedades do cliente são usados para a operação de conexão eXtreme Scale e as credenciais J2C padrão. Portanto, as credenciais que são especificadas com a API são usadas no tempo de conexão J2C para a conexão J2C. No entanto, se nenhuma credencial estiver especificada no tempo de conexão J2C, o gerenciador de credencial no arquivo de propriedades do cliente será usado.

Procedimento

1. Configure o acesso seguro em que a conexão J2C representa o cliente eXtreme Scale. Use a propriedade do connection factory ClientPropertiesResource ou a propriedade do connection factory ClientPropertiesURL para configurar a autenticação de cliente.

Se estiver usando o WebSphere eXtreme Scale com o WebSphere Application Server, especifique as propriedades do cliente na configuração do domínio de serviço de catálogo. Quando a connection factory referencia o domínio, ela usa automaticamente esta configuração.

2. Configure as propriedades de segurança do cliente para usar o connection factory que faz referência ao objeto gerador de credencial apropriado para eXtreme Scale. Essas propriedades também são compatíveis com a segurança do servidor eXtreme Scale. Por exemplo, use o gerador de credencial WSTokenCredentialGenerator para as credenciais WebSphere quando o eXtreme Scale estiver instalado com o WebSphere Application Server. Como alternativa, use o gerador de credencial UserPasswordCredentialGenerator quando executar o eXtreme Scale em um ambiente independente. No exemplo a seguir, as credenciais são passadas programaticamente usando a chamada de API em vez de usar a configuração nas propriedades do cliente:

   ```
   XSConnectionSpec spec = new XSConnectionSpec();
   spec.setCredentialGenerator(new UserPasswordCredentialGenerator("operator", "xxxxxx"));
   Connection conn = connectionFactory.getConnection(spec);
   ```

3. (Opcional) Desative o cache próximo, se necessário.

   Todas as conexões J2C de um único connection factory compartilham um único cache próximo. As permissões da entrada de grade e as permissões de mapa são validadas no servidor, mas não no cache próximo. Quando um aplicativo usa diversas credenciais para criar conexões J2C e a configuração usa permissões específicas para entradas de grade e mapas para essas credenciais, desative o cache próximo. Desative o cache próximo usando a propriedade do connection factory, ObjectGridResource ou ObjectGridURL. Para obter mais informações sobre como desativar o cache local, consulte Configurando o Cache Local.

4. (Opcional) Configure as configurações de política de segurança, se necessário.

   Se o aplicativo J2EE contém a configuração de arquivo Resource Adapter Archive (RAR) do eXtreme Scale integrado, pode ser necessário configurar as configurações de política de segurança adicionais no arquivo da política de segurança para o aplicativo. Por exemplo, essas políticas são necessárias:

   ```
   permission com.ibm.websphere.security.WebSphereRuntimePermission "accessRuntimeClasses";
   permission java.lang.RuntimePermission "accessDeclaredMembers";
   permission javax.management.MBeanTrustPermission "register";
   permission java.lang.RuntimePermission "getClassLoader";
   ```

   Além disso, quaisquer arquivos de propriedade ou recurso usados pelos connection factories precisarão do arquivo ou de outras permissões, como `permission java.io.FilePermission "filePath";`. Para WebSphere Application Server, o arquivo de políticas é `META-INF/was.policy`, e está localizado no arquivo EAR J2EE.

Resultados

As propriedades de segurança do cliente configuradas no domínio de serviço de catálogo são usadas como valores padrão. Os valores que você especifica substituem quaisquer propriedades definidas nos arquivos `client.properties`.

O que Fazer Depois

Use as APIs de acesso a dados eXtreme Scale para desenvolver os componentes do cliente que você deseja para usar as transações.

Programação para Segurança

Use as interfaces de programação para tratar vários aspectos da segurança em um ambiente do WebSphere eXtreme Scale.

API de Segurança

Java

O WebSphere eXtreme Scale adota uma arquitetura de segurança aberta. Ela fornece uma estrutura de segurança básica para autenticação, autorização e segurança de transporte e requer que os usuários implementem plug-ins para completar a infraestrutura de segurança.

A seguinte imagem mostra o fluxo básico de autenticação e autorização do cliente para um servidor eXtreme Scale.

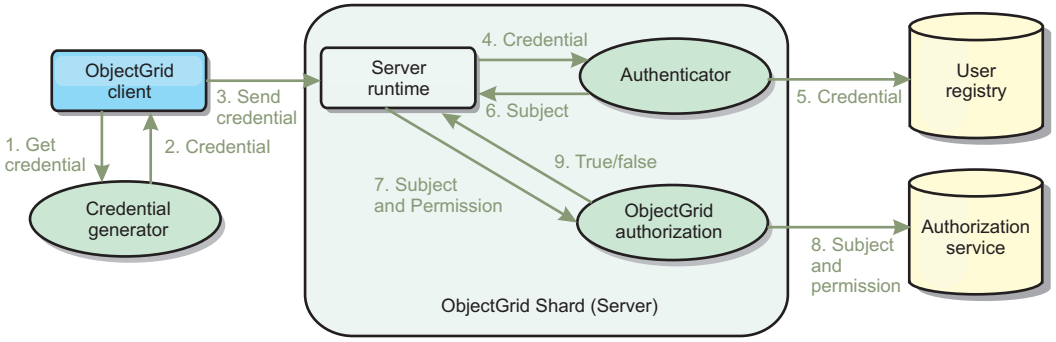


Figura 48. Fluxo de Autenticação e Autorização do Cliente

O fluxo de autenticação e o fluxo de autorização são os seguintes.

Fluxo de Autenticação

1. O fluxo de autenticação inicia com um cliente eXtreme Scale obtendo uma credencial. Isso é feito pelo plug-in com.ibm.websphere.objectgrid.security.plugins.CredentialGenerator.
2. Um objeto CredentialGenerator sabe como gerar uma credencial de cliente válida, por exemplo, um par de ID de usuário e senha, ticket Kerberos, e assim por diante. Essa credencial gerada é enviada de volta para o cliente.
3. Depois que o cliente recuperar o objeto Credential usando o objeto CredentialGenerator, esse objeto Credential será enviado junto com o pedido eXtreme Scale para o servidor eXtreme Scale.
4. O servidor eXtreme Scale autentica o objeto Credential antes de processar o pedido do eXtreme Scale. Em seguida, o servidor utiliza o plug-in do Autenticador para autenticar o objeto Credential.
5. O plug-in do Autenticador representa uma interface com o registro do usuário, por exemplo, um servidor Lightweight Directory Access Protocol (LDAP) ou um registro do usuário do sistema operacional. O Autenticador consulta o registro do usuário e toma as decisões de autenticação.
6. Se a autenticação for bem sucedida, um objeto Subject será retornado para representar este cliente.

   Fluxo de Autorização

O WebSphere eXtreme Scale adota um mecanismo de autorização baseado em permissão e possui categorias de permissão diferentes representadas por diferentes classes de permissão. Por exemplo, um objeto com.ibm.websphere.objectgrid.security.MapPermission representa permissões para ler, gravar, inserir, invalidar e remover as entradas de dados em um ObjectMap. Como o WebSphere eXtreme Scale suporta a autorização Java Authentication and Authorization Service (JAAS) disponível para uso imediato, é possível usar o JAAS para manipular autorização ao fornecer políticas de autorização.

Além disso, o eXtreme Scale suporta autorizações customizadas. As autorizações customizadas são conectadas pelo plug-in com.ibm.websphere.objectgrid.security.plugins.ObjectGridAuthorization. O fluxo de autorização do cliente é o seguinte.

7. O tempo de execução do servidor envia o objeto Subject e a permissão necessária para o plug-in de autorização.
8. O plug-in de autorização consulta o serviço de Autorização e toma uma decisão de autorização. Se a permissão for concedida para esse objeto Subject, um valor `true` ou `false` será retornado.
9. Essa decisão de autorização, true ou false, é retornada para o tempo de execução do servidor.

Implementação de Segurança

Os tópicos nessa sessão discutem como programar uma implementação WebSphere eXtreme Scale segura e como programar as implementações de plug-in. A seção é organizada com base nos vários recursos de segurança. Em cada subtópico, você aprenderá sobre os plug-ins relevantes e como implementar os plug-ins. Na seção de autenticação, você saberá como se conectar a um ambiente de implementação seguro do WebSphere eXtreme Scale.

Autenticação do Cliente: O tópico de autenticação do cliente descreve como um cliente WebSphere eXtreme Scale obtém uma credencial e como um servidor autentica o cliente. Ele também discutirá como um cliente do WebSphere eXtreme Scale se conecta a um servidor WebSphere eXtreme Scale seguro.

Autorização: O tópico de autorização explica como usar o ObjectGridAuthorization para efetuar autorização do cliente além da autorização JAAS.

Autenticação de Grade: O tópico de autenticação de grade de dados descreve como o SecureTokenManager pode ser usado para transportar segredos do servidor com segurança.

Programação do Java Management Extensions (JMX): Quando o servidor WebSphere eXtreme Scale estiver protegido, o cliente JMX poderá precisar enviar uma credencial JMX com o servidor.

Programação de Autenticação de Cliente

Java

Para autenticação, o WebSphere eXtreme Scale fornece um tempo de execução para enviar a credencial do cliente para o lado do servidor e, em seguida, chama o plug-in do autenticador para autenticar os usuários.

O WebSphere eXtreme Scale exige que você implemente os plug-ins a seguir para completar a autenticação.

- Credential: Uma Credential representa uma credencial de cliente, como um par de ID de usuário e senha.
- CredentialGenerator: Uma CredentialGenerator representa um factory de credenciais para gerar a credencial.
- Authenticator: Um Authenticator autentica a credencial do cliente e recupera as informações do cliente.

Plug-ins Credential e CredentialGenerator

Quando um cliente do eXtreme Scale se conecta a um servidor que exige autenticação, o cliente é obrigado a fornecer uma credencial do cliente. Uma credencial do cliente é representado por uma interface com.ibm.websphere.objectgrid.security.plugins.Credential. Uma credencial de cliente pode ser um par de nome de usuário e senha, um registro do Kerberos, um certificado cliente ou dados em qualquer formato concordado entre o cliente e o servidor. Esta interface explicitamente define os métodos equals(Object) e hashCode. Estes métodos são importantes porque os objetos Subject autenticados são armazenados em cache utilizando o objeto Credential como a chave no lado do servidor. O WebSphere eXtreme Scale também fornece um plug-in para gerar uma credencial. Este plug-in é representado pela interface com.ibm.websphere.objectgrid.security.plugins.CredentialGenerator e será útil quando a credencial puder expirar. Neste caso, o método getCredential é chamado para renovar uma credencial.

A interface Credential explicitamente define os métodos equals(Object) e hashCode. Estes métodos são importantes porque os objetos Subject autenticados são armazenados em cache utilizando o objeto Credential como a chave no lado do servidor.

Você também pode usar o plug-in fornecido para gerar uma credencial. Este plug-in é representado pela interface com.ibm.websphere.objectgrid.security.plugins.CredentialGenerator e é útil quando a credencial pode expirar. Neste caso, o método getCredential é chamado para renovar uma credencial. Consulte Interface CredentialGenerator para obter mais detalhes.

Há três implementações padrão fornecidas para as interfaces da Credencial:

- A implementação da com.ibm.websphere.objectgrid.security.plugins.builtins.UserPasswordCredential, que contém um par de ID de usuário e senha.
- A implementação da com.ibm.websphere.objectgrid.security.plugins.builtins.WSTokenCredential, que contém tokens de autenticação e autorização específicos do WebSphere Application Server. Estes tokens podem ser utilizados para propagar os atributos de segurança nos servidores de aplicativos no mesmo domínio de segurança.

O WebSphere eXtreme Scale também fornece um plug-in para gerar uma credencial. Este plug-in é representado pela interface com.ibm.websphere.objectgrid.security.plugins.CredentialGenerator. O WebSphere eXtreme Scale fornece duas implementações integradas padrão:

- O construtor com.ibm.websphere.objectgrid.security.plugins.builtins.UserPasswordCredentialGenerator

pega um ID de usuário e uma senha. Quando o método getCredential é chamado, retorna um objeto UserPasswordCredential, que contém o ID do usuário e a senha.

- O com.ibm.websphere.objectgrid.ssecurity.plugins.builtins. WSTokenCredentialGenerator representa um gerenciador de credenciais (token de segurança) ao executar no WebSphere Application Server. Quando o método getCredential é chamado, o Subject associado ao encadeamento atual é recuperado. Em seguida, as informações de segurança neste objeto Subject são convertidas em um objeto WSTokenCredential. É possível especificar se deseja recuperar um subject runAs ou um subject responsável pela chamada do encadeamento, utilizando a constante WSTokenCredentialGenerator.RUN_AS_SUBJECT ou WSTokenCredentialGenerator.CALLER_SUBJECT.

UserPasswordCredential e UserPasswordCredentialGenerator

Para propósitos de teste, o WebSphere eXtreme Scale fornece as seguintes implementações de plug-in:

1. `com.ibm.websphere.objectgrid.security.plugins.builtins.UserPasswordCredential`
2. `com.ibm.websphere.objectgrid.security.plugins.builtins.UserPasswordCredentialGenerator`

A credencial de senha do usuário armazena um ID de usuário e uma senha. O gerador de credenciais de senha de usuário contém este ID de usuário e senha.

O código de exemplo a seguir mostra como implementar estes dois plug-ins.

UserPasswordCredential.java

```
// This sample program is provided AS IS and may be used, executed, copied and modified
// without royalty payment by customer
// (a) for its own instruction and study,
// (b) in order to develop applications designed to run with an IBM WebSphere product,
// either for customer's own internal use or for redistribution by customer, as part of such an
// application, in customer's own products.
// Licensed Materials - Property of IBM
// 5724-J34 © COPYRIGHT International Business Machines Corp. 2007
package com.ibm.websphere.objectgrid.security.plugins.builtins;

import com.ibm.websphere.objectgrid.security.plugins.Credential;

/**
 * This class represents a credential containing a user ID and password.
 *
 * @ibm-api
 * @since WAS XD 6.0.1
 *
 * @see Credential
 * @see UserPasswordCredentialGenerator#getCredential()
 */
public class UserPasswordCredential implements Credential {

    private static final long serialVersionUID = 1409044825541007228L;

    private String ivUserName;

    private String ivPassword;

    /**
     * Creates a UserPasswordCredential with the specified user name and
     * password.
     *
     * @param userName the user name for this credential
     * @param password the password for this credential
     *
     * @throws IllegalArgumentException if userName or password is <code>null</code>
     */
    public UserPasswordCredential(String userName, String password) {
        super();
        if (userName == null || password == null) {
            throw new IllegalArgumentException("User name and password cannot be null.");
        }
        this.ivUserName = userName;
        this.ivPassword = password;
    }
```

```
    /**
     * Gets the user name for this credential.
     *
     * @return   the user name argument that was passed to the constructor
     *           or the <code>setUserName(String)</code>
     *           method of this class
     *
     * @see #setUserName(String)
     */
    public String getUserName() {
        return ivUserName;
    }

    /**
     * Sets the user name for this credential.
     *
     * @param userName the user name to set.
     *
     * @throws IllegalArgumentException if userName is <code>null</code>
     */
    public void setUserName(String userName) {
        if (userName == null) {
            throw new IllegalArgumentException("User name cannot be null.");
        }
        this.ivUserName = userName;
    }

    /**
     * Gets the password for this credential.
     *
     * @return   the password argument that was passed to the constructor
     *           or the <code>setPassword(String)</code>
     *           method of this class
     *
     * @see #setPassword(String)
     */
    public String getPassword() {
        return ivPassword;
    }

    /**
     * Sets the password for this credential.
     *
     * @param password the password to set.
     *
     * @throws IllegalArgumentException if password is <code>null</code>
     */
    public void setPassword(String password) {
        if (password == null) {
            throw new IllegalArgumentException("Password cannot be null.");
        }
        this.ivPassword = password;
    }

    /**
     * Checks two UserPasswordCredential objects for equality.
     * <p>
     * Two UserPasswordCredential objects are equal if and only if their user names
     * and passwords are equal.
     *
     * @param o the object we are testing for equality with this object.
     *
     * @return <code>true</code> if both UserPasswordCredential objects are equivalent.
     *
     * @see Credential#equals(Object)
     */
    public boolean equals (Object o)  {
        if (this == o) {
            return true;
        }
        if (o instanceof UserPasswordCredential) {
            UserPasswordCredential other = (UserPasswordCredential) o;
            return other.ivPassword.equals(ivPassword) && other.ivUserName.equals(ivUserName);
        }

        return false;
    }

    /**
     * Returns the hashcode of the UserPasswordCredential object.
     *
     * @return the hash code of this object
     *
     * @see Credential#hashCode()
     */
    public int hashCode ()  {
        return ivUserName.hashCode() + ivPassword.hashCode();
    }
}
```

UserPasswordCredentialGenerator.java

```
// This sample program is provided AS IS and may be used, executed, copied and modified
// without royalty payment by customer
// (a) for its own instruction and study,
// (b) in order to develop applications designed to run with an IBM WebSphere product,
// either for customer's own internal use or for redistribution by customer, as part of such an
// application, in customer's own products.
// Licensed Materials - Property of IBM
// 5724-J34 © COPYRIGHT International Business Machines Corp. 2007
package com.ibm.websphere.objectgrid.security.plugins.builtins;

import java.util.StringTokenizer;

import com.ibm.websphere.objectgrid.security.plugins.Credential;
import com.ibm.websphere.objectgrid.security.plugins.CredentialGenerator;

/**
 * This credential generator creates <code>UserPasswordCredential</code> objects.
 * <p>
 * UserPasswordCredentialGenerator has a one to one relationship with
 * UserPasswordCredential because it can only create a UserPasswordCredential
 * representing one identity.
 *
 * @since WAS XD 6.0.1
 * @ibm-api
 *
 * @see CredentialGenerator
 * @see UserPasswordCredential
 */
public class UserPasswordCredentialGenerator implements CredentialGenerator {

    private String ivUser;

    private String ivPwd;

    /**
     * Creates a UserPasswordCredentialGenerator with no user name or password.
     *
     * @see #setProperties(String)
     */
    public UserPasswordCredentialGenerator() {
        super();
    }

    /**
     * Creates a UserPasswordCredentialGenerator with a specified user name and
     * password
     *
     * @param user the user name
     * @param pwd the password
     */
    public UserPasswordCredentialGenerator(String user, String pwd) {
        ivUser = user;
        ivPwd = pwd;
    }

    /**
     * Creates a new <code>UserPasswordCredential</code> object using this
     * object's user name and password.
     *
     * @return a new <code>UserPasswordCredential</code> instance
     *
     * @see CredentialGenerator#getCredential()
     * @see UserPasswordCredential
     */
    public Credential getCredential() {
        return new UserPasswordCredential(ivUser, ivPwd);
    }

    /**
     * Gets the password for this credential generator.
     *
     * @return   the password argument that was passed to the constructor
     */
    public String getPassword() {
        return ivPwd;
    }

    /**
     * Gets the user name for this credential.
     *
     * @return   the user argument that was passed to the constructor
     *           of this class
     */
    public String getUserName() {
        return ivUser;
    }
    /**
     * Sets additional properties namely a user name and password.
     *
     * @param properties a properties string  with a user name and
```

```
     *                  a password separated by a blank.
     *
     * @throws IllegalArgumentException if the format is not valid
     */
    public void setProperties(String properties) {
        StringTokenizer token = new StringTokenizer(properties, " ");
        if (token.countTokens() != 2) {
            throw new IllegalArgumentException(
                "The properties should have a user name and password and separated by a blank.");
        }

        ivUser = token.nextToken();
        ivPwd = token.nextToken();
    }
    /**
     * Checks two UserPasswordCredentialGenerator objects for equality.
     * <p>
     * Two UserPasswordCredentialGenerator objects are equal if and only if
     * their user names and passwords are equal.
     *
     * @param obj the object we are testing for equality with this object.
     *
     * @return <code>true</code> if both UserPasswordCredentialGenerator objects
     *         are equivalent.
     */
    public boolean equals(Object obj) {
        if (obj == this) {
            return true;
        }

        if (obj != null && obj instanceof UserPasswordCredentialGenerator) {
            UserPasswordCredentialGenerator other = (UserPasswordCredentialGenerator) obj;

            boolean bothUserNull = false;
            boolean bothPwdNull = false;

            if (ivUser == null) {
                if (other.ivUser == null) {
                    bothUserNull = true;
                } else {
                    return false;
                }
            }

            if (ivPwd == null) {
                if (other.ivPwd == null) {
                    bothPwdNull = true;
                } else {
                    return false;
                }
            }

            return (bothUserNull || ivUser.equals(other.ivUser)) && (bothPwdNull || ivPwd.equals(other.ivPwd));
        }

        return false;
    }

    /**
     * Returns the hashcode of the UserPasswordCredentialGenerator object.
     *
     * @return the hash code of this object
     */
    public int hashCode ()  {

        return ivUser.hashCode() + ivPwd.hashCode();
    }

}
```

A classe UserPasswordCredential contém dois atributos: nome de usuário e senha. O UserPasswordCredentialGenerator serve como uma factory que contém os objetos UserPasswordCredential.

WSTokenCredential e WSTokenCredentialGenerator

Quando os clientes e servidores do WebSphere eXtreme Scale são todos implementados no WebSphere Application Server, o aplicativo cliente pode usar estas duas implementações integradas quando as seguintes condições forem satisfeitas:

1. A segurança global do WebSphere Application Server estiver ativada.

2. Todos os clientes e servidores do WebSphere eXtreme Scale estão em execução no WebSphere Application Server Java Virtual Machines.
3. Os servidores de aplicativos estiverem no mesmo domínio de segurança.
4. O cliente já estiver autenticado no WebSphere Application Server.

Nesta situação, o cliente pode usar a classe com.ibm.websphere.objectgrid.ssecurity.plugins.builtins. WSTokenCredentialGenerator para gerenciar uma credencial. O servidor usa a classe de implementação WSAuthenticator para autenticar a credencial.

Este cenário aproveita as vantagens do fato de que o cliente do eXtreme Scale já ter sido autenticado. Como os servidores de aplicativos que possuem servidores estão no mesmo domínio de segurança que os servidores de aplicativos que hospedam os clientes, os tokens de segurança podem ser propagados do cliente para o servidor para que o mesmo registro de usuário não precise ser autenticado novamente.

Nota: Não assuma que um CredentialGenerator sempre gera a mesma credencial. Para uma credencial expirável e atualizável, o CredentialGenerator deve poder gerar a credencial válida mais recente para certificar-se de que a autenticação foi bem-sucedida. Um exemplo é usar o bilhete Kerberos como um objeto Credential. Quando o bilhete Kerberos é atualizado, o CredentialGenerator deve recuperar o bilhete atualizado quando o CredentialGenerator.getCredential é chamado.

Plug-in Authenticator

Após o cliente do eXtreme Scale recuperar o objeto Credential utilizando o objeto CredentialGenerator, este objeto Credential do cliente é enviado junto o pedido do cliente para o servidor eXtreme Scale. O servidor autentica o objeto de Credencial antes de processar a solicitação. Se o objeto Credential for autenticado com êxito, um objeto Subject será retornado para representar este cliente.

Este objeto Subject é então armazenado em cache e expira após seu tempo de vida alcançar o valor de tempo limite da sessão. O valor de tempo limite da sessão de login pode ser configurado utilizando a propriedade loginSessionExpirationTime no arquivo XML do cluster. Por exemplo, configurar `loginSessionExpirationTime="300"` fará com que o objeto Subject expire em 300 segundos.

Esse objeto Subject é, então, utilizado para autorizar o pedido, que é mostrado posteriormente. Um servidor eXtreme Scale utiliza o plug-in do Autenticador para autenticar o objeto Credential. Consulte Authenticator para obter mais detalhes.

O plug-in Autenticador é onde o tempo de execução do eXtreme Scale autentica o objeto Credential a partir do registro do usuário do cliente como, por exemplo, um servidor protocolo LDAP (Lightweight Directory Access Protocol).

O WebSphere eXtreme Scale não fornece uma configuração de registro do usuário disponível imediatamente. A configuração e o gerenciamento do registro do usuário são deixados fora do WebSphere eXtreme Scale para simplificação e flexibilidade. Este plug-in implementa a conexão e a autenticação com o registro do usuário. Por exemplo, uma implementação do Autenticador extrai o ID do usuário e a senha da credencial, utiliza-os para conectar-se e validar em um servidor LDAP

e cria um objeto Subject como resultado da autenticação. A implementação pode usar módulos de login JAAS. Um objeto Subject é retornado como resultado de autenticação.

Observe que este método cria duas exceções: InvalidCredentialException e ExpiredCredentialException. A exceção InvalidCredentialException indica que a credencial não é válida. A exceção ExpiredCredentialException indica que a credencial expirou. Se uma destas duas exceções resultar do método authenticate, as exceções serão enviadas de volta para o cliente. Porém, o tempo de execução do cliente manipula estas duas exceções diferentemente:

- Se o erro for uma exceção InvalidCredentialException, o tempo de execução do cliente exibe esta exceção. Seu aplicativo deve tratar a exceção. É possível corrigir o CredentialGenerator, por exemplo, e em seguida tentar a operação novamente.
- Se o erro for uma exceção ExpiredCredentialException, e a quantidade de novas tentativas não for 0, o tempo de execução do cliente chama o método CredentialGenerator.getCredential novamente, e envia o novo objeto Credential para o servidor. Se a nova autenticação de credencial for bem-sucedida, o servidor processará o pedido. Se a nova autenticação da credencial falhar, a exceção será enviada de volta para o cliente. Se o número de novas tentativas de autenticação atingir o valor suportado e o cliente ainda receber uma exceção ExpiredCredentialException, resultará na exceção ExpiredCredentialException. O aplicativo deve tratar o erro.

A interface Authenticator oferece grande flexibilidade. É possível implementar a interface Authenticator de sua própria maneira específica. Por exemplo, é possível implementar essa interface para suportar dois registros do usuário diferentes.

O WebSphere eXtreme Scale oferece amostra de implementações de plug-in do autenticador. Exceto para o plug-in do autenticador do WebSphere Application Server, as outras implementações são apenas amostras para fins de teste.

KeyStoreLoginAuthenticator

Este exemplo usa uma implementação integrada do eXtreme Scale: KeyStoreLoginAuthenticator, que é para propósitos de teste e amostra (um keystore é um simples registro do usuário e não deve ser usado para um ambiente de produção). Novamente, a classe é exibida para demonstrar melhor como implementar um autenticador.

KeyStoreLoginAuthenticator.java

```
// This sample program is provided AS IS and may be used, executed, copied and modified
// without royalty payment by customer
// (a) for its own instruction and study,
// (b) in order to develop applications designed to run with an IBM WebSphere product,
// either for customer's own internal use or for redistribution by customer, as part of such an
// application, in customer's own products.
// Licensed Materials - Property of IBM
// 5724-J34 © COPYRIGHT International Business Machines Corp. 2007

package com.ibm.websphere.objectgrid.security.plugins.builtins;

import javax.security.auth.Subject;
import javax.security.auth.login.LoginContext;
import javax.security.auth.login.LoginException;

import com.ibm.websphere.objectgrid.security.plugins.Authenticator;
import com.ibm.websphere.objectgrid.security.plugins.Credential;
import com.ibm.websphere.objectgrid.security.plugins.ExpiredCredentialException;
import com.ibm.websphere.objectgrid.security.plugins.InvalidCredentialException;
import com.ibm.ws.objectgrid.Constants;
import com.ibm.ws.objectgrid.ObjectGridManagerImpl;
import com.ibm.ws.objectgrid.security.auth.callback.UserPasswordCallbackHandlerImpl;

/**
 * This class is an implementation of the <code>Authenticator</code> interface
```

```
 * when a user name and password are used as a credential.
 * <p>
 * When user ID and password authentication is used, the credential passed to the
 * <code>authenticate(Credential)</code> method is a UserPasswordCredential object.
 * <p>
 * This implementation will use a <code>KeyStoreLoginModule</code> to authenticate
 * the user into the keystore using the JAAS login module "KeyStoreLogin". The key
 * store can be configured as an option to the <code>KeyStoreLoginModule</code>
 * class. Please see the <code>KeyStoreLoginModule</code> class for more details
 * about how to set up the JAAS login configuration file.
 * <p>
 * This class is only for sample and quick testing purpose. Users should
 * write your own Authenticator implementation which can fit better into
 * the environment.
 *
 * @ibm-api
 * @since WAS XD 6.0.1
 *
 * @see Authenticator
 * @see KeyStoreLoginModule
 * @see UserPasswordCredential
 */
public class KeyStoreLoginAuthenticator implements Authenticator {

    /**
     * Creates a new KeyStoreLoginAuthenticator.
     */
    public KeyStoreLoginAuthenticator() {
        super();
    }

    /**
     * Authenticates a <code>UserPasswordCredential</code>.
     * <p>
     * Uses the user name and password from the specified UserPasswordCredential
     * to login to the KeyStoreLoginModule named "KeyStoreLogin".
     *
     * @throws InvalidCredentialException if credential isn't a
     *         UserPasswordCredential or some error occurs during processing
     *         of the supplied UserPasswordCredential
     *
     * @throws ExpiredCredentialException if credential is expired.  This exception
     *         is not used by this implementation
     *
     * @see Authenticator#authenticate(Credential)
     * @see KeyStoreLoginModule
     */
    public Subject authenticate(Credential credential) throws InvalidCredentialException, ExpiredCredentialException {

        if (credential == null) {
            throw new InvalidCredentialException("Supplied credential is null");
        }

        if ( ! (credential instanceof UserPasswordCredential) ) {
            throw new InvalidCredentialException("Supplied credential is not a UserPasswordCredential");
        }

        UserPasswordCredential cred = (UserPasswordCredential) credential;
        LoginContext lc = null;
        try {
            lc = new LoginContext("KeyStoreLogin",
                    new UserPasswordCallbackHandlerImpl(cred.getUserName(), cred.getPassword().toCharArray()));

            lc.login();

            Subject subject = lc.getSubject();

            return subject;
        }
        catch (LoginException le) {
            throw new InvalidCredentialException(le);
        }
        catch (IllegalArgumentException ile) {
            throw new InvalidCredentialException(ile);
        }
    }
}
```

KeyStoreLoginModule.java

```
// This sample program is provided AS IS and may be used, executed, copied and modified
// without royalty payment by customer
// (a) for its own instruction and study,
// (b) in order to develop applications designed to run with an IBM WebSphere product,
// either for customer's own internal use or for redistribution by customer, as part of such an
// application, in customer's own products.
// Licensed Materials - Property of IBM
// 5724-J34 © COPYRIGHT International Business Machines Corp. 2007
package com.ibm.websphere.objectgrid.security.plugins.builtins;

import java.io.File;
import java.io.FileInputStream;
import java.security.KeyStore;
```

```
import java.security.KeyStoreException;
import java.security.NoSuchAlgorithmException;
import java.security.PrivateKey;
import java.security.UnrecoverableKeyException;
import java.security.cert.Certificate;
import java.security.cert.CertificateException;
import java.security.cert.CertificateFactory;
import java.security.cert.X509Certificate;
import java.util.Arrays;
import java.util.HashSet;
import java.util.Map;
import java.util.Set;

import javax.security.auth.Subject;
import javax.security.auth.callback.Callback;
import javax.security.auth.callback.CallbackHandler;
import javax.security.auth.callback.NameCallback;
import javax.security.auth.callback.PasswordCallback;
import javax.security.auth.login.LoginException;
import javax.security.auth.spi.LoginModule;
import javax.security.auth.x500.X500Principal;
import javax.security.auth.x500.X500PrivateCredential;

import com.ibm.websphere.objectgrid.ObjectGridRuntimeException;
import com.ibm.ws.objectgrid.Constants;
import com.ibm.ws.objectgrid.ObjectGridManagerImpl;
import com.ibm.ws.objectgrid.util.ObjectGridUtil;

/**
 * A KeyStoreLoginModule is keystore authentication login module based on
 * JAAS authentication.
 * <p>
 * A login configuration should provide an option "<code>keyStoreFile</code>" to
 * indicate where the keystore file is located. If the <code>keyStoreFile</code>
 * value contains a system property in the form, <code>${system.property}</code>,
 * it will be expanded to the value of the system property.
 * <p>
 * If an option "<code>keyStoreFile</code>" is not provided, the default keystore
 * file name is <code>"${java.home}${/}.keystore"</code>.
 * <p>
 * Here is a Login module configuration example:
 * <pre><code>
 *    KeyStoreLogin {
 *        com.ibm.websphere.objectgrid.security.plugins.builtins.KeystoreLoginModule required
 *            keyStoreFile="${user.dir}${/}security${/}.keystore";
 *    };
 * </code></pre>
 *
 * @ibm-api
 * @since WAS XD 6.0.1
 *
 * @see LoginModule
 */
public class KeyStoreLoginModule implements LoginModule {

    private static final String CLASS_NAME = KeyStoreLoginModule.class.getName();

    /**
     * keystore file property name
     */
    public static final String KEY_STORE_FILE_PROPERTY_NAME = "keyStoreFile";

    /**
     * keystore type. Only JKS is supported
     */
    public static final String KEYSTORE_TYPE = "JKS";

    /**
     * The default keystore file name
     */
    public static final String DEFAULT_KEY_STORE_FILE = "${java.home}${/}.keystore";

    private CallbackHandler handler;

    private Subject subject;

    private boolean debug = false;

    private Set principals = new HashSet();

    private Set publicCreds = new HashSet();

    private Set privateCreds = new HashSet();

    protected KeyStore keyStore;

    /**
     * Creates a new KeyStoreLoginModule.
     */
    public KeyStoreLoginModule() {
    }
```

```
/**
 * Initializes the login module.
 *
 * @see LoginModule#initialize(Subject, CallbackHandler, Map, Map)
 */
public void initialize(Subject sub, CallbackHandler callbackHandler,
        Map mapSharedState, Map mapOptions) {

    // initialize any configured options
    debug = "true".equalsIgnoreCase((String) mapOptions.get("debug"));

    if (sub == null)
        throw new IllegalArgumentException("Subject is not specified");

    if (callbackHandler == null)
        throw new IllegalArgumentException(
        "CallbackHander is not specified");

    // Get the keystore path
    String sKeyStorePath = (String) mapOptions
        .get(KEY_STORE_FILE_PROPERTY_NAME);

    // If there is no keystore path, the default one is the .keystore
    // file in the java home directory
    if (sKeyStorePath == null) {
        sKeyStorePath = DEFAULT_KEY_STORE_FILE;
    }

    // Replace the system enviroment variable
    sKeyStorePath = ObjectGridUtil.replaceVar(sKeyStorePath);

    File fileKeyStore = new File(sKeyStorePath);

    try {
        KeyStore store = KeyStore.getInstance("JKS");
        store.load(new FileInputStream(fileKeyStore), null);

        // Save the keystore
        keyStore = store;

        if (debug) {
            System.out.println("[KeyStoreLoginModule] initialize: Successfully loaded keystore");
        }
    }
    catch(Exception e){
        ObjectGridRuntimeException re = new ObjectGridRuntimeException(
                "Failed to load keystore: " + fileKeyStore.getAbsolutePath());
        re.initCause(e);
        if (debug) {
            System.out.println("[KeyStoreLoginModule] initialize: keystore loading failed with exception "
                    + e.getMessage());
        }
    }

    this.subject = sub;
    this.handler = callbackHandler;
}

/**
 * Authenticates a user based on the keystore file.
 *
 * @see LoginModule#login()
 */
public boolean login() throws LoginException {

    if (debug) {
        System.out.println("[KeyStoreLoginModule] login: entry");
    }

    String name = null;
    char pwd[] = null;

    if (keyStore == null || subject == null || handler == null) {
        throw new LoginException("Module initialization failed");
    }

    NameCallback nameCallback = new NameCallback("Username:");
    PasswordCallback pwdCallback = new PasswordCallback("Password:", false);

    try {
        handler.handle(new Callback[] { nameCallback, pwdCallback });
    }
    catch(Exception e){
        throw new LoginException("Callback failed: " + e);
    }

    name = nameCallback.getName();
    char[] tempPwd = pwdCallback.getPassword();

    if (tempPwd == null) {
```

```
            // treat a NULL password as an empty password
            tempPwd = new char[0];
        }
        pwd = new char[tempPwd.length];
        System.arraycopy(tempPwd, 0, pwd, 0, tempPwd.length);

        pwdCallback.clearPassword();

        if (debug) {
            System.out.println("[KeyStoreLoginModule] login: "
                    + "user entered user name: " + name);
        }

        // Validate the user name and password
        try {
            validate(name, pwd);
        }
        catch (SecurityException se) {
            principals.clear();
            publicCreds.clear();
            privateCreds.clear();
            LoginException le = new LoginException(
            "Exception encountered during login");
            le.initCause(se);

            throw le;
        }

        if (debug) {
            System.out.println("[KeyStoreLoginModule] login: exit");
        }
        return true;
    }

    /**
     * Indicates the user is accepted.
     * <p>
     * This method is called only if the user is authenticated by all modules in
     * the login configuration file. The principal objects will be added to the
     * stored subject.
     *
     * @return false if for some reason the principals cannot be added; true
     *         otherwise
     *
     * @exception LoginException
     *                LoginException is thrown if the subject is readonly or if
     *                any unrecoverable exceptions is encountered.
     *
     * @see LoginModule#commit()
     */
    public boolean commit() throws LoginException {
        if (debug) {
            System.out.println("[KeyStoreLoginModule] commit: entry");
        }

        if (principals.isEmpty()) {
            throw new IllegalStateException("Commit is called out of sequence");
        }

        if (subject.isReadOnly()) {
            throw new LoginException("Subject is Readonly");
        }

        subject.getPrincipals().addAll(principals);
        subject.getPublicCredentials().addAll(publicCreds);
        subject.getPrivateCredentials().addAll(privateCreds);

        principals.clear();
        publicCreds.clear();
        privateCreds.clear();

        if (debug) {
            System.out.println("[KeyStoreLoginModule] commit: exit");
        }
        return true;
    }

    /**
     * Indicates the user is not accepted
     *
     * @see LoginModule#abort()
     */
    public boolean abort() throws LoginException {
        boolean b = logout();
        return b;
    }

    /**
     * Logs the user out. Clear all the maps.
     *
     * @see LoginModule#logout()
```

```
 */
public boolean logout() throws LoginException {


    // Clear the instance variables
    principals.clear();
    publicCreds.clear();
    privateCreds.clear();

    // clear maps in the subject
    if (!subject.isReadOnly()) {
        if (subject.getPrincipals() != null) {
            subject.getPrincipals().clear();
        }

        if (subject.getPublicCredentials() != null) {
            subject.getPublicCredentials().clear();
        }

        if (subject.getPrivateCredentials() != null) {
            subject.getPrivateCredentials().clear();
        }
    }
    return true;
}

/**
 * Validates the user name and password based on the keystore.
 *
 * @param userName user name
 * @param password password
 * @throws SecurityException if any exceptions encountered
 */
private void validate(String userName, char password[])
    throws SecurityException {

    PrivateKey privateKey = null;

    // Get the private key from the keystore
    try {
        privateKey = (PrivateKey) keyStore.getKey(userName, password);
    }
    catch (NoSuchAlgorithmException nsae) {
        SecurityException se = new SecurityException();
        se.initCause(nsae);
        throw se;
    }
    catch (KeyStoreException kse) {
        SecurityException se = new SecurityException();
        se.initCause(kse);
        throw se;
    }
    catch (UnrecoverableKeyException uke) {
        SecurityException se = new SecurityException();
        se.initCause(uke);
        throw se;
    }

    if (privateKey == null) {
        throw new SecurityException("Invalid name: " + userName);
    }

    // Check the certificats
    Certificate certs[] = null;
    try {
        certs = keyStore.getCertificateChain(userName);
    }
    catch (KeyStoreException kse) {
        SecurityException se = new SecurityException();
        se.initCause(kse);
        throw se;
    }

    if (debug) {
        System.out.println("  Print out the certificates:");
        for (int i = 0; i < certs.length; i++) {
            System.out.println("  certificate " + i);
            System.out.println("    " + certs[i]);
        }
    }

    if (certs != null && certs.length > 0) {

        // If the first certificate is an X509Certificate
        if (certs[0] instanceof X509Certificate) {
            try {
                // Get the first certificate which represents the user
                X509Certificate certX509 = (X509Certificate) certs[0];

                // Create a principal
                X500Principal principal = new X500Principal(certX509
```

```
                        .getIssuerDN()
                        .getName());
                principals.add(principal);

                if (debug) {
                    System.out.println("  Principal added: " + principal);
                }
                // Create the certification path object and add it to the
                // public credential set
                CertificateFactory factory = CertificateFactory
                    .getInstance("X.509");
                java.security.cert.CertPath certPath = factory
                    .generateCertPath(Arrays.asList(certs));
                publicCreds.add(certPath);

                // Add the private credential to the private credential set
                privateCreds.add(new X500PrivateCredential(certX509,
                        privateKey, userName));

            }
            catch (CertificateException ce) {
                SecurityException se = new SecurityException();
                se.initCause(ce);
                throw se;
            }
        }
        else {
            // The first certificate is not an X509Certificate
            // We just add the certificate to the public credential set
            // and the private key to the private credential set.
            publicCreds.add(certs[0]);
            privateCreds.add(privateKey);
        }
    }
  }
}
```

Uso do Plug-in do Autenticador LDAP

Você recebe a implementação padrão do com.ibm.websphere .plugins.builtins.LDAPAuthenticator para manipular a autenticação de nome do usuário e senha para um servidor LDAP. Esta implementação usa o módulo de login LDAPLogin para efetuar login do usuário em um servidor LDAP (Lightweight Directory Access Protocol). O fragmento a seguir demonstra como o método authenticate é implementado:

```
/**
* @see com.ibm.ws.objectgrid.security.plugins.Authenticator#
* authenticate(LDAPLogin)
*/
public Subject authenticate(Credential credential) throws
InvalidCredentialException, ExpiredCredentialException {

    UserPasswordCredential cred = (UserPasswordCredential) credential;
    LoginContext lc = null;
    try {
        lc = new LoginContext("LDAPLogin",
            new UserPasswordCallbackHandlerImpl(cred.getUserName(),
            cred.getPassword().toCharArray()));

        lc.login();

        Subject subject = lc.getSubject();

        return subject;
    }
    catch (LoginException le) {
        throw new InvalidCredentialException(le);
    }
    catch (IllegalArgumentException ile) {
        throw new InvalidCredentialException(ile);
    }
}
```

Além disso, o eXtreme Scale envia um módulo de login com.ibm.websphere.objectgrid.security.plugins.builtins.LDAPLoginModule para esta finalidade. Você deve fornecer as duas opções a seguir no arquivo de configuração de login JAAS.

- providerURL: A URL do provedor do servidor LDAP

- factoryClass: A classe de implementação do depósito de informações do contexto do LDAP

O módulo LDAPLoginModule chama o método com.ibm.websphere .plugins.builtins.LDAPAuthentcationHelper.authenticate. O trecho de código a seguir mostra como é possível implementar o método authenticate do LDAPAuthenticationHelper.

```
/**
* Authenticate the user to the LDAP directory.
* @param user the user ID, e.g., uid=xxxxxx,c=us,ou=bluepages,o=ibm.com
* @param pwd the password
*
* @throws NamingException
*/
public String[] authenticate(String user, String pwd)
throws NamingException {
    Hashtable env = new Hashtable();
    env.put(Context.INITIAL_CONTEXT_FACTORY, factoryClass);
    env.put(Context.PROVIDER_URL, providerURL);
    env.put(Context.SECURITY_PRINCIPAL, user);
    env.put(Context.SECURITY_CREDENTIALS, pwd);
    env.put(Context.SECURITY_AUTHENTICATION, "simple");

    InitialContext initialContext = new InitialContext(env);

    // Look up for the user
    DirContext dirCtx = (DirContext) initialContext.lookup(user);

    String uid = null;
    int iComma = user.indexOf(",");
    int iEqual = user.indexOf("=");
    if (iComma > 0 && iComma > 0) {
        uid = user.substring(iEqual + 1, iComma);
    }
    else {
        uid = user;
    }

    Attributes attributes = dirCtx.getAttributes("");

    // Check the UID
    String thisUID = (String) (attributes.get(UID).get());

    String thisDept = (String) (attributes.get(HR_DEPT).get());

    if (thisUID.equals(uid)) {
        return new String[] { thisUID, thisDept };
    }
    else {
        return null;
    }
}
```

Se a autenticação for bem-sucedida, o ID e a senha serão considerados válidos. Então o módulo de login obtém as informações de ID e informações do departamento a partir deste método authenticate. O módulo de login cria dois proprietários: SimpleUserPrincipal e SimpleDeptPrincipal. É possível utilizar o subject autenticado para autorização de grupo (neste caso, o departamento é um grupo) e para autorização individual.

O exemplo a seguir mostra uma configuração de módulo de login utilizado para efetuar login no servidor LDAP:

```
LDAPLogin { com.ibm.websphere.objectgrid.security.plugins.builtins.LDAPLoginModule required
    providerURL="ldap://directory.acme.com:389/"
    factoryClass="com.sun.jndi.ldap.LdapCtxFactory";
};
```

Na configuração anterior, o servidor LDAP aponta para `ldap://directory.acme.com:389/server`. Altere esta configuração para seu servidor LDAP. Este módulo de login usa o ID e a senha fornecidos para se conectar ao servidor LDAP. Esta implementação serve apenas para fins de teste.

Utilização do Plug-in Autenticador do WebSphere Application Server

Além disso, o eXtreme Scale fornece a implementação integrada do com.ibm.websphere.objectgrid.security.plugins.builtins.WSTokenAuthenticator para usar a infraestrutura de segurança do WebSphere Application Server. Esta implementação integrada pode ser usada quando as seguintes condições forem verdadeiras.

1. A segurança global do WebSphere Application Server estiver ativada.
2. Todos os clientes e servidores eXtreme Scale tiverem sido ativados nos JVMs do WebSphere Application Server.
3. Estes servidores de aplicativos estão no mesmo domínio de segurança.
4. O cliente do eXtreme Scale já estiver autenticado no WebSphere Application Server.

O cliente pode usar a classe com.ibm.websphere.objectgrid.ssecurity.plugins.builtins. WSTokenCredentialGenerator para gerar uma credencial. O servidor usa esta classe de implementação Authenticator para autenticar a credencial. Se o token for autenticado com êxito, será retornado um objeto Subject.

Este cenário tira vantagens do fato de o cliente já ter sido autenticado. Como os servidores de aplicativos que possuem servidores estão no mesmo domínio de segurança que os servidores de aplicativos que hospedam os clientes, os tokens de segurança podem ser propagados do cliente para o servidor para que o mesmo registro de usuário não precise ser autenticado novamente.

Utilização do Plug-in Autenticador do Tivoli Access Manager

O Tivoli Access Manager é amplamente utilizado como um servidor de segurança. Também é possível implementar o Authenticator usando os módulos de login fornecidos pelo Tivoli Access Manager.

Para autenticar um usuário para o Tivoli Access Manager, aplique o módulo de login com.tivoli.mts.PDLoginModule, o que exige que o aplicativo que efetua a chamada forneça as seguintes informações:

1. Um nome de proprietário, especificado como um nome abreviado ou um nome X.500 (DN)
2. Uma senha

O módulo de login autentica o shard primário e retorna a credencial do Tivoli Access Manager. O módulo espera que o aplicativo de chamada forneça as seguintes informações:

1. O nome de usuário, por meio de um objeto javax.security.auth.callback.NameCallback.
2. A senha, por meio de um objeto javax.security.auth.callback.PasswordCallback.

Quando a credencial do Tivoli Access Manager é recuperada com êxito, o JAAS LoginModule cria um Subject e um PDPrincipal. Nenhum módulo integrado para autenticação do Tivoli Access Manager é fornecido pois ele está apenas com o módulo PDLoginModule. Consulte a Autorização do IBM Tivoli Access Manager Java Classes Developer Reference para obter mais detalhes.

Conexão Segura com o WebSphere eXtreme Scale

Para se conectar um cliente do eXtreme Scale seguramente a um servidor, é possível usar qualquer método de conexão na interface ObjectGridManager que usa um objeto do ClientSecurityConfiguration. A seguir a um breve exemplo.

```
public ClientClusterContext connect(String catalogServerEndpoints,
   ClientSecurityConfiguration securityProps,
     URL overRideObjectGridXml) throws ConnectException;
```

Este método usa um parâmetro do tipo ClientSecurityConfiguration, que é uma interface representando uma configuração de segurança do cliente. É possível usar a API pública do com.ibm.websphere.objectgrid.security.config.ClientSecurityConfigurationFactory para criar uma instância com valores padrão, ou é possível criar uma instância por meio da transmissão do arquivo de propriedades do cliente do WebSphere eXtreme Scale. Este arquivo contém as seguintes propriedades que estão relacionadas à autenticação. O valor marcado com um sinal de mais (+) é o padrão.

- `securityEnabled (true, false+):` Esta propriedade indica se a segurança está ativada. Quando um cliente se conecta a um servidor, os valores de securityEnabled no lado do cliente e do servidor devem ser ambos `true` ou ambos `false`. Por exemplo, se a segurança do servidor conectado estiver ativada, o cliente terá que configurar esta propriedade como true para conectar-se ao servidor.
- authenticationRetryCount (um valor de número inteiro, 0+): Esta propriedade determina quantas novas tentativas devem ser feitas para efetuar login quando uma credencial tiver expirado. Se o valor for 0, nenhuma nova tentativa será feita. A nova tentativa de autenticação se aplicará apenas ao caso em que a credencial tiver expirado. Se a credencial não for válida, não haverá nova tentativa. Seu aplicativo é responsável por tentar a operação novamente.

Após criar um objeto com.ibm.websphere.objectgrid.security.config.ClientSecurityConfiguration, configure o objeto credentialGenerator no cliente utilizando o seguinte método:

```
/**
* Configure o objeto {@link CredentialGenerator} para este cliente.
* @param generator o objeto CredentialGenerator associado a este cliente
*/
void setCredentialGenerator(CredentialGenerator generator);
```

É possível configurar o objeto CredentialGenerator no arquivo de propriedades do cliente do WebSphere eXtreme Scale também, da seguinte forma.

- credentialGeneratorClass: O nome da implementação da classe para o objeto CredentialGenerator. Ele deve ter um construtor padrão.
- credentialGeneratorProps: As propriedades para a classe CredentialGenerator. Se o valor não for nulo, ele será configurado como o objeto CredentialGenerator construído utilizando o método setProperties(String).

A seguir está uma amostra para instanciar um a ClientSecurityConfiguration e, em seguida, utilizá-lo para conectar-se ao servidor.

```
/**
* Obter um ClientClusterContext seguro
* @return um objeto ClientClusterContext seguro
*/
protected ClientClusterContext connect() throws ConnectException {
ClientSecurityConfiguration csConfig = ClientSecurityConfigurationFactory
.getClientSecurityConfiguration("/properties/security.ogclient.props");

UserPasswordCredentialGenerator gen= new
UserPasswordCredentialGenerator("manager", "manager1");

csConfig.setCredentialGenerator(gen);

return objectGridManager.connect(csConfig, null);
}
```

Quando connect é chamado, o cliente do WebSphere eXtreme Scale chama o método CredentialGenerator.getCredential para obter a credencial do cliente. Esta credencial é enviada junto com o pedido de conexão com o servidor para autenticação.

Utilização de uma instância do CredentialGenerator diferente por sessão

Em alguns casos, um cliente do WebSphere eXtreme Scale representa apenas uma identidade do cliente mas, em outros, ele pode representar múltiplas identidades. Aqui há um cenário para o caso mais recente: Um cliente do WebSphere eXtreme Scale é criado e compartilhado em um servidor da web. Todos os servlets neste servidor da web usam este cliente do WebSphere eXtreme Scale. Como cada servlet representa um web client diferente, use credenciais diferentes ao enviar solicitações aos servidores do WebSphere eXtreme Scale.

O WebSphere eXtreme Scale permite a mudança da credencial no nível de sessão. Cada sessão pode usar um objeto CredentialGenerator diferente. Assim, os cenários anteriores podem ser implementados deixando o servlet obter uma sessão com um objeto CredentialGenerator diferente. O exemplo a seguir ilustra o ObjectGrid.getSession(CredentialGenerator)method na interface ObjectGridManager.

```
/**
     * Get a session using a <code>CredentialGenerator</code>.
     * <p>
     * This method can only be called by the ObjectGrid client in an ObjectGrid
     * client server environment. If ObjectGrid is used in a local model, that is,
     * within the same JVM with no client or server existing, <code>getSession(Subject)</code>
     * or the <code>SubjectSource</code> plugin should be used to secure the ObjectGrid.
     *
     * <p>If the <code>initialize()</code> method has not been invoked prior to
     * the first <code>getSession</code> invocation, an implicit initialization
     * will occur.  This ensures that all of the configuration is complete
     * before any runtime usage is required.</p>
     *
     * @param credGen A <code>CredentialGenerator</code> for generating a credential
     *                for the session returned.
     *
     * @return An instance of <code>Session</code>
     *
     * @throws ObjectGridException if an error occurs during processing
     * @throws TransactionCallbackException if the <code>TransactionCallback</code>
     *         throws an exception
     * @throws IllegalStateException if this method is called after the
     *         <code>destroy()</code> method is called.
     *
     * @see #destroy()
     * @see #initialize()
     * @see CredentialGenerator
     * @see Session
     * @since WAS XD 6.0.1
 */
Session getSession(CredentialGenerator credGen) throws
ObjectGridException, TransactionCallbackException;
```

A seguir está um exemplo:

```
ObjectGridManager ogManager = ObjectGridManagerFactory.getObjectGridManager();

CredentialGenerator credGenManager = new UserPasswordCredentialGenerator("manager", "xxxxxx");
CredentialGenerator credGenEmployee = new UserPasswordCredentialGenerator("employee", "xxxxxx");

ObjectGrid og = ogManager.getObjectGrid(ctx, "accounting");

// Get a session with CredentialGenerator;
Session session = og.getSession(credGenManager );

// Get the employee map
ObjectMap om = session.getMap("employee");

// start a transaction.
session.begin();

Object rec1 = map.get("xxxxxx");

session.commit();

// Get another session with a different CredentialGenerator;
session = og.getSession(credGenEmployee );

// Get the employee map
om = session.getMap("employee");

// start a transaction.
session.begin();

Object rec2 = map.get("xxxxx");

session.commit();
```

Se você usar o método ObjectGird.getSession para obter um objeto de Sessão, a sessão usa o conjunto de objetos CredentialGenerator no objeto ClientConfigurationSecurity. O método ObjectGrid.getSession(CredentialGenerator) substitui a configuração CredentialGenerator no objeto ClientSecurityConfiguration.

Se for possível reutilizar o objeto de Sessão, isto resulta em ganho de desempenho. Porém, a chamada do método ObjectGrid.getSession(CredentialGenerator) não é muito cara. A principal sobrecarga é o tempo maior de coleta de lixo do objeto. Certifique-se de liberar as referências quando tiver concluído os objetos Session. Geralmente, se o seu objeto de Sessão puder compartilhar a identidade, tente reutilizar o objeto de Sessão. Se não, utilize o método ObjectGrid.getSession(CredentialGenerator).

Informações relacionadas:

API de Credencial

Programação de Autorização de Cliente

Java

O WebSphere eXtreme Scale suporta a autorização Java Authentication and Authorization Service (JAAS) que está pronta para uso e também suporta a autorização customizada usando a interface ObjectGridAuthorization.

O plug-in ObjectGridAuthorization é usado para autorizar acessos do ObjectGrid, do ObjectMap e do JavaMap aos Principals representados por um objeto Subject de uma maneira customizada. Uma implementação típica deste plug-in é recuperar os Principals do objeto Subject e, em seguida, verificar se as permissões especificadas foram concedidas aos Principals.

Uma permissão passada para o método checkPermission(Subject, Permission) pode ser uma das seguintes permissões:

- MapPermission
- ObjectGridPermission

- ServerMapPermission
- AgentPermission

Consulte a documentação da API do ObjectGridAuthorization para obter detalhes adicionais.

MapPermission

A classe pública com.ibm.websphere.objectgrid.security.MapPermission representa permissões para os recursos ObjectGrid, especificamente os métodos de interfaces theObjectMap ou JavaMap. O WebSphere eXtreme Scale define as seguintes cadeias de permissões para acesso aos métodos de ObjectMap e JavaMap:

- **ler:** Permissão para ler os dados do mapa. A constante de número inteiro é definida como `MapPermission.READ`.
- **gravar:** Permissão para atualizar os dados no mapa. A constante de número inteiro é definida como `MapPermission.WRITE`.
- **inserir:** Permissão para inserir os dados no mapa. A constante de número inteiro é definida como `MapPermission.INSERT`.
- **remover:** Permissão para remover os dados do mapa. A constante de número inteiro é definida como `MapPermission.REMOVE`.
- **invalidar**: Permissão para invalidar os dados a partir do mapa. A constante de número inteiro é definida como `MapPermission.INVALIDATE`.
- **todos:** Todas as permissões acima: ler, gravar, inserir, remover e invalidar. A constante de número inteiro é definida como `MapPermission.ALL`.

Consulte a documentação da API da ServerMapPermission para obter mais detalhes.

É possível construir um objeto MapPermission transmitindo o nome completo do mapa do ObjectGrid (no formato [ObjectGrid_name].[ObjectMap_name]) e a cadeia de permissão ou valor inteiro. Uma cadeia de permissão pode ser uma cadeia delimitada por vírgulas das cadeias de permissão anteriores, tais como read, insert, ou podem ser todas. Um valor de número inteiro de permissão pode ser qualquer constante de número inteiro mencionada anteriormente ou um valor matemático de diversas constantes de permissão de número inteiro, tal como MapPermission.READ | MapPermission.WRITE.

A autorização ocorre quando um método ObjectMap ou JavaMap é chamado. O tempo de execução verifica diferentes permissões para métodos diferentes. Se as permissões requeridas não forem concedidas ao cliente, isso resultará em um AccessControlException.

Tabela 30. Lista de Métodos e a MapPermission Necessária

Permissão	ObjectMap/JavaMap
read	Boolean containsKey(Object)
	Boolean equals(Object)
	Object get(Object)
	Object get(Object, Serializable)
	List getAll(List)
	List getAll(List keyList, Serializable)
	List getAllForUpdate(List)
	List getAllForUpdate(List, Serializable)
	Object getForUpdate(Object)
	Object getForUpdate(Object, Serializable)
	public Object getNextKey(long)
write	Object put(Object key, Object value)
	void put(Object, Object, Serializable)
	void putAll(Map)
	void putAll(Map, Serializable)
	void update(Object, Object)
	void update(Object, Object, Serializable)
insert	public void insert (Object, Object)
	void insert(Object, Object, Serializable)
remove	Object remove (Object)
	void removeAll(Collection)
	void clear()
invalidate	public void invalidate (Object, Boolean)
	void invalidateAll(Collection, Boolean)
	void invalidateUsingKeyword(Serializable)
	int setTimeToLive(int)

A autorização é baseada exclusivamente em qual método é utilizado, ao invés do que o método realmente faz. Por exemplo, um método put pode inserir ou atualizar um registro, dependendo de existir ou não o registro. Entretanto, os casos de inserir ou atualizar não estão discriminados.

Nota: 8.6+ O método setPutMode(PutMode.UPSERT) é incluído para alterar o comportamento padrão dos métodos ObjectMap e JavaMap put() e putAll() para se comportarem como os métodos ObjectMap.upsert() e upsertAll().

O método PutMode.UPSERT substitui o método setPutMode(PutMode.INSERTUPDATE). Use o método PutMode.UPSERT para indicar ao BackingMap e ao carregador que uma entrada na grade de dados precisa colocar a chave e o valor na grade. O BackingMap e carregador executam uma inserção ou uma atualização para colocar o valor na grade e no carregador. Se você executar a API upsert dentro de seus aplicativos, o carregador obterá um tipo

UPSERT de LogElement, que permite que carregadores façam a mesclagem do banco de dados ou chamadas upsert em vez de usar insert ou update.

Um tipo de operação pode ser obtido por combinações de outros tipos. Por exemplo, uma atualização pode ser obtida por uma remoção e, em seguida, por uma inserção. Considere essas combinações quando projetar suas políticas de autorização.

ObjectGridPermission

Uma com.ibm.websphere.objectgrid.security.ObjectGridPermission representa permissões para o ObjectGrid:

- Query: permissão para criar uma consulta de objeto ou consulta de entidade. A constante de número inteiro é definida como ObjectGridPermission.QUERY.
- Dynamic map: permissão para criar um mapa dinâmico baseado no modelo de mapa. A constante de número inteiro é definida como ObjectGridPermission.DYNAMIC_MAP.

Consulte a documentação da API do ObjectGridAuthorization para obter mais detalhes.

A tabela a seguir resume os métodos e ObjectGridPermission necessários:

Tabela 31. Lista de Métodos e a ObjectGridPermission Necessária

Ação da permissão	Métodos
`consulta`	com.ibm.websphere.objectgrid.Session.createObjectQuery(String)
`consulta`	com.ibm.websphere.objectgrid.em.EntityManager.createQuery(String)
`dynamicmap`	com.ibm.websphere.objectgrid.Session.getMap(String)

ServerMapPermission

Uma ServerMapPermission representa permissões para um ObjectMap hospedado em um servidor. O nome da permissão é o nome completo do nome do mapa do ObjectGrid. Executar as seguintes ações:

- **replicar**: permissão para replicar um mapa do servidor para o próximo cache
- **dynamicIndex**: permissão para um cliente criar ou remover um um índice dinâmico em um servidor

Consulte a documentação da API da ServerMapPermission para obter mais detalhes. Os métodos detalhados, que requerem ServerMapPermission diferente, estão relacionados na seguinte tabela:

Tabela 32. Permissões para um ObjectMap Hospedado por Servidor

Ação da permissão	Métodos
`replicate`	com.ibm.websphere.objectgrid.ClientReplicableMap.enableClientReplication(Mode, int[], ReplicationMapListener)
`dynamicIndex`	com.ibm.websphere.objectgrid.BackingMap.createDynamicIndex(String, Boolean, String, DynamicIndexCallback)
`dynamicIndex`	com.ibm.websphere.objectgrid.BackingMap.removeDynamicIndex(String)

AgentPermission

Uma AgentPermission representa as permissões para os agentes datagrid. O nome da permissão é o nome completo do mapa ObjectGrid, e a ação é uma cadeia limitada por vírgulas de nomes de classe de implementação do agente ou de nomes do pacote.

Consulte a documentação da API AgentPermission para obter informações adicionais.

Os métodos a seguir na classe com.ibm.websphere.objectgrid.datagrid.AgentManager exigem AgentPermission.

`com.ibm.websphere.objectgrid.datagrid.AgentManager#callMapAgent(MapGridAgent, Collection)`

`com.ibm.websphere.objectgrid.datagrid.AgentManager#callMapAgent(MapGridAgent)`

`com.ibm.websphere.objectgrid.datagrid.AgentManager#callReduceAgent(ReduceGridAgent, Collection)`

`com.ibm.websphere.objectgrid.datagrid.AgentManager#callReduceAgent(ReduceGridAgent, Collection)`

Mecanismos de Autorização

O WebSphere eXtreme Scale suporta dois tipos de mecanismos de autorização: Autorização JAAS (Java Authentication and Authorization Service) e autorização customizada. Esses mecanismos aplicam-se a todas as autorizações. A autorização JAAS muda as políticas de segurança Java com controles de acesso centrados no usuário. As permissões podem ser concedidas com base não apenas em qual código está a execução, mas também em quem a está executando. Autorização JAAS é parte do SDK Versão 5 e posterior.

Além disso, o WebSphere eXtreme Scale também suporta a autorização customizada com o seguinte plug-in:

- ObjectGridAuthorization: maneira customizada para autorizar o acesso a todos os artefatos.

É possível implementar seu próprio mecanismo de autorização, se não desejar utilizar a autorização JAAS. Usando um mecanismo de autorização customizado é possível usar o banco de dados de políticas, servidor de políticas ou Tivoli Access Manager para gerenciar as autorizações.

É possível configurar o mecanismo de autorização de duas maneiras:

- Configuração XML

  1. *Configuração XML:* É possível utilizar o arquivo XML do ObjectGrid para definir um ObjectGrid e configurar o mecanismo de autorização como AUTHORIZATION_MECHANISM_JAAS ou AUTHORIZATION_MECHANISM_CUSTOM. A seguir está o arquivo secure-objectgrid-definition.xml que é utilizado no ObjectGridSample do aplicativo corporativo:

  ```
  <objectGrids>
   <objectGrid name="secureClusterObjectGrid" securityEnabled="true"
    authorizationMechanism="AUTHORIZATION_MECHANISM_JAAS">
    <bean id="TransactionCallback"
  classname="com.ibm.websphere.samples.objectgrid.HeapTransactionCallback" />
  ...
  </objectGrids>
  ```

- Configuração Programática

  2. *Configuração Programática:* Se desejar criar um ObjectGrid utilizando o método ObjectGrid.setAuthorizationMechanism(int), é possível chamar o seguinte método para configurar o mecanismo de autorização. A chamada deste método aplica-se somente ao modelo de programação local do WebSphere eXtreme Scale quando você instancia diretamente a instância do ObjectGrid:

  ```
  /**
   * Set the authorization Mechanism. The default is
   * com.ibm.websphere.objectgrid.security.SecurityConstants.
   * AUTHORIZATION_MECHANISM_JAAS.
  ```

```
     * @param authMechanism the map authorization mechanism
    */
    void setAuthorizationMechanism(int authMechanism);
```

Autorização JAAS

Um objeto javax.security.auth.Subject representa um usuário autenticado. Um Subject consiste em um conjunto de principals e cada Principal representa uma identidade para esse usuário. Por exemplo, um Subject pode ter um nome principal, por exemplo, Joe Smith, e um grupo principal, por exemplo, gerente.

Utilizando a política de autorização JAAS, as permissões podem ser concedidas a Principals específicos. O WebSphere eXtreme Scale associa o Subject ao contexto de controle de acesso atual. Para cada chamada para o método ObjectMap ou Javamap, o tempo de execução do Java automaticamente determina se a política concede a permissão necessária somente a um Principal específico e se for, a operação será permitida somente se o Subject associado ao contexto do controle de acesso contiver o Principal designado.

É necessário estar familiarizado com a sintaxe de política do arquivo de políticas. Para obter uma descrição detalhada da autorização do JAAS, consulte o Guia de Referência do JAAS.

O WebSphere eXtreme Scale possui uma base de código especial que é usada para verificação da autorização JAAS para as chamadas de método ObjectMap e JavaMap. Esta base de código especial é `http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction`. Utilize esta base de código ao conceder as permissões ObjectMap ou JavaMap a proprietários. Este código especial foi criado porque o arquivo JAR (Java Archive) para eXtreme Scale é concedido com todas as permissões.

O modelo da política para conceder a permissão MapPermission é:

```
grant codeBase "http://www.ibm.com/com/ibm/ws/objectgrid/security/PrivilegedAction"
   <Principal field(s)>{
    permission com.ibm.websphere.objectgrid.security.MapPermission
               "[ObjectGrid_name].[ObjectMap_name]", "action";
    ....
    permission com.ibm.websphere.objectgrid.security.MapPermission
               "[ObjectGrid_name].[ObjectMap_name]", "action";
  };
```

Um campo de Principal é semelhante ao seguinte exemplo:

```
principal
Principal_class "principal_name"
```

Nesta política, somente as permissões de inserção e leitura são concedidas a esses quatro mapas para um determinado principal. O outro arquivo de políticas, `fullAccessAuth.policy`, concede todas as permissões para estes mapas a um principal. Antes de executar o aplicativo, altere o principal_name e a classe do proprietário para os valores apropriados. O valor de principal_name depende do registro do usuário. Por exemplo, se o S.O. local for usado como registro do usuário, o nome da máquina será MACH1, o ID do usuário será user1 e o principal_name será `MACH1/user1`.

A política de autorização JAAS pode ser colocada diretamente no arquivo de políticas Java, ou pode ser colocada em um arquivo de autorização JAAS separado e, em seguida, configurado usando

- Use o seguinte argumento JVM:
  `-Djava.security.policy=file:[JAAS_AUTH_POLICY_FILE]`
- Use a seguinte propriedade no arquivo java.security:
  `-Dauth.policy.url.x=file:[JAAS_AUTH_POLICY_FILE]`

Autorização de ObjectGrid Customizada

O plug-in ObjectGridAuthorization é usado para autorizar acessos ObjectGrid, ObjectMap e JavaMap para Principals representados por um objeto Subject de modo customizado. Uma implementação típica desse plug-in é recuperar os Principals do objeto Subject, e então verificar se as permissões especificadas estão concedidas ou não aos Principals.

Uma permissão passada para o método checkPermission(Subject, Permission) poderia ser uma das seguintes:

- MapPermission
- ObjectGridPermission
- AgentPermission
- ServerMapPermission

Consulte a documentação da API do ObjectGridAuthorization para obter mais detalhes.

O plug-in ObjectGridAuthorization pode ser configurado da seguinte forma:

- Configuração XML

  É possível usar o arquivo XML do ObjectGrid para definir um plug-in de ObjectAuthorization. Veja um exemplo a seguir:

```
<objectGrids>
 <objectGrid name="secureClusterObjectGrid" securityEnabled="true"
  authorizationMechanism="AUTHORIZATION_MECHANISM_CUSTOM">
...
  <bean id="ObjectGridAuthorization"
className="com.acme.ObjectGridAuthorizationImpl" />
</objectGrids>
```

- Configuração Programática

  Se você quiser criar um ObjectGrid usando o método de API ObjectGrid.setObjectGridAuthorization(ObjectGridAuthorization), pode chamar o seguinte método para configurar o plug-in de autorização. Este método aplica-se somente ao modelo de programação local do eXtreme Scale quando você instancia diretamente a instância do ObjectGrid.

```
/**
     * Sets the <code>ObjectGridAuthorization</code> for this ObjectGrid instance.
     * <p>
     * Passing <code>null</code> to this method removes a previously set
     * <code>ObjectGridAuthorization</code> object from an earlier invocation of this method
     * and indicates that this <code>ObjectGrid</code> is not associated with a
     * <code>ObjectGridAuthorization</code> object.
     * <p>
     * This method should only be used when ObjectGrid security is enabled. Se
     * the ObjectGrid security is disabled, the provided <code>ObjectGridAuthorization</code> object
     * will not be used.
     * <p>
     * A <code>ObjectGridAuthorization</code> plug-in can be used to authorize
     * access to the ObjectGrid and maps. Please refer to <code>ObjectGridAuthorization</code> for more details.
     *
     * <p>
     * As of XD 6.1, the <code>setMapAuthorization</code> is deprecated and
     * <code>setObjectGridAuthorization</code> is recommended for use. However,
     * if both <code>MapAuthorization</code> plug-in and <code>ObjectGridAuthorization</code> plug-in
     * are used, ObjectGrid will use the provided <code>MapAuthorization</code> to authorize map accesses,
     * even though it is deprecated.
     * <p>
     * Note, to avoid an <code>IllegalStateException</code>, this method must be
```

```
     * called prior to the <code>initialize()</code> method.  Also, keep in mind
     * that the <code>getSession</code> methods implicitly call the
     * <code>initialize()</code> method if it has yet to be called by the
     * application.
     *
     * @param ogAuthorization the <code>ObjectGridAuthorization</code> plug-in
     *
     * @throws IllegalStateException if this method is called after the
     *         <code>initialize()</code> method is called.
     *
     * @see #initialize()
     * @see ObjectGridAuthorization
     * @since WAS XD 6.1
     */
    void setObjectGridAuthorization(ObjectGridAuthorization ogAuthorization);
```

Implementação de ObjectGridAuthorization

O método Boolean checkPermission(Subject subject, Permission permission) da interface ObjectGridAuthorization é chamado pelo tempo de execução do WebSphere eXtreme Scale para verificar se o objeto subject transmitido possui a permissão de passagem. A implementação da interface ObjectGridAuthorization retorna true se o objeto possui a permissão e false se não possui.

Uma implementação típica deste plug-in é recuperar os proprietários do objeto Subject e verificar se as permissões especificadas serão concedidas aos proprietários consultando políticas específicas. Estas políticas são definidas por usuários. Por exemplo, as políticas podem ser definidas em um banco de dados, um arquivo simples ou em um servidor de políticas Tivoli Access Manager.

Por exemplo, podemos usar o servidor de políticas Tivoli Access Manager para gerenciar a política de autorização e usar sua API para autorizar o acesso. Para saber como usar as APIs do Tivoli Access Manager Authorization, consulte o IBM Tivoli Access Manager Authorization Java Classes Developer Reference para obter detalhes adicionais.

Esta implementação da amostra faz as seguintes suposições:

- Verifique as autorização apenas para MapPermission. Para outras permissões, retorne sempre `true`.
- O objeto Subject contém um proprietário com.tivoli.mts.PDPrincipal.
- O servidor de políticas do Tivoli Access Manager definiu as permissões a seguir para o objeto de nome ObjectMap ou JavaMap. O objeto definido no servidor de política deve ter o mesmo nome que o nome ObjectMap ou JavaMap no formato de [ObjectGrid_name].[ObjectMap_name]. A permissão é o primeiro caractere das cadeias de permissão definidas na permissão MapPermission. Por exemplo, a permissão "r" definida no servidor de política representa a permissão de leitura para o mapa ObjectMap.

O fragmento de código a seguir demonstra como implementar o método checkPermission:

```
/**
* @see com.ibm.websphere.objectgrid.security.plugins.
* MapAuthorization#checkPermission
* (javax.security.auth.Subject, com.ibm.websphere.objectgrid.security.
* MapPermission)
*/
public boolean checkPermission(final Subject subject,
 Permission p) {

  // For non-MapPermission, we always authorize.
  if (!(p instanceof MapPermission)){
    return true;
  }
```

```
  MapPermission permission = (MapPermission) p;

  String[] str = permission.getParsedNames();

  StringBuffer pdPermissionStr = new StringBuffer(5);
  for (int i=0; i<str.length; i++) {
    pdPermissionStr.append(str[i].substring(0,1));
  }

  PDPermission pdPerm = new PDPermission(permission.getName(),
  pdPermissionStr.toString());

  Set principals = subject.getPrincipals();

  Iterator iter= principals.iterator();
  while(iter.hasNext()) {
    try {
      PDPrincipal principal = (PDPrincipal) iter.next();
      if (principal.implies(pdPerm)) {
        return true;
      }
    }
    catch (ClassCastException cce) {
      // Handle exception
    }
  }
  return false;
}
```

Informações relacionadas:

"Módulo 4: Usar a Autorização do Java Authentication and Authorization Service (JAAS) no WebSphere Application Server" na página 64
Agora que você configurou a autenticação de clientes, é possível configurar ainda mais a autenticação para conceder aos usuários diferentes permissões. Por exemplo, um usuário operador pode apenas visualizar dados, enquanto que um usuário administrador pode executar todas as operações.

Autenticação da Grade de Dados

Java

É possível utilizar o plug-in do gerenciador de token seguro para ativar a autenticação servidor-para-servidor, que requer que você implemente a interface SecureTokenManager.

O método generateToken(Object) obtém uma proteção de objeto, e depois gera um token que não pode ser compreendido pelos outros. O método verifyTokens(byte[]) faz o processo inverso: converte o token de volta ao objeto original.

Uma implementação SecureTokenManager simples usa um algoritmo de codificação simples, como um algoritmo XOR, para codificar o objeto na forma serializada e depois usa o algoritmo de codificação correspondente para decodificar o token. Esta implementação não é segura e é fácil de ser interrompida.

Implementação padrão do **WebSphere eXtreme Scale**

O WebSphere eXtreme Scale fornece uma implementação imediatamente disponível para esta interface. Esta implementação padrão utiliza um par de chaves para assinar e verificar a assinatura e utiliza uma chave secreta para criptografar o conteúdo. Cada servidor tem um armazenamento de chaves de tipo JCKES para

armazenar o par de chaves, uma chave privada e uma chave pública e uma chave secreta. O armazenamento de chaves tem que ser do tipo JCKES para armazenar as chaves secretas. Estas chaves são utilizadas para criptografar e assinar ou verificar a cadeia de segredo na extremidade de envio. Além disso, o token está associado ao tempo de expiração. Na extremidade de recebimento, os dados são verificados, decriptografados e comparados com a cadeia de segredo do receptor. Os protocolos de comunicação Secure Sockets Layer (SSL) não são necessários entre um par de servidores para autenticação, porque as chaves privadas e as chaves públicas servem para a mesma finalidade. No entanto, se a comunicação do servidor não for criptografada, os dados poderão ser roubados por violação na comunicação. Como o token expira em breve, a ameaça de ataque à reprodução é minimizada. Esta possibilidade é significativamente reduzida se todos os servidores forem implementados atrás de um firewall.

A desvantagem desta abordagem é que os administradores do WebSphere eXtreme Scale precisam gerar chaves e transportá-las para todos os servidores, o que pode causar violação de segurança durante o transporte.

Tarefas relacionadas:

8.6+ "Ativando Autenticação LDAP nos Servidores de Catálogos e de Contêineres do eXtreme Scale" na página 780
Ative seus servidores WebSphere eXtreme Scale e servidores de catálogos para autenticação Lightweight Directory Access Protocol (LDAP) com um arquivo de políticas Java Authentication and Authorization Service (JAAS) utilizado para autorização.

"Autenticando e Autorizando Clientes" na página 771
É possível ativar a segurança e a autenticação de credencial para autenticar clientes. Além disso, é possível autorizar clientes administrativos para acessar a grade de dados.

"Autenticando Aplicativos Clientes" na página 772
A autenticação de cliente do aplicativo consiste em ativar a autenticação de credencial e de segurança cliente/servidor e de configurar um autenticador e um gerador de credencial de sistema.

"Autorizando Aplicativos Clientes" na página 774
A autorização do cliente do aplicativo consiste de classes de permissão do ObjectGrid, de mecanismos de autorização, de um período de verificação de permissão e de autorização de acesso apenas pelo criador.

8.6+ "Autorizando Clientes Administrativos" na página 778
Por meio da segurança administrativa, você pode autorizar os usuários a acessar a grade de dados. Algumas condições são necessárias, dependendo de seu ambiente de instalação do WebSphere eXtreme Scale e dos usuários que você deseja que tenham acesso.

Referências relacionadas:

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Classe ClientSecurityConfigurationFactory

Programação de Segurança Local

Java

WebSphere eXtreme Scale fornece vários terminais de segurança para permitir que você integre mecanismos customizados. No modelo de programação local, a principal função de segurança é a autorização e não possui suporte à autenticação.

É necessário autenticar fora do WebSphere Application Server. Entretanto, são fornecidos plug-ins para obter e validar objetos Subject.

Autenticação

No modelo de programação local, o eXtreme Scale não fornece nenhum mecanismo de autenticação, mas conta com o ambiente, servidores de aplicativos ou aplicativos, para autenticação. Quando o eXtreme Scale é usado no WebSphere Application Server ou WebSphere Extended Deployment, os aplicativos podem usar o mecanismo de autenticação de segurança do WebSphere Application Server. Quando o eXtreme Scale está sendo executado em um ambiente J2SE (Java 2 Platform, Standard Edition, o aplicativo tem que gerenciar as autenticações com autenticação JAAS (Java Authentication and Authorization Service) ou outros mecanismos de autenticação. Para obter informações adicionais sobre como utilizar a autenticação JAAS, consulte o Guia de Referência do JAAS. O contrato entre um aplicativo e uma instância do ObjectGrid é o objeto javax.security.auth.Subject. Quando o cliente é autenticado pelo servidor de aplicativos ou pelo aplicativo, o aplicativo pode recuperar o objeto javax.security.auth.Subject autenticado e utilizar este objeto Subject para obter uma sessão da instância do ObjectGrid, chamando o método ObjectGrid.getSession(Subject). Este objeto Subject é utilizado para autorizar o acesso aos dados do mapa. Este contrato é chamado de mecanismo de transmissão de subject. O exemplo a seguir ilustra a API ObjectGrid.getSession(Subject).

```
/**
 * This API allows the cache to use a specific subject rather than the one
 * configured on the ObjectGrid to get a session.
 * @param subject
 * @return An instance of Session
 * @throws ObjectGridException
 * @throws TransactionCallbackException
 * @throws InvalidSubjectException the subject passed in is not valid based
 * on the SubjectValidation mechanism.
 */
public Session getSession(Subject subject)
throws ObjectGridException, TransactionCallbackException, InvalidSubjectException;
```

O método ObjectGrid.getSession() na interface ObjectGrid também pode ser utilizando para obter um objeto Session:

```
/**
 * This method returns a Session object that can be used by a single thread at a time.
 * You cannot share this Session object between threads without placing a
 * critical section around it. While the core framework allows the object to move
 * between threads, the TransactionCallback and Loader might prevent this usage,
 * especially in J2EE environments. When security is enabled, this method uses the
 * SubjectSource to get a Subject object.
 *
 * If the initialize method has not been invoked prior to the first
 * getSession invocation, then an implicit initialization occurs.  This
 * initialization ensures that all of the configuration is complete before
 * any runtime usage is required.
 *
 * @see #initialize()
 * @return An instance of Session
 * @throws ObjectGridException
 * @throws TransactionCallbackException
 * @throws IllegalStateException if this method is called after the
 *         destroy() method is called.
 */
public Session getSession()
throws ObjectGridException, TransactionCallbackException;
```

Conforme especifica a documentação da API, quando a segurança é ativada, este método utiliza o plug-in SubjectSource para obter um objeto Subject. O plug-in SubjectSource é um dos plug-ins de segurança no eXtreme Scale para suportar a

propagação de objetos Subject. Consulte Plug-ins Relacionados à Segurança para obter informações adicionais. O método getSession(Subject) pode ser chamado na instância do ObjectGrid local apenas. Se você chamar o método getSession(Subject) em um lado do cliente em uma configuração distribuída do eXtreme Scale, o resultado será um IllegalStateException.

Plug-ins de Segurança

O WebSphere eXtreme Scale oferece dois plug-ins de segurança que estão relacionados ao mecanismo de transmissão de assunto: os plug-ins SubjectSource e SubjectValidation.

Plug-in SubjectSource

O plug-in SubjectSource, representado pela interface com.ibm.websphere.objectgrid.security.plugins.SubjectSource, é um plug-in usado para obter um objeto Subject de um ambiente de execução do eXtreme Scale. Este ambiente pode ser um aplicativo usando o ObjectGrid ou um servidor de aplicativos que hospeda o aplicativo. Considere o plug-in SubjectSource uma alternativa para o mecanismo de transmissão de subject. Utilizando o mecanismo de transmissão de subject, o aplicativo recupera o objeto Subject e utiliza-o para obter o objeto de sessão do ObjectGrid. Com o plug-in SubjectSource, o tempo de execução do eXtreme Scale recupera o objeto Subject e o utiliza para obter o objeto de sessão. O mecanismo de transmissão de subject fornece o controle de objetos Subject para aplicativos, enquanto o mecanismo do plug-in SubjectSource libera aplicativos de recuperar o objeto Subject. É possível utilizar o plug-in SubjectSource para obter um objeto Subject que representa um cliente do eXtreme Scale que é utilizado para autorização. Quando o método ObjectGrid.getSession é chamado, o Subject getSubject emite uma ObjectGridSecurityException se a segurança estiver ativada. O WebSphere eXtreme Scale oferece uma implementação padrão deste plug-in: com.ibm.websphere.objectgrid.security.plugins.builtins.WSSubjectSourceImpl. Esta implementação pode ser usada para recuperar um assunto do responsável pela chamada ou um assunto RunAs do encadeamento quando um aplicativo está em execução no WebSphere Application Server. É possível configurar esta classe no arquivo XML descritor do ObjectGrid como a classe de implementação SubjectSource ao usar o eXtreme Scale no WebSphere Application Server. O trecho de código a seguir mostra o fluxo principal do método WSSubjectSourceImpl.getSubject.

```
Subject s = null;
try {
  if (finalType == RUN_AS_SUBJECT) {
    // obter o subject RunAs
    s = com.ibm.websphere.security.auth.WSSubject.getRunAsSubject();
  }
  else if (finalType == CALLER_SUBJECT) {
    // obter o callersubject
    s = com.ibm.websphere.security.auth.WSSubject.getCallerSubject();
  }
}
catch (WSSecurityException wse) {
  throw new ObjectGridSecurityException(wse);
}

return s;
```

Para obter outros detalhes, consulte a documentação da API para o plug-in SubjectSource e a implementação do WSSubjectSourceImpl.

Plug-in SubjectValidation

O plug-in SubjectValidation, que é representado pela interface com.ibm.websphere.objectgrid.security.plugins.SubjectValidation, é outro plug-in de segurança. O plug-in SubjectValidation pode ser utilizado para validar que um javax.security.auth.Subject, quer transmitido para o ObjectGrid quer recuperado pelo plug-in SubjectSource, é um Subject válido desde que não violado.

O método SubjectValidation.validateSubject(Subject) na interface SubjectValidation obtém um objeto Subject e retorna um objeto Subject. Tudo está definido nas suas implementações: se o objeto Subject é ou não válido e qual objeto Subject será retornado. Se o objeto Subject não for válido, o resultado será um InvalidSubjectException.

É possível utilizar esse plug-in se não confiar no objeto Subject transmitido para esse método. Isso dificilmente ocorrerá, desde que você confie nos desenvolvedores que redigiram o código do aplicativo para recuperar o objeto Subject.

Uma implementação deste plug-in precisa de suporte do criador do objeto Subject, porque apenas o criador sabe se o objeto Subject foi violado. No entanto, alguns criadores de subjects podem não saber se o Subject foi violado. Neste caso, este plug-in não é útil.

O WebSphere eXtreme Scale oferece uma implementação padrão de SubjectValidation: com.ibm.websphere.objectgrid.security.plugins.builtins.WSSubjectValidationImpl. É possível usar esta implementação para validar o assunto autenticado pelo WebSphere Application Server. Você pode configurar esta classe com a classe de implementação SubjectValidation ao usar o eXtreme Scale no WebSphere Application Server. A implementação do WSSubjectValidationImpl levará em consideração um objeto Subject válido apenas se o token da credencial associado a tal Subject não estiver violado. Você pode alterar outras partes do objeto Subject. A implementação WSSubjectValidationImpl solicita ao WebSphere Application Server o Subject original correspondendo ao token de credencial e retorna o Subject original como o objeto Subject validado. Portanto, as alterações feitas no conteúdo do Subject diferentes do token de credencial não têm nenhum efeito. O trecho de código a seguir mostra o fluxo básico do WSSubjectValidationImpl.validateSubject(Subject).

```
// Create a LoginContext with scheme WSLogin and
// pass a Callback handler.
LoginContext lc = new LoginContext("WSLogin",
new WSCredTokenCallbackHandlerImpl(subject));

// When this method is called, the callback handler methods
// will be called to log the user in.
lc.login();

// Get the subject from the LoginContext
return lc.getSubject();
```

O trecho de código anterior cria um objeto de manipulador de retorno de chamada do token de credencial, WSCredTokenCallbackHandlerImpl, com o objeto Subject a ser validado. Em seguida, um objeto LoginContext é criado com o esquema de login WSLogin. Quando o método lc.login é chamado, a segurança WebSphere Application Server recupera o token de credencial do objeto Subject e, em seguida, retorna o Subject correspondente como o objeto Subject validado.

Para obter outros detalhes, consulte as APIs Java da implementação SubjectValidation e WSSubjectValidationImpl.

Configuração do Plug-in

Você pode configurar os plug-ins SubjectValidation e SubjectSource de dois modos:

- **Configuração XML**É possível utilizar o arquivo XML do ObjectGrid para definir um ObjectGrid e configurar estes dois plug-ins. A seguir está um exemplo, no qual a classe WSSubjectSourceImpl está configurada como o plug-in SubjectSource e a classe WSSubjectValidation está configurada como o plug-in SubjectValidation.

```
<objectGrids>
 <objectGrid name="secureClusterObjectGrid" securityEnabled="true"
  authorizationMechanism="AUTHORIZATION_MECHANISM_JAAS">
        <bean id="SubjectSource"
className="com.ibm.websphere.objectgrid.security.plugins.builtins.
 WSSubjectSourceImpl" />
    <bean id="SubjectValidation"
 className="com.ibm.websphere.objectgrid.security.plugins.builtins.
 WSSubjectValidationImpl" />
    <bean id="TransactionCallback"
className="com.ibm.websphere.samples.objectgrid.
 HeapTransactionCallback" />
...
</objectGrids>
```

- **Programação** Se você desejar criar um ObjectGrid através de APIs, é possível chamar os seguintes métodos para configurar os plug-ins SubjectSource ou SubjectValidation.

```
**
* Set the SubjectValidation plug-in for this ObjectGrid instance. A
* SubjectValidation plug-in can be used to validate the Subject object
* passed in as a valid Subject. Refer to {@link SubjectValidation}
* for more details.
* @param subjectValidation the SubjectValidation plug-in
*/
void setSubjectValidation(SubjectValidation subjectValidation);


/**
* Set the SubjectSource plug-in. A SubjectSource plug-in can be used
* to get a Subject object from the environment to represent the
* ObjectGrid client.
*
* @param source the SubjectSource plug-in
*/
void setSubjectSource(SubjectSource source);
```

Gravar Seu Código de Autenticação JAAS

Você pode escrever seu próprio código de autenticação JAAS (Java Authentication and Authorization Service) para manipular a autenticação. É necessário gravar seus próprios módulos de login e, em seguida, configurá-los para seu módulo de autenticação.

O módulo de login recebe informações sobre um usuário e autentica o usuário. Estas informações podem ser tudo o que pode identificar o usuário. Por exemplo, as informações podem ser um ID de usuário e senha, certificado do cliente, e assim por diante. Depois de receber tais informações, o módulo de login verifica se elas representam um Subject válido e cria o objeto Subject. No momento, várias implementações de módulos de login estão disponíveis para o público.

Depois que um módulo de login for gravado, configure-o para o tempo de execução a ser utilizado. Configure um módulo de login do JAAS. Este módulo de login contém o módulo de login e seu esquema de autenticação. Por exemplo:

```
FileLogin
{
    com.acme.auth.FileLoginModule required
};
```

O esquema de autenticação é FileLogin e o módulo de login é com.acme.auth.FileLoginModule. O token requerido indica que o módulo FileLoginModule deve validar tal login ou todo o esquema falhará.

A configuração do arquivo de configuração do módulo de login JAAS pode ser feita de um dos seguintes modos:

- Configure o arquivo de configuração do módulo de login do JAAS na propriedade login.config.url no arquivo java.security, por exemplo:
  ```
  login.config.url.1=file:${java.home}/lib/security/file.login
  ```
- Configure o arquivo de configuração de módulo de login JAAS a partir da linha de comandos usando os argumentos JVM (Java Virtual Machine) **-Djava.security.auth.login.config** como, por exemplo,
  ```
  -Djava.security.auth.login.config ==$JAVA_HOME/lib/security/file.login
  ```

Para obter mais informações, consulte o “Tutorial de Segurança do Java SE - Etapa 2” na página 22.Para obter mais informações, consulte o “Tutorial de Segurança do Java SE - Etapa 2” na página 22.

Se o seu código estiver em execução no WebSphere Application Server, configure o login do JAAS no console administrativo e armazene esta configuração de login na configuração do servidor de aplicativos. Consulte a configuração de login para Java Authentication and Authorization Service para obter detalhes.

Autenticação de Cliente .NET de Programação

.NET

Para enviar credenciais do cliente .NET para o lado do servidor, você deve implementar as interfaces ICredentialGenerator e ICredential. Essas interfaces geram um objeto de credencial que é transmitido para a grade de dados e interpretados no lado do servidor. No lado do servidor, o plug-in correspondente interpreta o objeto de credencial.

Sobre Esta Tarefa

Para concluir a autenticação, o aplicativo .NET deve implementar as seguintes interfaces:

- ICredential: Um Credential representa uma credencial de cliente, tal como um par de ID do usuário e senha.
- ICredentialGenerator: Um CredentialGenerator representa uma factory de credencial para gerar a credencial.

Quando um aplicativo cliente .NET se conecta a um servidor que requer autenticação, o cliente precisa fornecer uma credencial de cliente. Uma credencial de cliente é representada pela interface ICredential. Uma credencial de cliente pode ser um par de nome de usuário e senha, um registro do Kerberos, um certificado cliente ou dados em qualquer formato concordado entre o cliente e o servidor. Esta interface explicitamente define os métodos equals(Object) e hashCode. Estes

métodos são importantes porque os objetos Subject autenticados são armazenados em cache utilizando o objeto Credential como a chave no lado do servidor. Também é possível gerar uma credencial com a interface ICredentialGenerator. Esta interface é útil quando a credencial pode expirar. Uma nova credencial é gerada sempre que a propriedade Credential for obtida.

Também é possível usar o plug-in CredentialGenerator fornecido para criar uma credencial baseada na configuração **Client.Net.Properties credentialGeneratorProps=** no arquivo `Client.Net.Properties`. As configurações adicionais que definem plug-in de credencial são **credentialGeneratorAssembly** e **credentialGeneratorClass**.

Procedimento

Implemente as interfaces ICredentialGenerator e ICredential no aplicativo cliente .NET. É possível utilizar os seguintes exemplos para desenvolver seu aplicativo:

- "Exemplo: Implementando uma Credencial de Senha de Usuário para Aplicativos .NET" na página 704
- "Exemplo: Implementando um Gerador de Credencial do Usuário para Aplicativos .NET" na página 706

Referências relacionadas:

"Exemplo: Implementando uma Credencial de Senha de Usuário para Aplicativos .NET" na página 704
É possível usar este exemplo para gravar sua própria implementação da interface ICredential. A credencial de senha do usuário armazena um ID de usuário e uma senha.

"Exemplo: Implementando um Gerador de Credencial do Usuário para Aplicativos .NET" na página 706
É possível usar este exemplo para gravar sua própria implementação da interface ICredentialGenerator. A interface utiliza um ID do usuário e uma senha. O objeto UserPasswordCredential contém o ID do usuário e a senha, que são obtidos da propriedade Credential somente leitura.

Arquivo de Propriedades do Cliente
Crie um arquivo de propriedades com base nos requisitos para os processos do cliente do WebSphere eXtreme Scale.

Informações relacionadas:

Interface ICredential

Interface ICredentialGenerator

Exemplo: Implementando uma Credencial de Senha de Usuário para Aplicativos .NET

.NET

É possível usar este exemplo para gravar sua própria implementação da interface ICredential. A credencial de senha do usuário armazena um ID de usuário e uma senha.

UserPasswordCredential.cs

```
// Module  :  UserPasswordCrediential.cs

using System;
using IBM.WebSphere.Caching.Security;

namespace com.ibm.websphere.objectgrid.security.plugins.builtins
{
```

```
public class UserPasswordCredential : ICredential
{
    private String ivUserName;

    private String ivPassword;

    /// <summary>
    ///Creates a UserPasswordCredential with the specified user name and
    /// password.
    ///
    /// ArgumentException if userName or password is null
    /// </summary>
    /// <param name="userName">the user name for this credential</param>
    /// <param name="password">the password for this credential</param>
    public UserPasswordCredential(String userName, String password) {
        if (userName == null || password == null) {
            throw new ArgumentException("User name and password cannot be null.");
        }
        this.ivUserName = userName;
        this.ivPassword = password;
    }

    /// <summary>Gets the user name for this credential.</summary>
    /// <returns>the user name argument that was passed to the constructor
    ///or the setUserName(String) method of this class </returns>
    public String GetUserName() {
        return ivUserName;
    }

    /// <summary>Sets the user name for this credential.
    ///ArgumentException if userName is null
    /// </summary>
    /// <param name="userName">userName the user name to set.</param>
    public void SetUserName(String userName) {
        if (userName == null) {
            throw new ArgumentException("User name cannot be null.");
        }
        this.ivUserName = userName;
    }

    /// <summary>Gets the password for this credential.
    /// </summary>
    /// <returns>the password argument that was passed to the constructor or the setPassword(String) method of this class</returns>
    public String GetPassword() {
        return ivPassword;
    }

    /// <summary>Sets the password for this credential.
    ///ArgumentException if password is null
    /// </summary>
    /// <param name="password">the password to set.</param>
    public void SetPassword(String password) {
        if (password == null) {
            throw new ArgumentException("Password cannot be null.");
        }
        this.ivPassword = password;
    }

    /// <summary>Checks two UserPasswordCredential objects for equality.
    ///<p>
    /// Two UserPasswordCredential objects are equal if and only if their user names
    /// and passwords are equal.
    /// </summary>
    /// <param name="o">the object we are testing for equality with this object.</param>
    /// <returns>true if both UserPasswordCredential objects are equivalent.</returns>
    public bool Equals(ICredential credential)
    {
        if (this == credential) {
            return true;
        }
        if (credential is UserPasswordCredential) {
            UserPasswordCredential other = (UserPasswordCredential)credential;
            return other.ivPassword.Equals(ivPassword) && other.ivUserName.Equals(ivUserName);
        }
        return false;
    }

    /// <summary>Returns the hashcode of the UserPasswordCredential object.
    /// </summary>
```

```
        /// <returns>return the hash code of this object</returns>
        public override int GetHashCode() {
            int ret = ivUserName.GetHashCode() + ivPassword.GetHashCode();
            return ret;
        }

        /// <summary>this.Object as a string
        /// </summary>
        /// <returns>return the string presentation of the UserPasswordCredential object.</returns>
        public override String ToString() {
            return typeof(UserPasswordCredential).FullName + "[" + ivUserName + ",xxxxxx]";
        }

    }
}
```

Tarefas relacionadas:

"Autenticação de Cliente .NET de Programação" na página 703
Para enviar credenciais do cliente .NET para o lado do servidor, você deve implementar as interfaces ICredentialGenerator e ICredential. Essas interfaces geram um objeto de credencial que é transmitido para a grade de dados e interpretados no lado do servidor. No lado do servidor, o plug-in correspondente interpreta o objeto de credencial.

Informações relacionadas:

Interface ICredential

Interface ICredentialGenerator

Exemplo: Implementando um Gerador de Credencial do Usuário para Aplicativos .NET

É possível usar este exemplo para gravar sua própria implementação da interface ICredentialGenerator. A interface utiliza um ID do usuário e uma senha. O objeto UserPasswordCredential contém o ID do usuário e a senha, que são obtidos da propriedade Credential somente leitura.

UserPasswordCredentialGenerator.cs

```
// Module  :  UserPasswordCredientialGenerator.cs
//
// Source File Description: Reference Documentation
//
using System;
using System.Security.Authentication;
using IBM.WebSphere.Caching.Security;
using com.ibm.websphere.objectgrid.security.plugins.builtins;

namespace IBM.WebSphere.Caching.Security
{
    public class UserPasswordCredentialGenerator : ICredentialGenerator
    {

        private String ivUser;

        private String ivPwd;

        public ICredential Credential { get { return _getCredential(); } }

        public string Properties { set {_setProperties(value);} }

        public UserPasswordCredentialGenerator() {
            ivUser = null;
            ivPwd = null;
        }


        public UserPasswordCredentialGenerator(String user=null, String pwd=null)
        {
            ivUser = user;
            ivPwd = pwd;
        }

        /// <summary>Creates a new UserPasswordCredential object using this object's user name and password.
```

```
/// </summary>
/// <returns>new UserPasswordCredential instance</returns>
private ICredential _getCredential()
{
    try
    {
        ICredential MyCredential = new UserPasswordCredential(ivUser, ivPwd) as ICredential;
        return (ICredential) MyCredential;
    }
    catch (Exception e)
    {
        AuthenticationException CannotGenerateCredentialException = new AuthenticationException(e.ToString());
        throw CannotGenerateCredentialException;
    }
}

/// <summary>Gets the password for this credential generator.
/// </summary>
/// <returns>the password argument that was passed to the constructor</returns>
public String getPassword() {
    return ivPwd;
}

/// <summary>Gets the user name for this credential.
/// </summary>
/// <returns>the user argument that was passed to the constructor of this class</returns>
public String getUserName()
{
    return ivUser;
}

/// <summary>Sets additional properties namely a user name and password.
///Throws ArgumentException if the format is not valid
/// </summary>
/// <param name="properties">properties a properties string  with a user name and a password separated by a blank.</param>
private void _setProperties(string properties)
{
    String token = properties;
    char[] Seperator = { ' ' };
    String[] StringProperty = properties.Split(Seperator);
    if (StringProperty.Length != 2)
    {
        throw new ArgumentException(
            "The properties should have a user name and password and separated by a space.");
    }

    ivUser = StringProperty[0];
    ivPwd = StringProperty[1];
}

/// <summary>Checks two UserPasswordCredentialGenerator objects for equality.
///<p>
///Two UserPasswordCredentialGenerator objects are equal if and only if
///their user names and passwords are equal.
/// </summary>
/// <param name="obj">the object we are testing for equality with this object.</param>
/// <returns><code>true</code> if both UserPasswordCredentialGenerator objects are equivalent</returns>
public override bool Equals(Object obj)
{
    if (obj == this) {
        return true;
    }

    if (obj != null && obj is UserPasswordCredentialGenerator)
    {
        UserPasswordCredentialGenerator other = (UserPasswordCredentialGenerator) obj;

        Boolean bothUserNull = false;
        Boolean bothPwdNull = false;

        if (ivUser == null) {
            if (other.ivUser == null) {
                bothUserNull = true;
            }
            else
            {
                return false;
            }
        }
```

```
                if (ivPwd == null) {
                    if (other.ivPwd == null) {
                        bothPwdNull = true;
                    }
                    else
                    {
                        return false;
                    }
                }
                return (bothUserNull || ivUser.Equals(other.ivUser)) && (bothPwdNull || ivPwd.Equals(other.ivPwd));
            }
            return false;
        }

        /// <summary>Returns the hashcode of the UserPasswordCredentialGenerator object.
        /// </summary>
        /// <returns>the hash code of this object</returns>
        public override int GetHashCode()
        {
           return ivUser.GetHashCode() + ivPwd.GetHashCode();
        }

    }

}
```

Tarefas relacionadas:

"Autenticação de Cliente .NET de Programação" na página 703
Para enviar credenciais do cliente .NET para o lado do servidor, você deve implementar as interfaces ICredentialGenerator e ICredential. Essas interfaces geram um objeto de credencial que é transmitido para a grade de dados e interpretados no lado do servidor. No lado do servidor, o plug-in correspondente interpreta o objeto de credencial.

Informações relacionadas:

Interface ICredential

Interface ICredentialGenerator

Capítulo 8. Resolução de Problemas

Além dos logs e do rastreio, de mensagens e notas sobre a liberação discutidos nesta seção, é possível usar as ferramentas de monitoramento para descobrir problemas, como o local de dados no ambiente, a disponibilidade de servidores na grade de dados, e assim por diante. Se você estiver executando um ambiente do WebSphere Application Server, poderá usar a Performance Monitoring Infrastructure (PMI). Se você estiver executando em um ambiente independente, poderá usar uma ferramenta de monitoramento do fornecedor, como CA Wily Introscope ou Hyperic HQ. Também é possível usar e customizar o utilitário **xscmd** para exibir informações de texto sobre o ambiente.

Resolução de Problemas e Suporte para WebSphere eXtreme Scale

Para isolar e resolver problemas com seus produtos IBM, é possível usar a resolução de problemas e as informações de suporte. Essas informações contêm instruções para usar os recursos de determinação de problema que são fornecidos com seus produtos IBM, incluindo o WebSphere eXtreme Scale .

Técnicas para Resolução de Problemas

Resolução de Problemas é uma abordagem sistemática para solucionar um problema. O objetivo da resolução de problemas é determinar por que algo não funciona conforme se espera e como resolver o problema. Determinadas técnicas comuns podem ajudar com a tarefa de resolução de problemas.

A primeira etapa no processo de resolução de problemas é descrever o problema completamente. As descrições de problemas podem ajudar você e o representante de suporte técnico IBM a saber onde começar a localizar a causa do problema. Essa etapa inclui fazer perguntas básicas a si mesmo:

- Quais são os sintomas do problema?
- Onde o problema ocorre?
- Quando o problema ocorre?
- Em quais condições o problema ocorre?
- O problema pode ser reproduzido?

As respostas a essas perguntas geralmente levam a uma boa descrição do problema, o que pode levar você a uma resolução do problema.

Quais São os Sintomas do Problema?

Ao começar a descrever um problema, a pergunta mais óbvia é “Qual é o problema?” Essa pergunta pode ser direta; entretanto, é possível quebrá-la em várias perguntas mais focadas que criam uma figura mais descritiva do problema. Essas perguntas podem incluir:

- Quem, ou o que, está relatando o problema?
- Qual são os códigos e mensagens de erro?
- Como o sistema falha? Por exemplo, é um loop, interrupção, travamento, degradação de desempenho ou resultado incorreto?

Onde o problema ocorre?

Determinar de onde o problema se origina nem sempre é fácil, mas é uma das etapas mais importantes na resolução de um problema. Muitas camadas de tecnologia podem existir entre o relatório e os componentes com falha. As redes, a grade de dados e os servidores são apenas alguns dos componentes a serem considerados quando você está investigando problemas.

As perguntas a seguir ajudam você a focar onde o problema ocorre para isolar a camada do problema:

- O problema é específico para uma plataforma ou sistema operacional, ou é comum em diversas plataformas ou sistemas operacionais?
- O ambiente e a configuração atuais são suportados?
- Todos os usuários têm o problema?
- (Para instalações em diversos sites.) Todos os sites têm o problema?

Se uma camada relata o problema, o problema não se origina necessariamente nessa camada. Parte da identificação de onde um problema se origina é entender o ambiente no qual ele existe. Use algum tempo para descrever completamente o ambiente do problema, incluindo o sistema operacional e versão, todo software e versões correspondentes e informações de hardware. Confirme se você está executando em um ambiente que seja uma configuração suportada; muitos problemas podem ser rastreados retroativamente para níveis incompatíveis de software que não deveriam ser executados juntos ou não foram totalmente testados juntos.

Quando o problema ocorre?

Desenvolva uma linha de tempo detalhada dos eventos que precedem uma falha, especialmente para os casos que são ocorrências únicas. É possível desenvolver uma linha de tempo mais facilmente trabalhando retroativamente: Inicie no horário em que um erro foi relatado (do modo mais exato possível, até o milissegundo) e trabalhe retroativamente nos logs e informações disponíveis. Normalmente, é necessário examinar apenas até o primeiro evento suspeito localizado em um log de diagnóstico.

Para desenvolver uma linha de tempo detalhada de eventos, responda a estas perguntas:

- O problema acontece apenas em um determinado horário do dia ou noite?
- Com que frequência o problema acontece?
- Qual sequência de eventos precede o horário em que o problema é relatado?
- O problema acontece após uma mudança de ambiente, como upgrade ou instalação de software ou hardware?

Responder a esses tipos de perguntas pode fornecer a você um quadro de referência para investigar o problema.

Em quais condições o problema ocorre?

Conhecer quais sistemas e aplicativos estavam em execução no momento em que um problema ocorreu é uma parte importante da resolução de problemas. Estas perguntas sobre seu ambiente pode ajudá-lo a identificar a causa raiz do problema:

- O problema sempre ocorre quando a mesma tarefa está sendo executada?

- Uma determinada sequência de eventos precisa acontecer para que o problema ocorra?
- Quaisquer outros aplicativos falham ao mesmo tempo?

Responder a esses tipos de perguntas pode ajudar você a aplicar o ambiente no qual o problema ocorre e correlacionar quaisquer dependências. Lembre-se que só porque diversos problemas podem ter ocorrido aproximadamente ao mesmo tempo, eles não estão necessariamente relacionados.

O Problema Pode Ser Reproduzido?

De um ponto de vista de resolução de problemas, o problema ideal é aquele que pode ser reproduzido. Normalmente, quando um problema pode ser reproduzido, você tem um conjunto maior de ferramentas ou procedimentos à sua disposição para ajudar na investigação. Consequentemente, os problemas que podem ser reproduzidos são geralmente mais fáceis de depurar e resolver.

Entretanto, os problemas que podem ser reproduzidos podem ter uma desvantagem: Se o problema for de impacto comercial significativo, você não desejará sua recorrência. Se possível, recrie o problema em um ambiente de teste ou desenvolvimento, que normalmente oferece mais flexibilidade e controle durante a investigação.

- O problema pode ser recriado em um sistema de teste?
- Diversos usuários ou aplicativos estão encontrando o mesmo tipo de problema?
- O problema pode ser recriado executando um único comando, um conjunto de comandos ou um aplicativo específico?

Procurando Bases de Conhecimento

Muitas vezes, é possível localizar soluções para problemas procurando as bases de conhecimento IBM. É possível otimizar seus resultados usando recursos disponíveis, ferramentas de suporte e métodos de procura.

Sobre Esta Tarefa

É possível localizar informações úteis procurando o centro de informações do WebSphere eXtreme Scale . Entretanto, às vezes é necessário ir mais além do centro de informações para responder às perguntas e resolver problemas.

Procedimento

Para procurar bases de conhecimento para obter as informações necessárias, use uma ou mais das abordagens a seguir:

- Procure o conteúdo usando o IBM Support Assistant (ISA).

  ISA é um ambiente de trabalho de capacidade de manutenção de software gratuito que ajuda você a responder às perguntas e resolver problemas com produtos de software IBM. É possível localizar instruções para fazer download e instalar o ISA no website do ISA.
- Localize o conteúdo necessário usando o IBM Support Portal.

  O IBM Support Portal é uma visualização centralizada e unificada de todas as ferramentas e informações de suporte técnico para todos os sistemas, software e serviços IBM. O IBM Support Portal permite acessar o portfólio de suporte eletrônico IBM a partir de um único local. É possível customizar as páginas para focar as informações e os recursos que são necessários para a prevenção de

problemas a resolução de problemas mais rápida. Familiarize-se com o IBM Support Portal visualizando os vídeos demo (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) sobre essa ferramenta. Esses vídeos apresentam o IBM Support Portal, exploram a resolução de problemas e outros recursos e demonstram como é possível customizar a página movendo, incluindo e excluindo portlets.

- Procure conteúdo sobre o WebSphere eXtreme Scale usando um dos recursos técnicos adicionais a seguir:
  - WebSphere eXtreme Scale notas sobre o release
  - WebSphere eXtreme ScaleWeb site de suporte
  - Fórum do WebSphere eXtreme Scale
- Procure conteúdo usando a procura de cabeçalho principal da IBM. É possível usar a procura de cabeçalho principal da IBM digitando sua sequência de procura no campo de Procura na parte superior de qualquer página ibm.com.
- Procure conteúdo usando qualquer mecanismo de procura externo, como Google, Yahoo ou Bing. Se você usar um mecanismo de procura externo, seus resultados provavelmente incluirão informações que estão fora do domínio ibm.com. Entretanto, às vezes é possível localizar informações úteis de resolução de problemas sobre produtos IBM em grupos de notícias, fóruns e blogs que não estão em ibm.com.

  Dica: Inclua "IBM" e o nome do produto em sua procura se você estiver procurando informações sobre um produto IBM.

Obtendo Correções

Uma correção de produtos pode estar disponível para resolver seu problema.

Procedimento

Para localizar e instalar correções:

1. Obtenha as ferramentas necessárias para obter a correção. Use o IBM Update Installer para instalar e aplicar vários tipos de pacotes de manutenção para o WebSphere eXtreme Scale ou WebSphere eXtreme Scale Client. Como o Update Installer executa manutenção regular, é necessário usar a versão mais atual da ferramenta.
2. Determine de qual correção você precisa. Consulte as Correções Recomendadas para o WebSphere eXtreme Scale para selecionar a correção mais recente. Quando você seleciona uma correção, o documento de download para essa correção é aberto.
3. Faça download da correção. No documento de download, clique no link da correção mais recente na seção "Fazer Download do Pacote".
4. Aplique a correção. Siga as instruções na seção "Instruções de Instalação" do documento de download.
5. Subscreva-se para receber notificações por email semanais sobre correções e outras informações do Suporte IBM.

Obtendo Correções do Fix Central

É possível usar o Fix Central para localizar as correções que são recomendadas pelo Suporte IBM para uma variedade de produtos, incluindo o WebSphere eXtreme Scale . Com o Fix Central, é possível procurar, selecionar, pedir e fazer download de correções para seu sistema com uma escolha de opções de entrega. Uma correção do produto WebSphere eXtreme Scale pode estar disponível para resolver seu problema.

Procedimento

Para localizar e instalar correções:

1. Obtenha as ferramentas necessárias para obter a correção. Se não estiver instalado, obtenha seu instalador de atualização do produto. É possível fazer download do instalador a partir do Fix Central. Esse site fornece instruções de download, instalação e configuração para o instalador de atualização.
2. Selecione o produto e marque uma ou mais caixas de seleção que sejam relevantes para o problema que você deseja resolver.
3. Identifique e selecione a correção necessária.
4. Faça download da correção.
   a. Abra o documento de download e siga o link na seção "Fazer Download do Pacote".
   b. Ao fazer download do arquivo, assegure-se de que o nome do arquivo de manutenção não seja alterado. Essa mudança pode ser intencional, ou pode ser uma mudança inadvertente causada por determinados navegadores da web ou utilitários de download.
5. Aplique a correção.
   a. Siga as instruções na seção "Instruções de Instalação" do documento de download.
   b. Para obter informações adicionais, consulte o tópico "Instalando Correções com o Update Installer" na documentação do produto.
6. Opcional: Subscreva-se para receber notificações por email semanais sobre correções e outras atualizações do Suporte IBM.

Entrando em Contato com o Suporte IBM

O Suporte IBM fornece assistência a defeitos do produto, responde às FAQs e ajuda os usuários a resolverem problemas com o produto.

Antes de Iniciar

Depois de tentar localizar sua resposta ou solução usando outras opções de autoajuda, como notas sobre a liberação, é possível entrar em contato com o Suporte IBM. Antes de entrar em contato com o Suporte IBM, sua empresa ou organização deve ter um contrato de manutenção da IBM ativo e você deve estar autorizado a enviar problemas para a IBM. Para obter informações sobre os tipos de suporte disponível, consulte o tópico Support portfolio no "*Software Support Handbook*".

Procedimento

Para entrar em contato com o Suporte IBM sobre um problema:

1. Defina o problema, reúna informações de segundo plano e determine a gravidade do problema. Para obter informações adicionais, consulte o tópico Getting IBM support no *Software Support Handbook*.
2. Reúna informações de diagnóstico.
3. Submeta o problema para o Suporte IBM de uma das maneiras a seguir:
   - Com o IBM Support Assistant (ISA). Para obter informações adicionais, consulte "IBM Support Assistant for WebSphere eXtreme Scale" na página 897 ou "Coletando Dados com o IBM Support Assistant Data Collector" na página 896.

- Online por meio do IBM Support Portal: É possível abrir, atualizar e visualizar todas as solicitações de serviço a partir do portlet Service Request na página Solicitação de Serviço.
- Por telefone: Para obter o número do telefone para chamada em sua região, consulte a página da web Directory of worldwide contacts.

Resultados

Se o problema que você deseja submeter for relativo a um defeito de software ou documentação ausente ou inexata, o Suporte IBM criará um Authorized Program Analysis Report (APAR). O APAR descreve o problema em detalhe. Sempre que possível, o Suporte IBM fornece uma solução alternativa que pode ser implementada até que o APAR ser resolvido e uma correção seja entregue. A IBM publica APARs resolvidos no website do Suporte IBM diariamente, para que outros usuários que encontrarem o mesmo problema possam se beneficiar da mesma resolução.

Trocando Informações com a IBM

Para diagnosticar ou identificar um problema, talvez seja necessário fornecer ao Suporte IBM dados e informações de seu sistema. Em outros casos, o Suporte IBM pode fornecer ferramentas ou utilitários para serem usados para determinação de problema.

Enviando Informações para o Suporte IBM

Para reduzir o tempo que é necessário para resolver seu problema, é possível enviar informações de rastreio e diagnóstico para o Suporte IBM.

Procedimento

Para submeter informações de diagnóstico para o Suporte IBM:

1. Abra um Problem Management Record (PMR).
2. Colete os dados diagnósticos necessários. Os dados diagnósticos ajudam a reduzir o tempo que leva para resolver seu PMR. É possível coletar os dados diagnósticos manualmente ou automaticamente:
   - Colete os dados manualmente.
   - Colete os dados automaticamente.
3. Compacte os arquivos usando o formato de arquivo `.zip` ou `.tar`.
4. Transfira os arquivos para a IBM. É possível usar um dos métodos a seguir para transferir os arquivos para a IBM:
   - IBM Support Assistant
   - A ferramenta Service Request
   - Métodos de upload de dados padrão: FTP, HTTP
   - Métodos de upload de dados seguros: FTPS, SFTP, HTTPS
   - Email

   Se você estiver usando um produto z/OS e usar o ServiceLink / IBMLink para submeter PMRs, será possível enviar dados diagnósticos para o Suporte IBM em um email ou usando FTP.

   Todos esses métodos de troca de dados são explicados no website do Suporte IBM.

Recebendo Informações do Suporte IBM

Ocasionalmente, um representante de suporte técnico IBM pode solicitar a você para fazer download de ferramentas de diagnóstico ou outros arquivos. É possível usar o FTP para fazer download desses arquivos.

Antes de Iniciar

Assegure-se de que seu representante de suporte técnico IBM lhe forneça o servidor preferencial a ser usado para fazer download dos arquivos e os nomes exatos de diretório e arquivo a serem acessados.

Procedimento

Para fazer download de arquivos do Suporte IBM:

1. Use o FTP para se conectar ao site fornecido por seu representante de suporte técnico IBM e efetue login como `anonymous`. Use seu endereço de email como a senha.
2. Altere para o diretório apropriado:
   a. Altere para o diretório `/fromibm`.
      ```
      cd fromibm
      ```
   b. Altere para o diretório fornecido por seu representante de suporte técnico IBM.
      ```
      cd nameofdirectory
      ```
3. Ative o modo binário para sua sessão.
   ```
   binário
   ```
4. Use o comando **get** para fazer download do arquivo especificado por seu representante de suporte técnico IBM.
   ```
   get filename.extension
   ```
5. Termine sua sessão de FTP.
   ```
   quit
   ```

Subscrevendo-se para Atualizações de Suporte

Para manter-se atualizado das informações importantes sobre os produtos IBM que você usa, é possível subscrever-se para as atualizações.

Sobre Esta Tarefa

Subscrevendo-se para receber atualizações sobre o produto, é possível receber informações técnicas e atualizações importantes para ferramentas e recursos específicos do Suporte IBM. É possível subscrever-se para atualizações usando uma destas duas abordagens:

Assinaturas de mídia social

O feed RSS a seguir está disponível para o produto:

- Feed RSS para o fórum do WebSphere eXtreme Scale

Para obter informações gerais sobre RSS, incluindo etapas para introdução e uma lista de páginas da web IBM ativadas para RSS, visite o site IBM Software Support RSS feeds.

My Notifications

Com My Notifications, é possível subscrever-se para atualizações de Suporte para qualquer produto IBM. My Notifications substitui My Support, que é uma ferramenta semelhante que você pode ter usado no

passado. Com My Notifications, é possível especificar se você deseja receber comunicados por email diários ou semanais. É possível especificar quais tipos de informações você deseja receber, como publicações, dicas e sugestões, atualizações do produto (também conhecidas como alertas), downloads e drivers. My Notifications permite customizar e categorizar os produtos sobre os quais você deseja ser informado e os métodos de entrega que melhor se adequam às suas necessidades.

Procedimento

Para subscrever-se para atualizações de Suporte:

1. Subscreva-se para o feed RSS do fórum do WebSphere eXtreme Scale .
   a. Na página de assinatura, clique no ícone de feed RSS.
   b. Selecione a opção que você deseja usar para subscrever-se para o feed.
   c. Clique em **Subscribear**.
2. Subscreva-se para My Notifications acessando o IBM Support Portal e clicando em **My Notifications** no portlet **Notifications**.
3. Efetue sign in usando seu ID IBM e senha e clique em **Submeter**.
4. Identifique o que e como você deseja receber atualizações.
   a. Clique na guia **Subscrever**.
   b. Selecione a marca de software apropriada ou tipo de hardware.
   c. Selecione um ou mais produtos por nome e clique em **Continuar**.
   d. Selecione suas preferências de como receber atualizações, se por email, online em uma pasta designada ou como um feed RSS ou Atom.
   e. Selecione os tipos de atualizações de documentação que você deseja receber, por exemplo, novas informações sobre downloads do produto e comentários do grupo de discussão.
   f. Clique em **Enviar**.

Resultados

Até que modifique suas preferências de feeds RSS e My Notifications, você recebe notificações de atualizações solicitadas. É possível modificar suas preferências quando necessário; por exemplo, se você parar de usar um produto e começar a usar outro produto.

Informações relacionadas

- IBM Software Support RSS feeds
- Subscribe to My Notifications support content updates
- My Notifications for IBM technical support
- My Notifications for IBM technical support overview

Ativando a Criação de Log

É possível usar logs para monitorar e solucionar problemas em seu ambiente.

Sobre Esta Tarefa

Os logs são salvos em diferentes locais e formatos dependendo da sua configuração.

Procedimento

- **Ative os logs em um ambiente independente.**

  Com servidores de catálogos independentes, os logs estão no local no qual você executa o comando start server. Para os servidores de contêiner, é possível usar o local padrão ou definir um local de log customizado:

  – **Local do log padrão:** Os logs estão no diretório no qual o comando start server foi executado. Se você iniciar os servidores no diretório *wxs_home*/bin, os arquivos de log e de rasteio estão nos diretórios logs/<*server_name*> no diretório bin.

  – **Local de log customizado:** Para especificar um local alternativo para os logs do servidor de contêiner, crie um arquivo de propriedades, como server.properties, com o seguinte conteúdo:

  ```
  workingDirectory=<directory>
  traceSpec=
  systemStreamToFileEnabled=true
  ```

  A propriedade **workingDirectory** é o diretório-raiz para os logs e para o arquivo de rastreio opcional. O WebSphere eXtreme Scale cria um diretório com o nome do servidor de contêiner com um arquivo SystemOut.log, um arquivo SystemErr.log e um arquivo de rastreio. Para usar um arquivo de propriedades durante a inicialização de contêiner, use a opção **-serverProps** e forneça o local do arquivo de propriedades do servidor.

- **Ative os logs no WebSphere Application Server.**

  ConsulteWebSphere Application Server: Ativando e Desativando Criação de Log para obter mais informações.

- **Recupere os arquivos FFDC.**

  Os arquivos FFDC servem para que o suporte IBM auxilie na depuração. Estes arquivos poderão ser solicitados pelo suporte IBM quando ocorrer um problema. Esses arquivos aparecem no diretório ffdc e contêm arquivos semelhantes ao seguinte:

  ```
  server2_exception.log
  server2_20802080_07.03.05_10.52.18_0.txt
  ```

- .NET 8.6+ **Ative os logs em um cliente .NET.** Os logs em um cliente .NET são configurados por padrão e são gravados no diretório logs no cliente. Para obter mais informações sobre logs do cliente .NET, consulte "Logs do Cliente .NET" na página 857.

O que Fazer Depois

Visualize os arquivos de log e seus locais especificados. As mensagens comuns para procurar no arquivo SystemOut.log são as mensagens de confirmação de início, como o seguinte exemplo:

```
CWOBJ1001I: ObjectGrid Server catalogServer01 is ready to process requests.
```

Para obter mais informações sobre uma mensagem específica nos arquivos de log, consulte Mensagens.

Referências relacionadas:

"Opções de Rastreio do Servidor" na página 860
É possível ativar o rastreio para fornecer informações sobre o seu ambiente para o suporte IBM.

Mensagens
Quando encontrar uma mensagem em um log ou em outras partes de uma interface de produto, será possível procurar pela mensagem pelo prefixo do componente para obter mais informações.

Configurando a Criação de Log Remota

É possível ativar a criação de log remota para salvar as entradas de log em um servidor remoto. A criação de log remota pode ser útil quando você deve configurar um nível de log de depuração detalhado para ajudar a isolar um problema ou comportamento do monitor durante um período longo.

Antes de Iniciar

- Você deve ter um servidor syslog disponível para atender e capturar eventos.
- Os nomes de seus servidores de catálogos, servidores de contêineres e servidores de aplicativos (se estiver usando o WebSphere Application Server) devem conter somente caracteres alfanuméricos. O Syslog RFC 1364 não permite caracteres não alfanuméricos para o campo TAG. O campo TAG contém o nome do servidor nas mensagens de syslog.

Sobre Esta Tarefa

Use a criação de log remota para análise dos dados históricos. Os servidores em seu ambiente mantêm um número limitado de arquivos de log no sistema. Configure a criação de log remota se você precisar que mais arquivos de log sejam salvos para análise adicional. O servidor de criação de log remoto agrega os dados de diversos servidores. É possível configurar a sua topologia inteira de servidores de catálogo e servidores de contêiner para enviar arquivos para o mesmo servidor de criação de log remoto.

Procedimento

1. Configure a criação de log remota em cada servidor de catálogo ou servidor de contêiner. Ativar a criação de log remota editando as seguintes propriedades no arquivo de propriedades do servidor:

   8.6+ syslogEnabled
   Ativa a criação de log remota para análise de dados históricos. Você deve ter um servidor syslog disponível para atender e capturar eventos.

   Padrão: `false`

   8.6+ syslogHostName
   Especifica o nome do host ou o endereço IP do servidor remoto no qual você deseja registrar dados históricos.

   8.6+ syslogHostPort
   Especifica o número da porta do servidor remoto no qual você deseja registrar dados históricos.

   Valores válidos: `0-65535`

   Padrão: `512`

8.6+ syslogFacility
Indica o tipo de recurso de criação de log remoto que está sendo utilizado.

Valores válidos: `kern, user, mail, daemon, auth, syslog, lpr, news, uucp, cron, authpriv, ftp, sys0, sys1, sys2, sys3,local0, local1, local2, local3, local4, local5, local6, local7`

Padrão: `user`

8.6+ syslogThreshold
Especifica o limite da gravidade das mensagens que você deseja enviar para o servidor de criação de log remoto. Para enviar as mensagens de aviso e graves, insira um valor de `WARNING`. Para enviar mensagens graves apenas, insira `SEVERE`.

Valores válidos: `SEVERE`, `WARNING`

Padrão: `WARNING`

2. Reinicie os servidores de catálogos e servidores de contêiner nos quais você alterou as propriedades. Para obter informações adicionais, consulte Iniciando e Parando Servidores Independentes.

Resultados

As mensagens são enviadas para seu servidor de criação de log remoto configurado para arquivamento e análise.

Logs do Cliente .NET

.NET

Os logs em um cliente .NET são configurados por padrão e são gravados em arquivos no diretório `logs` e no log de eventos do Windows.

Arquivos de Log Padrão

Os arquivos de log a seguir são gerados por padrão.

- **`SystemOut.log`**: Contém mensagens de informações, erro, aviso e falha. Este arquivo está no diretório `logs/` do cliente.
- **`SystemErr.log`**: Contém mensagens de erro e falha. Este arquivo está no diretório `logs/` do cliente.
- **Log de eventos do Windows:** Erros fatais ficam no log de eventos do Windows. Erros fatais ocorrem quando o cliente não pode mais executar transações. As mensagens do WebSphere eXtreme Scale são registradas no log de eventos do Windows como mensagens `WXSEventLog`.

Logs de Rastreio e FFDC

Os logs de rastreio e captura de dados de erros (FFDC) não são ativados por padrão nos clientes .NET. Se você precisar coletar logs de rastreio ou FFDC para um cliente .NET, entre em contato com a equipe de Suporte para obter assistência adicional. Para obter informações adicionais, consulte “Entrando em Contato com o Suporte IBM” na página 851.

Coletando Rastreio

É possível usar o rastreio para monitorar e solucionar problemas em seu ambiente. O rastreio deve ser fornecido para um servidor quando trabalhar com o suporte IBM.

Sobre Esta Tarefa

Coletar rastreio pode ajudá-lo a monitorar e corrigir problemas em sua implementação do WebSphere eXtreme Scale. A maneira como o rastreio é coletado depende da sua configuração. Consulte "Opções de Rastreio do Servidor" na página 860 para obter a lista das especificações de rastreio diferentes que podem ser coletadas.

Procedimento

- **Colete o rastreio dentro de um ambiente WebSphere Application Server.**

  Se o seus servidores de catálogos e de contêiner estiverem em um ambiente WebSphere Application Server, consulte WebSphere Application Server: Trabalhando com Rastreio para obter mais informações.

- **Colete o rastreio com o comando start do servidor de catálogos ou de contêiner independente.**

  É possível configurar o rastreio em um serviço de catálogo ou servidor de contêiner utilizando os parâmetros **-traceSpec** e **-traceFile** com o comando start server. Por exemplo:

  ```
  startOgServer.sh catalogServer -traceSpec ObjectGridPlacement=all=enabled -traceFile  /home/user1/logs/trace.log
  ```

  8.6+

  ```
  startXsServer.sh catalogServer -traceSpec ObjectGridPlacement=all=enabled -traceFile  /home/user1/logs/trace.log
  ```

  O parâmetro **-traceFile** é opcional. Se não configurar um local **-traceFile**, o arquivo de rastreio irá para o mesmo local dos arquivos de log do sistema.Para obter mais informações sobre estes parâmetros, consulte Script **startOgServer** (ORB) e Script **startXsServer** (XIO).

- **Colete o rastreio no servidor de catálogos ou de contêiner independente com um arquivo de propriedades.**

  Para coletar rastreio a partir de um arquivo de propriedades, crie um arquivo, como `server.properties`, com o seguinte conteúdo:

  ```
  workingDirectory=<directory>
  traceSpec=<trace_specification>
  systemStreamToFileEnabled=true
  ```

  A propriedade **workingDirectory** é o diretório-raiz para os logs e para o arquivo de rastreio opcional. Se o valor **workingDirectory** não estiver configurado, o diretório de trabalho padrão será o local usado para iniciar os servidores, como *wxs_home*`/bin`. Para usar um arquivo de propriedades durante a inicialização do servidor, utilize o parâmetro **-serverProps** com o comando **startOgServer** e forneça o local do arquivo de propriedades do servidor.Para obter mais informações sobre o arquivo de propriedades de servidor e como usar o arquivo, consulte Arquivo de Propriedades do Servidor.

- Java **Colete o rastreio em um cliente Java independente.**

  É possível iniciar a coleção de rastreio em um cliente independente ao incluir propriedades do sistema no script de inicialização para o aplicativo cliente. No exemplo a seguir, as configurações de rastreio são especificadas para o aplicativo `com.ibm.samples.MyClientProgram`:

```
java -DtraceSettingsFile=MyTraceSettings.properties
-Djava.util.logging.manager=com.ibm.ws.bootstrap.WsLogManager
-Djava.util.logging.configureByServer=true com.ibm.samples.MyClientProgram
```

Para obter mais informações, consulte WebSphere Application Server: Ativando o Rastreio nos Aplicativos Clientes e Independentes.

- .NET 8.6+ **Colete o rastreio em um cliente .NET.**

  O rastreio não é ativado por padrão para clientes .NET. Se desejar coletar o rastreio para um cliente .NET, entre em contato com a equipe de Suporte para obter assistência adicional. Para obter informações adicionais, consulte "Entrando em Contato com o Suporte IBM" na página 851.

- Java **Colete o rastreio com a interface ObjectGridManager.**

  Também é possível configurar o rastreio durante o tempo de execução em uma interface ObjectGridManager. A configuração de um rastreio em uma interface ObjectGridManager pode ser usada para obter rastreio em um cliente eXtreme Scale enquanto ele se conecta com um eXtreme Scale e confirma as transações. Para configurar o rastreio em uma interface ObjectGridManager, forneça uma especificação de rastreio e um log de rastreio.

  ```
  ObjectGridManager manager= ObjectGridManagerFactory.getObjectGridManager();
  ...
  manager.setTraceEnabled(true);
  manager.setTraceFileName("logs/myClient.log");
  manager.setTraceSpecification("ObjectGridReplication=all=enabled");
  ```

  Para obter mais informações sobre a interface ObjectGridManager, consulte "Interagindo com um ObjectGrid Usando a Interface ObjectGridManager" na página 350.

- **Colete o rastreio em servidores de contêiner com o utilitário `xscmd`.**

  Para coletar o rastreio com o utilitário **`xscmd`**, use o comando **`-c setTraceSpec`**. Use o utilitário **`xscmd`** para coletar o rastreio em um ambiente independente durante o tempo de execução em vez de durante a inicialização. É possível coletar o rastreio em todos os servidores e serviços de catálogo ou filtrar os servidores com base no nome do ObjectGrid, e em outras propriedades. Por exemplo, para coletar o rastreio ObjectGridReplication com acesso ao servidor de serviço de catálogo, execute:

  ```
  xscmd -c setTraceSpec -spec "ObjectGridReplication=all=enabled"
  ```

  Também é possível desativar o rastreio ao configurar a especificação de rastreio para `*=all=disabled.`.

Resultados

Os arquivos de rastreio são gravados no local especificado.

Referências relacionadas:

"Opções de Rastreio do Servidor"
É possível ativar o rastreio para fornecer informações sobre o seu ambiente para o suporte IBM.

Mensagens
Quando encontrar uma mensagem em um log ou em outras partes de uma interface de produto, será possível procurar pela mensagem pelo prefixo do componente para obter mais informações.

Opções de Rastreio do Servidor

É possível ativar o rastreio para fornecer informações sobre o seu ambiente para o suporte IBM.

Sobre o Rastreio

O rastreio do WebSphere eXtreme Scale é dividido em vários componentes diferentes. É possível especificar o nível de rastreio a ser usado para um servidor de catálogos ou servidor de contêiner. Os níveis comuns de rastreio incluem: all, debug, entryExit e event.

Um exemplo de cadeia de rastreio é o seguinte:

```
ObjectGridComponent=level=enabled
```

É possível concatenar as cadeias de rastreio. Use o sinal de asterisco (*) para especificar um valor de curinga, como `ObjectGrid*=all=enabled`. Se for necessário fornecer um rastreio para o suporte IBM, uma cadeia de rastreio específica será solicitada. Por exemplo, se ocorrer um problema com a replicação, a cadeia de rastreio `ObjectGridReplication=debug=enabled` pode ser solicitada.

Especificação de Rastreio

ObjectGrid
Mecanismo de cache principal geral.

ObjectGridCatalogServer
Serviço de catálogo geral.

ObjectGridChannel
Comunicações de topologia de implementação estática.

ObjectGridClientInfo
Informações do cliente do DB2.

ObjectGridClientInfoUser
Informações sobre o usuário do DB2.

ObjectgridCORBA
Comunicações de topologia de implementação dinâmica.

ObjectGridDataGrid
A API do AgentManager.

ObjectGridDynaCache
O provedor de cache dinâmico do WebSphere eXtreme Scale.

ObjectGridEntityManager
A API do EntityManager. Utilize com a opção Projector.

ObjectGridEvictors
Evictors integrados do ObjectGrid.

ObjectGridJPA
Carregadores do Java Persistence API (JPA).

ObjectGridJPACache
Plug-ins do Cache JPA

ObjectGridLocking
Gerenciador de bloqueios de entrada de cache do ObjectGrid.

8.6+ ObjectGridLogHandler
Informações de criação de log remota.

ObjectGridMBean
Beans de gerenciamento.

ObjectGridMonitor
Infraestrutura de monitoramento histórico.

ObjectGridNative
Rastreio do código nativo do WebSphere eXtreme Scale, incluindo o código nativo eXtremeMemory.

ObjectGridOSGi
Os componente de integração de OSGi do WebSphere eXtreme Scale.

ObjectGridPlacement
Serviço de disposição de shards do servidor de catálogos.

ObjectGridQuery
Consulte ObjectGrid.

ObjectGridReplication
Serviço de replicação.

ObjectGridRouting
Detalhes de roteamento do cliente/servidor.

ObjectGridSecurity
Rastreio de segurança.

ObjectGridSerializer
A infraestrutura do plug-in DataSerializer.

ObjectGridStats
Estatísticas do ObjectGrid.

ObjectGridTransactionManager
O gerenciador de transações do WebSphere eXtreme Scale.

ObjectGridWriteBehind
Atributo write-behind do ObjectGrid.

ObjectGridXA
Rastreio de transação multipartição.

ObjectGridXM
Rastreio geral do IBM eXtremeMemory.

ObjectGridXMEviction
Rastreio de despejo do eXtremeMemory.

ObjectGridXMTransport
Rastreio de transporte geral do eXtremeMemory.

ObjectGridXMTransportInbound
Rastreio de transporte específico da entrada do eXtremeMemory.

ObjectGridXMTransportOutbound
Rastreio de transporte específico da saída do eXtremeMemory.

Projector
O mecanismo dentro da API do EntityManager.

QueryEngine
O mecanismo de consulta para a API de Consulta do Objeto e a API de Consulta do EntityManager.

QueryEnginePlan
Rastreio do plano de consulta.

TCPChannel
O canal TCP/IP do IBM eXtremeIO.

XsByteBuffer
Rastreio do buffer de bytes do WebSphere eXtreme Scale.

Tarefas relacionadas:

"Ativando a Criação de Log" na página 854
É possível usar logs para monitorar e solucionar problemas em seu ambiente.

"Coletando Rastreio" na página 858
É possível usar o rastreio para monitorar e solucionar problemas em seu ambiente. O rastreio deve ser fornecido para um servidor quando trabalhar com o suporte IBM.

Iniciando Servidores Independentes que Usam o Transporte ORB
(Descontinuado) Quando estiver executando uma configuração independente, o ambiente será constituído pelos servidores de catálogos, servidores de contêiner e processos do cliente. Os servidores do WebSphere eXtreme Scale também podem ser integrados em aplicativos Java existentes usando a API do servidor integrado. É necessário configurar e iniciar estes processos manualmente.

Administrando com o Utilitário **xscmd**
Com o utilitário **xscmd**, é possível concluir tarefas administrativas no ambiente, tal como: estabelecer links de replicação multi-master, substituir o quorum e parar os grupos de servidores com o comando teardown.

Resolução de Problemas com High Performance Extensible Logging (HPEL)

HPEL é um recurso de log e de rastreio que você pode utilizar em ambientes independentes e WebSphere Application Server. É possível utilizar HPEL para armazenar e acessar informações de log, rastreio, `System.err` e `System.out` produzidas pelo servidor de aplicativos ou aplicativos. HPEL é uma alternativa para o recurso básico de log e de rastreio, que fornece os logs da Java virtual machine (JVM), o rastreio de diagnóstico e os arquivos de log de serviço. Esses arquivos são geralmente chamados de `SystemOut.log/SystemErr.log`, `trace.log` e `activity.log`. O HPEL fornece um repositório de dados de log, um repositório de dados de rastreio e um arquivo de log de texto.

Sobre Esta Tarefa

Em vez do recurso de criação de log existente, é possível utilizar HPEL, que é desativado por padrão. No modo HPEL, o conteúdo de log e de rastreio é gravado em um repositório de dados do log ou dados de rastreio em um formato binário do proprietário. Portanto, desativar HPEL pode melhorar o desempenho do servidor fornecendo recursos de manipulação de log e de rastreio mais rápidos. Ative o HPEL com os arquivos de propriedades do servidor para seus servidores

de contêiner e servidores de catálogo. Depois de ativar o HPEL, toda a criação de log do WebSphere eXtreme Scale e os arquivos de log resultantes são colocados no local do repositório HPEL especificado.

Procedimento

1. Configure as propriedades para ativar a criação de log HPEL. Edite o Arquivo de Propriedades do Servidor para cada servidor de contêiner e de catálogo com as propriedades que você deseja utilizar.

   8.6+ hpelEnable
   Especifica se o High Performance Extensible Log (HPEL) está ativado. A criação de log de HPEL é ativada quando a propriedade é configurada como `true`.

   Padrão: `false`

   8.6+ hpelRepositoryLocation
   Especifica o local do repositório de criação de log HPEL.

   Padrão: `"."` (o local de tempo de execução)

   8.6+ hpelEnablePurgeBySize
   Indica se o HPEL limpa arquivos de log por tamanho. É possível configurar o tamanho dos arquivos com a propriedade hpelMaxRepositorySize.

   Padrão: `true` (ativado)

   8.6+ hpelEnablePurgeByTime
   Indica se o HPEL limpa arquivos de log por tempo. Configure a quantidade de tempo com a propriedade hpelMaxRetentionTime.

   Padrão: `true` (ativado)

   8.6+ hpelEnableFileSwitch
   Indica se o arquivo HPEL está ativado para criar um novo arquivo em uma hora especificada. Utilize a propriedade hpelFileSwitchHour para especificar a hora em que deseja criar um novo arquivo.

   Padrão: `false` (desativado)

   8.6+ hpelEnableBuffering
   Indica se o armazenamento em buffer HPEL está ativado.

   Padrão: `false` (desativado)

   8.6+ hpelIncludeTrace
   Indica se os arquivos de texto HPEL incluem o rastreio.

   Padrão: `false` (desativado)

   8.6+ hpelOutOfSpaceAction
   Indica a ação a ser executada quando o espaço em disco foi excedido.

   Padrão: `PurgeOld`

   Valores possíveis: `PurgeOld, StopServer, StopLogging`

   8.6+ hpelOutputFormat
   Indica o formato dos arquivos de log a serem gerados.

   Padrão: `Basic`

   Valores possíveis: `Basic, Advanced, CBE-1.0.1`

8.6+ hpelMaxRepositorySize
Indica o tamanho máximo de arquivos, em megabytes. Este valor é utilizado quando você ativa a propriedade hpelEnablePurgeBySize.

Padrão: `50`

8.6+ hpelMaxRetentionTime
Indica o tempo máximo de retenção para conter os arquivos, em horas.

Padrão: `48`

8.6+ hpelFileSwitchHour
Indica a hora na qual criar um novo arquivo. Este valor é utilizado quando a propriedade hpelEnableFileSwitch é ativada.

Padrão: `0`

2. Reinicie os servidores nos quais você modificou o arquivo de propriedades do servidor para configurar as propriedades HPEL. Após o HPEL ser ativado e o servidor reiniciado, as informação de criação de log do WebSphere eXtreme Scale anteriores não estarão mais disponíveis. As informações de criação de log anteriores são substituídas por informações de HPEL equivalentes. Para obter mais informações, consulte Iniciando e Parando Servidores Independentes e Iniciando e Parando Servidores em um Ambiente do WebSphere Application Server.
3. Use o visualizador de logs de linha de comandos do HPEL para visualizar seus arquivos de log. O visualizador de log da linha de comandos é uma solução poderosa, porém simples, para visualizar informações de criação de log. Para obter uma referência detalhada das opções do visualizador de linha de comandos, consulte Centro de Informações do WebSphere Application Server: Ferramenta de Linha de Comandos LogViewer.
   a. Em um prompt de comandos, vá para o diretório `bin`. Windows
   ```
   C:\Arquivos de Programas\IBM\WebSphere\eXtremeScale\ObjectGrid\bin
   ```
   Linux UNIX
   ```
   /opt/IBM/WebSphere/eXtremeScale/ObjectGrid/bin
   ```
   b. Execute o seguinte comando para obter ajuda com o visualizador de log:
   Windows
   ```
   logViewer -help
   ```
   Linux UNIX
   ```
   ./logViewer.sh -help
   ```
4. Alguns comandos comuns que você pode usar com o visualizador de log estão a seguir:
   - Execute o comando a seguir para criar um arquivo de log de formato legado, `legacyFormat.log`, que contém somente registros de log INFO, WARNING e SEVERE: Windows
   ```
   logViewer -outLog ..\logs\legacyFormat.log -minLevel INFO -maxLevel SEVERE
   ```
   Linux UNIX
   ```
   ./logViewer.sh -outLog ../logs/legacyFormat.log -minLevel INFO -maxLevel SEVERE
   ```
   Utilize um editor de texto para visualizar o arquivo de log de formato legado que você criou.

- Execute o seguinte comando para visualizar apenas os registros de log para o encadeamento 0: Windows

  ```
  logViewer -thread 0
  ```

  Linux UNIX

  ```
  ./logViewer.sh -thread 0
  ```

- Execute o seguinte comando para visualizar apenas mensagens WARNING: Windows

  ```
  logViewer -level WARNING
  ```

  Linux UNIX

  ```
  ./logViewer.sh -level WARNING
  ```

- Execute o seguinte comando para recuperar todos os registros de log NÃO de criadores de logs que começam com `com.ibm`: Windows

  ```
  logViewer -excludeLoggers com.ibm.*
  ```

  Linux UNIX

  ```
  ./logViewer.sh -excludeLoggers com.ibm.*
  ```

- Execute o comando a seguir para extrair um repositório apenas de mensagens WARNING e SEVERE e salve o arquivo resultante em um novo diretório: Windows

```
logViewer -minLevel WARNING -maxLevel SEVERE -extractToNewRepository ..\logs\newHPELRepository
```

Linux UNIX

```
./logViewer.sh -minLevel WARNING -maxLevel SEVERE -extractToNewRepository ../logs/newHPELRepository
```

- Execute o seguinte comando para exportar o conteúdo do repositório resultante para um arquivo de log de formato de texto: Windows

```
logViewer -repositoryDir ..\logs\newHPELRepository -outLog ..\logs\newFormat.log
```

Linux UNIX

```
./logViewer.sh -repositoryDir ../logs/newHPELRepository -outLog ../logs/newFormat.log
```

Use um editor de texto para visualizar o arquivo de log resultante.

Analisando Dados de Log e de Rastreio

É possível utilizar as ferramentas de análise de log para analisar como seu ambiente de tempo de execução está sendo executado e resolver problemas que ocorrem no ambiente.

Sobre Esta Tarefa

É possível gerar relatórios a partir dos arquivos existentes de log e de rastreio no ambiente. Esses relatórios visuais podem ser usados para as seguintes finalidades:

- **Analisar o status e o desempenho do ambiente de tempo de execução:**
  - Implementar consistência do ambiente
  - Criar log da frequência
  - Topologia de execução versus topologia configurada
  - Mudanças de topologia não planejadas

  - Status de quorum
  - Status de replicação de partição
  - Estatísticas de memória, rendimento, uso do processador, e assim por diante
- **Para resolver problemas no ambiente:**
  - Visualizações de topologia em pontos no tempo específicos
  - Estatísticas de memória, rendimento, uso do processador durante falhas do cliente
  - Níveis de fix pack atuais, ajuste de configurações
  - Status de quorum

Visão Geral de Análise de Log

É possível usar a ferramenta **xsLogAnalyzer** para ajudar a resolver problemas no ambiente.

Todas as Mensagens de Failover

Exibe o número total de mensagens de failover como um gráfico ao longo do tempo. Também exibe uma lista das mensagens de failover, incluindo os servidores que foram afetados.

Todas as Mensagens Críticas do eXtreme Scale

Exibe os IDs de mensagem junto com as explicações e ações do usuário associadas, o que pode economizar o tempo de procura por mensagens.

Todas as Exceções

Exibe as cinco principais exceções, incluindo as mensagens e quantas vezes elas ocorreram e quais servidores foram afetados pela exceção.

Resumo de Topologia

Exibe um diagrama de como sua topologia é configurada de acordo com os arquivos de log. Este resumo pode ser usado para comparar a configuração real, possivelmente a identificação de erros de configuração.

Consistência de Topologia: Tabela de Comparação do Object Request Broker (ORB)

Exibe configurações ORB no ambiente. É possível usar essa tabela para ajudar a determinar se as configurações estão consistentes em seu ambiente.

Visualização de Linha de Tempo de Eventos

Exibe um diagrama de linha de tempo de diferentes ações que ocorreram na grade de dados, incluindo eventos de ciclo de vida, exceções, mensagens críticas e eventos de captura de dados de erros (FFDC).

Executando Análise de Log

É possível executar a ferramenta **xsLogAnalyzer** em um conjunto de arquivos de log e de rastreio a partir de qualquer computador.

Antes de Iniciar

- Ative os logs e rastreio. Consulte “Ativando a Criação de Log” na página 854 e “Coletando Rastreio” na página 858 para obter mais informações.
- Colete os arquivos de log. Os arquivos de log podem estar em vários locais dependendo de como eles foram configurados. Se você estiver usando as configurações de log padrão, os arquivos de log poderão ser obtidos a partir dos seguintes locais:
  - Em uma instalação independente:*wxs_install_root*/bin/logs/<*server_name*>
  - Em uma instalação integrada ao WebSphere Application Server: *was_root*/logs/<*server_name*>
- Colete os arquivos de rastreio. Os arquivos de rasteio podem estar em vários locais dependendo de como eles foram configurados. Se você estiver usando as configurações de rastreio padrão, os arquivos de trace poderão ser obtidos a partir dos seguintes locais:
  - Em uma instalação independente: Se nenhum valor de rastreio específico for configurado, os arquivos de rastreio serão gravados para o mesmo local que o sistema de arquivos de log.
  - Em uma instalação que é integrada com o WebSphere Application Server: *was_root*/profiles/*server_name*/logs.

  Copie os arquivos de log e rastreio no computador a partir do qual você está planejando usar a ferramenta Log Analyzer.
- Se desejar criar scanners customizados no relatório gerado, crie um arquivo de propriedades de especificações do scanner e o arquivo de configuração antes de executar a ferramenta. Para obter informações adicionais, consulte “Criando Scanners Customizados para Análise do Log” na página 868.

Procedimento

1. Execute a ferramenta **xsLogAnalyzer**.

   O script está nos seguintes locais:

   - Em uma instalação independente : *wxs_install_root*/ObjectGrid/bin
   - Em uma instalação integrada ao WebSphere Application Server: *was_root*/bin

   Dica: Se seus arquivos de log forem grandes, considere usar os parâmetros **-startTime**, **-endTime** e **-maxRecords** quando executar o relatório para restringir o número de entradas de log que são varridos. Usar esses parâmetros quando você executa o relatório torna os relatórios mais fáceis de ler e de executar com mais eficiência. É possível executar diversos relatórios no mesmo conjunto de arquivos de log.

   ```
   xsLogAnalyzer.sh|bat -logsRoot c:\myxslogs -outDir c:\myxslogs\out
   -startTime 11.09.27_15.10.56.089 -endTime 11.09.27_16.10.56.089 -maxRecords 100
   ```

   -logsRoot
   Especifica o caminho absoluto para o diretório de log que você deseja avaliar (necessário).

   -outDir
   Especifica um diretório existente para gravar a saída do relatório. Se você não especificar um valor, o relatório será gravado no local raiz da ferramenta **xsLogAnalyzer**.

   -startTime
   Especifica o horário de início para avaliar nos logs. A data está no formato a seguir: *year.month.day_hour.minute.second.millisecond*

-endTime
Especifica o horário de encerramento para avaliar nos logs. A data está no formato a seguir: *year.month.day_hour.minute.second.millisecond*

-trace Especifica uma sequência de rastreio, tal como `ObjectGrid*=all=enabled`.

-maxRecords
Especifica o número máximo de registros a serem gerados no relatório. O padrão é `100`. Se você especificar o valor como 50, os primeiros 50 registros serão gerados para o período de tempo especificado.

2. Abra os arquivos gerados. Se um diretório de saída não foi definido, os relatórios serão gerados em uma pasta chamada `report_date_time`. Para abrir a página principal dos relatórios, abra o arquivo `index.html`.
3. Use os relatórios para analisar os dados do log. Use as dicas a seguir para maximizar o desempenho das exibições de relatório:
   - Para maximizar o desempenho de consultas nos dados de log, use informações o mais específicas possível. Por exemplo, uma consulta para `server` leva muito mais tempo para ser executada e retorna mais resultados do que `server_host_name`.
   - Algumas visualizações têm um número limitado de pontos de dados que são exibidos de uma vez. É possível ajustar o segmento de tempo que está sendo visualizado alterando os dados atuais, tais como a hora de início e de encerramento, na visualização.

O que Fazer Depois

Para obter mais informações sobre resolução de problemas da ferramenta **xsLogAnalyzer** e os relatórios gerados, consulte "Resolução de Problemas da Análise do Log" na página 869.

Criando Scanners Customizados para Análise do Log

É possível criar scanners customizados para análise do log. Depois de configurar o scanner, os resultados são gerados nos relatórios quando você executa a ferramenta **xsLogAnalyzer**. O scanner customizado varre os logs para os registros de eventos com base nas expressões regulares que você especificou.

Procedimento

1. Crie um arquivo de propriedades de especificações do scanner que especifica a expressão geral para executar o scanner customizado.
   a. Crie e salve um arquivo de propriedades. O arquivo deve estar no diretório *loganalyzer_root*`/config/custom`. É possível nomear o arquivo como: you like. O arquivo é usado pelo novo scanner, portanto, nomear o scanner no arquivo de propriedades é útil, por exemplo: *my_new_server_scanner_spec*`.properties`.
   b. Inclua as propriedades a seguir no arquivo *my_new_server_scanner_spec*`.properties`:

      ```
      include.regular_expression = REGULAR_EXPRESSION_TO_SCAN
      ```

      A variável *REGULAR_EXPRESSION_TO_SCAN* é uma expressão regular na qual filtrar os arquivos de log.

      Exemplo: Para varrer em busca de instâncias de linhas que contêm as sequências `"xception"` e `"rror"` independentemente da ordem, configure a propriedade **include.regular_expression** com o valor a seguir:

```
include.regular_expression = (xception.+rror)|(rror.+xception)
```

Esta expressão regular faz com que os eventos sejam registrados se a sequência "rror" vier antes ou após a sequência "xception".

Exemplo:Para varrer através de cada linha nos logs em busca de instâncias de linhas que contêm as sequências de frase "xception" ou a frase "rror" independetemente da ordem, configure a propriedade **include.regular_expression** com o valor a seguir:

```
include.regular_expression = (xception)|(rror)
```

Essa expressão regular faz com que os eventos sejam registrados se a sequência "rror" ou "xception" existir.

2. Crie um arquivo de configuração que a ferramenta **xsLogAnalyer** usa para criar o scanner.
   a. Crie e salve um arquivo de configuração. O arquivo deve estar no diretório *loganalyzer_root*/config/custom. É possível nomear o arquivo como *scanner_name*Scanner.config, em que *scanner_name* é um nome exclusivo para o novo scanner. Por exemplo, você pode nomear o arquivo serverScanner.config
   b. Inclua as propriedades a seguir no arquivo *scanner_name*Scanner.config:

      ```
      scannerSpecificationFiles = LOCATION_OF_SCANNER_SPECIFICATION_FILE
      ```

      A variável *LOCATION_OF_SCANNER_SPECIFICATION_FILE* é o caminho e o local do arquivo de especificação que você criou na etapa anterior. Por exemplo: *loganalyzer_root*/config/custom/my_new_scanner_spec.properties. Também é possível especificar diversos arquivos de especificação de scanner usando uma lista separada por ponto e vírgula:

```
scannerSpecificationFiles = LOCATION_OF_SCANNER_SPECIFICATION_FILE1;LOCATION_OF_SCANNER_SPECIFICATION_FILE2
```

3. Execute a ferramenta **xsLogAnalyzer**. Para obter informações adicionais, consulte “Executando Análise de Log” na página 866.

Resultados

Depois de executar a ferramenta **xsLogAnalyzer**, o relatório contém novas guias no relatório para os scanners customizados que você configurou. Cada guia contém as visualizações a seguir:

Gráficos
Um gráfico plotado que ilustra os eventos registrados. Os eventos são exibidos na ordem na qual os eventos foram localizados.

Tabelas
Uma representação tabular dos eventos registrados.

Relatórios Resumo

Resolução de Problemas da Análise do Log

Use as informações de resolução de problemas a seguir para diagnosticar e corrigir problemas com a ferramenta **xsLogAnalyzer** e seus relatórios gerados.

Procedimento

- **Problema:** Ocorrem condições de falta de memória quando você está usando a ferramenta **xsLogAnalyzer** para gerar relatórios. Um exemplo de um erro que pode ocorrer é o seguinte: `java.lang.OutOfMemoryError: Limite de sobrecarga de GC excedido`.

  Solução: A ferramenta **xsLogAnalyzer** é executada dentro de uma Java virtual machine (JVM). É possível configurar a JVM para aumentar o tamanho de heap antes de executar a ferramenta **xsLogAnalyzer** especificando algumas configurações quando você executa a ferramenta. O aumento do tamanho de heap permite que mais registros de eventos sejam armazenados na memória da JVM. Comece com uma configuração de 2048 M, assumindo que o sistema operacional possui memória principal suficiente. Na mesma instância de linha de comandos na qual você está planejando executar a ferramenta **xsLogAnalyzer**, configure o tamanho máximo de heap da JVM:

  ```
  java -Xmx HEAP_SIZE m
  ```

  O valor de *HEAP_SIZE* pode ser qualquer número inteiro e representa o número de megabytes que são alocados para o heap da JVM. Por exemplo, você pode executar `java -Xmx2048m`. Se as mensagens de falta de memória continuarem, ou você não tiver os recursos para alocar 2048m ou mais de memória, limite o número de eventos que estão sendo mantidos no heap. É possível limitar o número máximo de eventos no heap transmitindo o parâmetro **-maxRecords** para o comando **xsLogAnalyzer**

- **Problema:** Quando você abre um relatório gerado a partir da ferramenta **xsLogAnalyzer**, o navegador é interrompido ou não carrega a página.

  Causa: Os arquivos HTML gerados são muito grandes e não podem ser carregados pelo navegador. Esses arquivos são grandes porque o escopo dos arquivos de log que você está analisando é muito amplo.

  Solução: Considere usar os parâmetros **-startTime**, **-endTime** e **-maxRecords** quando você executar a ferramenta **xsLogAnalyzer** para restringir o número de entradas de log que são varridas. Usar esses parâmetros quando você executa o relatório torna os relatórios mais fáceis de ler e de executar com mais eficiência. É possível executar diversos relatórios no mesmo conjunto de arquivos de log.

Resolução de Problemas da Instalação do Produto

O IBM Installation Manager é um instalador comum para muitos produtos de software IBM que você utiliza para instalar esta versão do WebSphere eXtreme Scale.

Resultados

Notas sobre criação de log e rastreio:

- Uma maneira fácil de visualizar os logs é abrir o Installation Manager e ir para **Arquivo > Visualizar Log**. Um arquivo de log individual pode ser aberto selecionando-o na tabela e, em seguida, clicando no ícone **Abrir Arquivo de Log**.
- Os logs estão localizados no diretório `logs` do local de dados do aplicativo Installation Manager. Por exemplo:
  - Windows **Instalação administrativa:**

```
C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager
```

  - Windows **Instalação não administrativa:**

```
C:\Documents and Settings\user_name\Application Data\IBM\Installation Manager
```

– UNIX Linux **Instalação administrativa:**

```
/var/IBM/InstallationManager
```

– UNIX Linux **Instalação não administrativa:**

```
user_home/var/ibm/InstallationManager
```

- Os arquivos de log principais são arquivos XML com registro de data e hora no diretório `logs` e podem ser visualizados usando qualquer navegador da Web padrão.
- O arquivo `log.properties` no diretório `logs` especifica o nível de criação de log ou de rastreio que o Installation Manager utiliza. Para ativar o rastreio para os plug-ins do WebSphere eXtreme Scale, por exemplo, crie um arquivo `log.properties` com o conteúdo a seguir:

```
com.ibm.ws=DEBUG
com.ibm.cic.agent.core.Engine=DEBUG
global=DEBUG
```

Reinicie o Installation Manager conforme necessário e as saídas do Installation Manager são rastreadas para os plug-ins do WebSphere eXtreme Scale.

Observações sobre resolução de problemas:

- UNIX Linux Por padrão, alguns sistemas HP-UX são configurados para utilizar DNS para resolver nomes de host. Isso poderia resultar no Installation Manager não poder se conectar a um repositório externo.

  É possível executar ping no repositório, mas o nslookup não retorna nada.

  Trabalhe com o seu administrador do sistema para configurar sua máquina para usar DNS ou use o endereço IP do repositório.
- Em alguns casos, você poderá precisar ignorar os mecanismos de verificação existentes no Installation Manager.
  – Em alguns sistemas de arquivos de rede, às vezes o espaço em disco talvez não seja relatado corretamente e você poderá precisar ignorar a verificação do espaço em disco e continuar com a instalação.

    Para desativar a verificação do espaço em disco, especifique a seguinte propriedade do sistema no arquivo `config.ini` em *IM_install_root*`/eclipse/configuration` e reiniciar o Installation Manager:

```
cic.override.disk.space=sizeunit
```

em que *size* é um número inteiro positivo e *unit* está em branco para bytes, k para kilo, m para megabytes ou g para gigabytes. Por exemplo:

```
cic.override.disk.space=120 (120 bytes)
cic.override.disk.space=130k (130 kilobytes)
cic.override.disk.space=140m (140 megabytes)
cic.override.disk.space=150g (150 gigabytes)
cic.override.disk.space=true
```

O Installation Manager relatará o tamanho de um espaço em disco de Long.MAX_VALUE. Em vez de exibir uma quantidade muito grande de espaço em disco disponível, N/D será exibido.

  – Para ignorar a verificação de pré-requisito do sistema operacional, inclua `disableOSPrereqChecking=true` no arquivo `config.ini` em *IM_install_root*`/eclipse/configuration` e reinicie o Installation Manager.

  Se você precisar usar qualquer um desses métodos de bypass, contate o Suporte IBM para obter assistência no desenvolvimento de uma solução que não envolva o bypass de mecanismos de verificação do Installation Manager.
- Para obter informações adicionais sobre o uso do Installation Manager, leia o Centro de Informações do IBM Installation Manager Versão 1.5.

Leia as notas sobre o release para aprender mais sobre a versão mais recente do Installation Manager. Para acessar as notas sobre o release, conclua a seguinte tarefa:

  – Windows Clique em **Iniciar > Programas > IBM Installation Manager > Notas sobre a Liberação**.

  – UNIX Linux Vá para o subdiretório de documentação no diretório em que o Installation Manager está instalado e abra o arquivo `readme.html`.

- Se ocorrer um erro fatal ao tentar instalar o produto, execute as etapas a seguir:
  – Faça uma cópia de backup de seu diretório de instalação do produto atual no caso de o suporte IBM precisar revisá-lo posteriormente.
  – Use o Installation Manager para desinstalar tudo o que você instalou sob o local da instalação do produto (grupo de pacotes). Você pode se deparar com erros, mas eles podem ser seguramente ignorados.
  – Exclua tudo o que permanecer no diretório de instalação do produto.
  – Use o Installation Manager para reinstalar o produto para o mesmo local ou para um novo local.

Observação sobre informações de versão e histórico: Os comandos **`versionInfo`** e **`historyInfo`** retornam informações de versão e histórico com base em todas as atividades de instalação, desinstalação, atualização e retrocesso executadas no sistema.

Resolução de Problemas de Conectividade do Cliente

Java

Há vários problemas comuns específicos para clientes e de conectividade do cliente que podem ser resolvidos conforme descrito nas seções a seguir.

Procedimento

- **Problema:** Se você estiver usando a API EntityManager ou mapas de matriz de bytes com o modo de cópia COPY_TO_BYTES, os métodos de acesso a dados do cliente resultarão em várias exceções relacionadas à serialização ou uma exceção NullPointerException.
  – O seguinte erro ocorre quando você está usando o modo de cópia COPY_TO_BYTES:

```
java.lang.NullPointerException
        at com.ibm.ws.objectgrid.map.BaseMap$BaseMapObjectTransformer2.inflateObject(BaseMap.java:5278)
        at com.ibm.ws.objectgrid.map.BaseMap$BaseMapObjectTransformer.inflateValue(BaseMap.java:5155)
```

  – O seguinte erro ocorre quando você está usando a API EntityManager :

```
java.lang.NullPointerException
  at com.ibm.ws.objectgrid.em.GraphTraversalHelper.fluffFetchMD(GraphTraversalHelper.java:323)
  at com.ibm.ws.objectgrid.em.GraphTraversalHelper.fluffFetchMD(GraphTraversalHelper.java:343)
  at com.ibm.ws.objectgrid.em.GraphTraversalHelper.getObjectGraph(GraphTraversalHelper.java:102)
  at com.ibm.ws.objectgrid.ServerCoreEventProcessor.getFromMap(ServerCoreEventProcessor.java:709)
  at com.ibm.ws.objectgrid.ServerCoreEventProcessor.processGetRequest(ServerCoreEventProcessor.java:323)
```

Causa: A API EntityManager e o modo de cópia COPY_TO_BYTES usam um repositório de metadados que é integrado na grade de dados. Quando os clientes se conectam, a grade de dados armazena os identificadores de repositório no cliente e armazena em cache os identificadores enquanto o cliente estiver conectado. Se você reiniciar a grade de dados, todos os metadados serão perdidos e os identificadores regenerados não corresponderão aos identificadores em cache no cliente.

Solução: Se você estiver usando a API EntityManager ou o modo de cópia COPY_TO_BYTES, desconecte e reconecte todos os clientes se o ObjectGrid for interrompido e reiniciado. Desconectar e reconectar os clientes atualiza o cache do identificador de metadados. Os clientes podem ser desconectados usando o método ObjectGridManager.disconnect ou o método ObjectGrid.destroy.

- **Problema:** O cliente é interrompido durante uma chamada de método de getObjectGrid.

  Um cliente pode ser interrompido ao chamar o método getObjectGrid no ObjectGridManager ou lançar uma exceção: com.ibm.websphere.projector.MetadataException. O repositório EntityMetadata não está disponível e o limite de tempo limite é alcançado.

  Causa: O motivo é que o cliente está aguardando os metadados da entidade no servidor ObjectGrid estarem disponíveis.

  Solução: Este erro pode ocorrer quando um servidor de contêiner tiver sido iniciado, mas o posicionamento ainda não foi iniciado. Execute as ações a seguir:

  – Examine a política de implementação para o ObjectGrid e verifique se o número de contêineres ativos é maior ou igual aos atributos numInitialContainers e minSyncReplicas no arquivo descritor da política de implementação.

  – Examine a configuração para a propriedade **placementDeferralInterval** no arquivo de propriedade de servidor do servidor de contêiner para ver quanto tempo precisa passar antes de as operações de posicionamento ocorrerem.

  – Se você usou o comando **xscmd -c suspendBalancing** para parar o balanceamento de shards para um conjunto de mapas e grade de dados específicos, use o comando **xscmd -c resumeBalancing** para iniciar novamente o balanceamento.

Conceitos relacionados:

Java "Criando Instâncias do ObjectGrid com a Interface ObjectGridManager" na página 351
Cada um desses métodos cria uma instância local de um ObjectGrid.

Resolvendo Problemas da Integração de Cache

Use estas informações para resolver problemas com a configuração de integração de seu cache, incluindo sessões HTTP e configurações de cache dinâmico.

Procedimento

- **Problema:** Os IDs da sessão de HTTP não estão sendo reutilizados.

  Causa: É possível reutilizar os IDs de sessão. Se você criar uma grade de dados para persistência de sessão na Versão 7.1.1 ou posterior, a reutilização do ID de sessão será automaticamente ativada. No entanto, se você criou configurações anteriores, esta configuração já poderá ser configurada com o valor incorreto.

  Solução: Consulte as seguintes configurações para verificar se a reutilização do ID de sessão de HTTP estáativada:

  – A propriedade `reuseSessionId` no arquivo `splicer.properties` deve ser configurada para `true`.

  – O valor da propriedade customizada `HttpSessionIdReuse` deve ser configurado para `true`. Essa propriedade customizada pode ser configurada em um dos seguintes caminhos no console administrativo do WebSphere Application Server:

    - **Servidores** > *server_name* > **Gerenciamento de Sessões** > **Propriedades customizadas**

- **Clusters Dinâmicos** > *dynamic_cluster_name* > **Modelo doServidor** > **Gerenciamento de Sessões** > **Propriedades Customizadas**
- **Servidores** > **Tipos de Servidor** > **Servidores de Aplicativos WebSphere** > *server_name* e, em seguida, em Infraestrutura do Servidor, clique em **Gerenciamento Java e processos** > **Definição de Processo** > **Java virtual machine** > **Propriedades Customizadas**
- **Servidores** > **Tipos de Servidor** > **Servidores de Aplicativos do WebSphere** > *server_name* > **Configurações do Contêiner da Web** > **Contêiner da Web**.

Se você atualizar quaisquer valores de propriedade customizada, reconfigure o gerenciamento de sessão eXtreme Scale para que o arquivo `splicer.properties` reconheça a mudança.

- **Problema:** Quando você estiver usando uma grade de dados para armazenar as sessões HTTP e o carregamento de transações for alto, uma mensagem CWOBJ0006W será exibida no arquivo `SystemOut.log`.

  ```
  CWOBJ0006W: Ocorreu uma exceção:
  com.ibm.websphere.objectgrid.ObjectGridRuntimeException:
  java.util.ConcurrentModificationException
  ```

  Esta mensagem ocorre apenas quando o parâmetro **`replicationInterval`** no arquivo `splicer.properties` é configurado com um valor maior que zero e o aplicativo da Web modifica um objeto List que foi configurado como um atributo na HTTPSession.

  Solução: Clone o atributo que contém o objeto List modificado e coloque o atributo clonado no objeto de sessão.

- 8.6+ **Problema:** Ao executar aplicativos da web com a especificação do Servlet 3.0, os filtros de aplicativos da web e listeners não são chamados pelo gerenciamento de sessões do WebSphere eXtreme Scale. Por exemplo, os listeners não são chamados de volta quando as sessões são invalidadas usando despejo do contêiner remoto com o WebSphere eXtreme Scale.

  Causa: WebSphere eXtreme Scale não identifica os filtros e listeners definidos utilizando anotações ou programaticamente.

  Solução: Filtros e listeners devem ser explicitamente declarados no arquivo web.xml do aplicativo da web.

Referências relacionadas:

Arquivos XML para Configuração do Gerenciador de Sessões HTTP
Quando você inicia um servidor de contêiner que armazena dados da sessão HTTP, é possível usar os arquivos XML padrão ou você pode especificar arquivos XML customizados. Estes arquivos criam nomes de ObjectGrid específicos, número de réplicas, etc.

Parâmetros de inicialização do contexto do servlet
A lista de parâmetros de inicialização de contexto de servlet a seguir pode ser especificada no arquivo splicer properties conforme requerido no método de conexão escolhido.

Arquivo `splicer.properties`
O arquivo `splicer.properties` contém todas as opções de configuração para configurar um gerenciador de sessões baseado em filtro de servlet.

Resolução de Problemas do Plug-in do Cache JPA

Java

Use estas informações para resolver problemas com sua configuração de plug-in do cache JPA. Estes problemas podem ocorrer em ambas as configurações Hibernate e OpenJPA.

Procedimento

- **Problema:** A exceção a seguir é exibida: `CacheException: Falha ao obter o servidor ObjectGrid`.

  Com um valor de atributo **`ObjectGridType`** de `EMBEDDED` ou `EMBEDDED_PARTITION`, o cache eXtreme Scale tenta obter uma instância do servidor a partir do tempo de execução. Em um ambiente Java Platform, Standard Edition, um servidor eXtreme Scale com serviço de catálogo integrado é iniciado. O serviço de catálogo integrado tentará atender na porta 2809. Se essa porta estiver sendo usada por outro processo, ocorrerá um erro.

  Solução: Se terminais de serviço de catálogo externo forem especificados, por exemplo, com o arquivo `objectGridServer.properties`, este erro ocorrerá se o nome do host ou a porta for especificada incorretamente. Corrija o conflito de porta.

- **Problema:** A exceção a seguir é exibida: `CacheException: Falha ao obter o REMOTE ObjectGrid para o REMOTE ObjectGrid configurado. objectGridName = [ObjectGridName], Nome da PU = [persistenceUnitName]`

  Esse erro ocorre porque o cache não pode obter a instância do ObjectGrid a partir dos terminais de serviço de catálogo fornecidos.

  Solução: Esse problema geralmente ocorre devido a um nome de host ou porta incorreto.

- **Problema:** A exceção a seguir é exibida: `CacheException: Não é possível ter duas PUs [persistenceUnitName_1, persistenceUnitName_2] configuradas com o mesmo ObjectGridName [ObjectGridName] do EMBEDDED ObjectGridType`

  Essa exceção ocorrerá se você tiver muitas unidades de persistência configuradas e os caches do eXtreme Scale destas unidades forem configurados com o mesmo nome de ObjectGrid e valor de atributo `EMBEDDED` do **`ObjectGridType`**. Estas configurações de unidade de persistência podem estar no mesmo arquivo `persistence.xml` ou diferente.

  Solução: É necessário verificar se o nome do ObjectGrid é exclusivo para cada unidade de persistência quando o valor do atributo **`ObjectGridType`** for `EMBEDDED`.

- **Problema:** A exceção a seguir é exibida: `CacheException: O REMOTE ObjectGrid [ObjectGridName] não inclui os BackingMaps [mapName_1, mapName_2,...] necessários`

  Com um tipo de ObjectGrid REMOTE, se o ObjectGrid do lado do cliente obtido não tiver os mapas de apoio de entidade completos para suportar o cache da unidade de persistência, esta exceção ocorrerá. Por exemplo, cinco classes de entidade são listadas na configuração da unidade de persistência, mas o ObjectGrid obtido possui apenas dois BackingMaps. Embora o ObjectGrid obtido possa ter 10 BackingMaps, se algum destes cinco BackingMaps de entidade necessários não for localizado nos dez BackingMaps, esta exceção ainda ocorrerá.

  Solução: Certifique-se de que a configuração do mapa de apoio suporte o cache da unidade de persistência.

Resolução de Problemas do IBM eXtremeMemory

Use as informações a seguir para resolução de problemas do eXtremeMemory.

Procedimento

Problema: Se o recurso compartilhado, libstdc++.so.5, não estiver instalado, então quando você iniciar o servidor de contêiner, as biblioteca nativas do IBM eXtremeMemory não serão carregadas.

Linux **Sintoma:** Em um sistema operacional Linux de 64 bit, se tentar iniciar um servidor de contêiner com a propriedade do servidor enableXM configurada como `true` e o recurso compartilhado `libstdc++.so.5` não estiver instalado, você receberá um erro semelhante ao exemplo a seguir:

```
00000000 Initialization W CWOBJ0006W: An exception occurred: java.lang.reflect.InvocationTargetException
 at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
 at sun.reflect.NativeConstructorAccessorImpl.newInstance(NativeConstructorAccessorImpl.java:56)
 at sun.reflect.DelegatingConstructorAccessorImpl.newInstance(DelegatingConstructorAccessorImpl.java:39)
 at java.lang.reflect.Constructor.newInstance(Constructor.java:527)
 at com.ibm.websphere.objectgrid.server.ServerFactory.initialize(ServerFactory.java:350)
 at com.ibm.websphere.objectgrid.server.ServerFactory$2.run(ServerFactory.java:303)
 at java.security.AccessController.doPrivileged(AccessController.java:202)
 at com.ibm.websphere.objectgrid.server.ServerFactory.getInstance(ServerFactory.java:301)
 at com.ibm.ws.objectgrid.InitializationService.main(InitializationService.java:302)

Caused by: com.ibm.websphere.objectgrid.ObjectGridRuntimeException: java.lang.UnsatisfiedLinkError:
 OffheapMapdbg (Not found in java.library.path)
 at com.ibm.ws.objectgrid.ServerImpl.<init&gt;(ServerImpl.java:1033)
... 9 more Caused by: java.lang.UnsatisfiedLinkError: OffheapMapdbg (Not found in java.library.path)
 at java.lang.ClassLoader.loadLibraryWithPath(ClassLoader.java:1011)
 at java.lang.ClassLoader.loadLibraryWithClassLoader(ClassLoader.java:975)
 at java.lang.System.loadLibrary(System.java:469)
 at com.ibm.ws.objectgrid.io.offheap.ObjectGridHashTableOH.initializeNative(ObjectGridHashTableOH.java:112)
 at com.ibm.ws.objectgrid.io.offheap.ObjectGridHashTableOH.<clinit&gt;(ObjectGridHashTableOH.java:87)
 at java.lang.J9VMInternals.initializeImpl(Native Method)
 at java.lang.J9VMInternals.initialize(J9VMInternals.java:200)
 at com.ibm.ws.objectgrid.ServerImpl.<init&gt;(ServerImpl.java:1028)
... 9 more
```

Causa: O recurso compartilhado `libstdc++.so.5` não foi instalado.
Diagnosticando o problema: Para verificar se o `libstdc++.so.5` está instalado, emita o comando a seguir a partir do diretório ObjectGrid/native da sua instalação:

```
ldd libOffheapMap.so
```

Se você não tiver a biblioteca compartilhada instalada, receberá o erro a seguir:

```
ldd libOffheapMap.so
libstdc++.so.5 => not found
```

Resolvendo o problema: Use o instalador do pacote da sua distribuição Linux de 64 bits para instalar o arquivo de recursos necessário. O pacote pode estar listado como `compat-libstdc++-33.x86_64` ou `libstdc++5`. Depois de instalar o recurso necessário, verifique se o pacote `libstdc++5` está instalado emitindo o comando a seguir a partir do diretório ObjectGrid de sua instalação:

```
ldd libOffheapMap.so
```

Resolução de Problemas de Administração

Use as informações a seguir para solucionar problemas de administração, incluindo iniciar e parar servidores, usar o utilitário **xscmd** e assim por diante.

Procedimento

- **Problema:** Scripts de administração estão ausentes do diretório *profile_root*`/bin` de uma instalação do WebSphere Application Server.

  Causa: Quando você atualiza a instalação, novos arquivos de script não são instalados automaticamente nos perfis.

  Solução: Se você deseja executar um script a partir de seu diretório *profile_root*`/bin`, cancele o aumento e aumente novamente o perfil com a

liberação mais recente. Para obter mais informações, consulte Cancelando o Aumento de um Perfil Usando o Prompt de Comandos e Criando e Alterando Perfis para o WebSphere eXtreme Scale.

- **Problema:** Quando você está executando um comando **xscmd**, a mensagem a seguir é impressa na tela:

```
java.lang.IllegalStateException: Placement service MBean not available.
[]
        at
com.ibm.websphere.samples.objectgrid.admin.OGAdmin.main(OGAdmin.java:1449)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at
sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:60)
        at
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:37)
        at java.lang.reflect.Method.invoke(Method.java:611)
        at com.ibm.ws.bootstrap.WSLauncher.main(WSLauncher.java:267)
Ending at: 2011-11-10 18:13:00.000000484
```

  Causa: Ocorreu um problema de conexão com o servidor de catálogos.

  Solução: Verifique se seus servidores de catálogos estão em execução e estão disponíveis pela rede. Esta mensagem também pode ocorrer quando você possui um domínio de serviço de catálogo definido, mas menos de dois servidores de catálogos estão em execução. O ambiente não está disponível até dois servidores de catálogo serem iniciados.

- **Problema:** Quando você está executando um comando **xscmd**, a mensagem a seguir é impressa na tela:

```
CWXSI0066E: O argumento argument_name incompatível foi detectado.
```

  Causa: Você inseriu um formato de comando que o utilitário **xscmd** não reconheceu.

  Solução: Verifique o formato do comando. É possível encontrar esse comando ao executar expressões regulares com o comando **-c findbyKey**. Para obter informações adicionais, consulte Consultando , Exibindo e Invalidando Dados.

- 8.6+ **Problema:** Todos os comandos start, stop e **xscmd** falham com um erro java.lang.UnsupportedClassVersionError.

  Por exemplo, você poderá ver um dos seguintes erros quando estiver utilizando os comandos de utilitário start, stop ou**xscmd**:

```
A classe Java não pôde ser carregada. java.lang.UnsupportedClassVersionError:
(com/ibm/ws/xs/admin/wxscli/WXSAdminCLI) bad major version at offset=6
```

```
A classe Java não pôde ser carregada. java.lang.UnsupportedClassVersionError:
(com/ibm/ws/objectgrid/server/impl/ProcessLauncher) bad major version at offset=6
```

  Causa: Os comandos estão em execução com uma versão Java não suportada para o WebSphere eXtreme Scale.

  Solução: Atualize a variável de ambiente *JAVA_HOME* para apontar para uma instalação de Java Development Kit (JDK) suportada. Para obter versões de JDK suportadas e instruções sobre como atualizar o JDK, consulte “Considerações sobre o Java SE” na página 310.

Conceitos relacionados:

Exemplo: Configurando os Domínios de Serviço de Catálogo
Quando estiver usando o serviço de catálogo, no mínimo dois servidores de catálogos são necessários para evitar um ponto de falha único. Dependendo do número de nós em seu ambiente, é possível criar configurações diferentes para assegurar que pelo menos dois servidores de catálogos estejam sempre em execução.

Administrando

Resolução de Problemas de Monitoramento de Dados

Utilize estas informações para resolver problemas das atividades de monitoramento que você conclui com o console da web do WebSphere eXtreme Scale ou outros utilitários para monitorar o desempenho do seu ambiente de aplicativo.

Procedimento

Problema: Não é possível alternar entre os domínios com diferentes configurações de segurança no console da web do WebSphere eXtreme Scale.
É possível alternar domínios entre dois domínios não seguros. Também é possível alternar domínios entre dois domínios seguros com a mesma segurança configurada. No entanto, você não pode alternar entre um domínio não seguro e um domínio seguro ou entre dois domínios seguros com configurações de segurança diferentes.
Diagnóstico: O comando **`startOgServer`** é usado para iniciar dois servidores de catálogos diferentes em domínios separados. Cada servidor de catálogo não está ciente do outro. No entanto, ambos os servidores de catálogo são iniciados com o mesmo nome de domínio. Quando você não especifica o nome de domínio, ambos os servidores de catálogos iniciam em diferentes domínios com o nome padrão, DefaultDomain. Além disso, o console de monitoramento exibe dados apenas para um dos domínios do servidor de catálogos.
Causa: Quando você alterna domínios no console de monitoramento, você é conectado ao segundo domínio. No entanto, nenhuma grade de dados desse domínio é exibida e os dados da grade do primeiro domínio ainda estão na visualização. Portanto, durante o tempo de execução, ambos os servidores de catálogo são executados em domínios separados com o nome DefaultDomain.
Solução: Determine quais nomes de domínio são utilizados quando os servidores de catálogo iniciam nos dois domínios. Para identificar os nomes de domínio, analise sua sintaxe de comando **`startOgServer`** e investigue qual domínio está sendo especificado.
Como esse cenário problema não é suportado, conclua as seguintes ações para exibir as estatísticas de domínio do serviço de catálogo correto:

1. Encerre os servidores de catálogos e verifique se eles estão configurados para iniciar com nomes de domínio exclusivos.
2. Reinicie o console do monitor.
3. Opcional: Se uma interrupção não for possível, considere a execução de um segundo console de monitoramento para monitorar o segundo domínio.

Resolução de Problemas de Várias Configurações do Datacenter

Use estas informações para resolver problemas de diversas configurações do datacenter,incluindo vinculação entre domínios do serviço de catálogo.

Antes de Iniciar

Você deve utilizar o utilitário **xscmd** para resolver problemas de suas configurações com múltiplos datacenters. Para obter informações adicionais, consulte Administrando com o Utilitário **xscmd**.

Procedimento

- 8.6+ **Problema:** É necessário determinar se a replicação de dados é sincronizada entre os servidores de contêiner e domínios de serviço de catálogo.

  Solução: Execute o comando **xscmd -c showReplicationState** ou **xscmd.sh -c showDomainReplicationState**. Esses comandos exibem informações sobre o status de replicação no ambiente. Para obter informações adicionais, consulte Monitorando com o Utilitário **xscmd**.

- 8.6+ **Problema:** É necessário verificar quais domínios de serviço de catálogo são vinculados ao seu domínio de serviço de catálogo local.

  Solução: Execute o comando **xscmd -c showLinkedDomains**. Este comando lista os domínios de serviço de catálogo externos que estão vinculados ao domínio de serviço de catálogo local.

- 8.6+ **Problema:** Você deseja detectar qualquer problema de configuração com links do shard primário para os domínios de serviço de catálogo, sem passar por toda a saída do comando **xscmd -c showLinkedPrimaries**.

  Solução: Use a opção **xscmd -hc** ou **xscmd --linkHealthCheck**. O comando verifica se os shards primários possuem o número apropriado de links de domínio de serviço de catálogo. O comando lista quaisquer shards primários que possuem o número errado de links. Se eles estão todos vinculados corretamente (por exemplo, seu domínio está vinculado a 1 outro domínio, espera-se que todos os shards primários individuais tenham 1 link), você obterá uma mensagem informando que eles são vinculados:

```
CWXSI0092I: Todos os shards primários para a
grade de dados {0} e o conjunto de mapas {1} possuem o número correto de links
para shards primários estrangeiros.
```

  Se você descobrir problemas, tente algumas das seguintes soluções possíveis:

  – Revise suas configurações de rede e do firewall para assegurar que os servidores que estão hospedando servidores de contêiner nos domínios possam se comunicar entre si.
  – Revise os logs SystemOut e FFDC para os shards primários com os links incorretos para obter mensagens de erro mais específicas.
  – Descarte e restabeleça o link entre os domínios.

- **Problema:** Os dados estão ausentes em um ou mais domínios do serviço de catálogo. Por exemplo, você pode executar o comando **xscmd -c establishLink**. Quando você examina os dados para cada domínio do serviço de catálogo vinculado, os dados têm uma outra aparência, por exemplo, a partir do comando **xscmd -c showMapSizes**.

  Solução: É possível solucionar esse problema com o comando **xscmd -c showLinkedPrimaries**. Esse comando imprime cada shard primário, incluindo quais primários estrangeiros são vinculados.

  No cenário descrito, é possível descobrir, a partir da execução do comando **xscmd -c showLinkedPrimaries**, que os shards primários do primeiro domínio do serviço de catálogo são vinculados aos shards primários do segundo domínio de serviço de catálogo, porém o segundo domínio de serviço de catálogo não possui links para o primeiro domínio de serviço de catálogo. Você pode

considerar executar novamente o comando **xscmd -c establishLink** a partir do segundo domínio de serviço de catálogo para o primeiro domínio de serviço de catálogo.

Resolução de Problemas de Carregadores

Java

Use estas informações para resolver problemas com os carregadores de banco de dados.

Procedimento

- **Problema:** O carregador é incapaz de se comunicar com o banco de dados. Ocorreu uma exceção LoaderNotAvailableException.

  Explicação: O plug-in do carregador pode falhar quando não consegue se comunicar com o back end do banco de dados. Essa falha pode acontecer se o servidor de banco de dados ou a conexão de rede estiver inativa. O carregador write-behind enfileira as atualizações e tenta executar o push das mudanças de dados para o carregador periodicamente. O utilitário de carga deve notificar o tempo de execução do ObjectGrid que há um problema de conectividade do banco de dados lançando uma exceção LoaderNotAvailableException.

  Solução: A implementação do carregador deve ser capaz de distinguir uma falha de dados ou uma falha do carregador físico. A falha de dados deve ser lançada ou relançada como um LoaderException ou um OptimisticCollisionException, mas uma falha do carregador físico deve ser lançada ou relançada como um LoaderNotAvailableException. O ObjectGrid manipula estas exceções de maneira diferente:

  – Se uma LoaderException for capturada pelo carregador write-behind, este carregador considerará a exceção como falha, tal como uma falha de chave duplicada. O carregador write-behind removerá a atualização do lote e tentará atualizar um registro em um momento para isolar a falha de dados. Se uma {{LoaderException}} for capturada durante uma atualização de registro, um registro de atualização falho é criado e registrado no mapa de atualização falho.

  – Se uma LoaderNotAvailableException for capturada pelo carregador write-behind, este carregador a considerará falha porque não pode se conectar com o final do banco de dados, por exemplo, porque o backend do banco de dados está inativo, uma conexão com o banco de dados não está disponível ou a rede está inativa. O carregador write-behind espera 15 segundos e tenta novamente executar a atualização de lote no banco de dados.

  O erro comum é lançar uma LoaderException enquanto uma LoaderNotAvailableException deve ser lançada. Todos os registros enfileirados no carregador write-behind se tornarão atualizações de registro falhas, o que anula o propósito do isolamento de falha do backend.

- **Problema:** Quando estiver usando um carregador OpenJPA com DB2 no WebSphere Application Server, uma exceção de cursor fechado ocorre.

  A exceção a seguir é do DB2 no arquivo de log org.apache.openjpa.persistence.PersistenceException:

  ```
  [jcc][t4][10120][10898][3.57.82] Invalid operation: result set is closed.
  ```

  Solução: Por padrão, o servidor de aplicativos configura a propriedade customizada resultSetHoldability com um valor de 2 (CLOSE_CURSORS_AT_COMMIT). Esta propriedade faz com o DB2 feche seu

resultSet/cursor nos limites da transação. Para remover a exceção, altere o valor da propriedade customizada para 1 (HOLD_CURSORS_OVER_COMMIT). Configure a propriedade customizada resultSetHoldability no seguinte caminho na célula do WebSphere Application Server: **Recursos** > **Provedor JDBC** > **Provedor Driver Universal JDBC** > **DataSources** > *data_source_name* > **Propriedades Customizadas** > **Novo**.

- **Problema** O DB2 exibe uma exceção: `A transação atual foi retrocedida devido a um conflito ou tempo limite. Código de razão "2".. SQLCODE=-911, SQLSTATE=40001, DRIVER=3.50.152`

  Essa exceção ocorre devido a um problema de contenção de bloqueio quando estiver executando com o OpenJPA com DB2 no WebSphere Application Server. O nível de isolamento padrão para a Leitura Repetida (RR) do WebSphere Application Server, que obtém bloqueios de longa duração com o DB2.**Solução:**

  Configure o nível de isolamento para Leitura Confirmada para reduzir a contenção de bloqueio. Configure a propriedade customizada da origem de dados webSphereDefaultIsolationLevel para configurar o nível de isolamento para 2(TRANSACTION_READ_COMMITTED) no seguinte caminho na célula WebSphere Application Server: **Recursos** > **Provedor JDBC** > *JDBC_provider* > **Origens de Dados** > *data_source_name* > **Propriedades Customizadas** > **Novo**. Para obter informações adicionais sobre a propriedade customizada webSphereDefaultIsolationLevel e níveis de isolamento de transação, consulte Requisitos para Configurar os Níveis de Isolamento de Acesso a Dados.

- **Problema:** Quando estiver usando a função de pré-carregamento do JPALoader ou JPAEntityLoader, a seguinte mensagem CWOBJ1511 não é exibida para a partição em um servidor de contêiner: `CWOBJ1511I: GRID_NAME:MAPSET_NAME:PARTITION_ID (primário) está aberto para negócios.`

  Em vez disso, ocorrerá uma exceção TargetNotAvailableException no servidor de contêiner, que ativa a partição que é especificada pela propriedade preloadPartition.

  Solução: Configure o atributo preloadMode para `true` se você utilizar um JPALoader ou JPAEntityLoader para pré-carregar dados no mapa. Se a propriedade preloadPartition da JPALoader ou JPAEntityLoader estiver configurada para um valor entre `0` e `total_number_of_partitions-1`, então o JPALoader e o JPAEntityLoader tentarão pré-carregar os dados a partir do banco de dados backend no mapa. O trecho de código a seguir ilustra como o atributo preloadMode é configurado para ativar o pré-carregamento assíncrono:

  ```
  BackingMap bm = og.defineMap( "map1" );
  bm.setPreloadMode( true );
  ```

  Também é possível configurar o atributo preloadMode usando um arquivo XML conforme ilustrado no seguinte exemplo:

  ```
   <backingMap name="map1" preloadMode="true" pluginCollectionRef="map1"
  " lockStrategy="OPTIMISTIC" />
  ```

Conceitos relacionados:

"Programação para Integração de JPA" na página 658
O Java Persistence API (JPA) é uma especificação que permite o mapeamento de objetos Java para bancos de dados relacionais. O JPA contém uma especificação completa de object-relational mapping (ORM) usando anotações de metadados da linguagem Java, descritores XML, ou ambos para definir o mapeamento entre objetos Java e um banco de dados relacional. Inúmeras implementações comerciais e de software livre estão disponíveis.

Configurando a Integração de Cache
O WebSphere eXtreme Scale pode integrar-se com outros produtos relacionados ao armazenamento em cache. Também é possível usar o provedor de cache dinâmico do WebSphere eXtreme Scale para plugar o WebSphere eXtreme Scale no componente de cache dinâmico no WebSphere Application Server. Outra extensão para o WebSphere Application Server é o gerenciador de sessões HTTP do WebSphere eXtreme Scale, que pode ajudar a armazenar em cache as sessões HTTP.

Resolução de Problemas de Configuração XML

Quando você configura o eXtreme Scale, é possível encontrar um comportamento inesperado com seus arquivos XML. As seções a seguir descrevem problemas que podem ocorrer e soluções.

Procedimento

- **Problema:** A política de implementação e os arquivos XML do ObjectGrid devem corresponder.

  A política de implementação e os arquivos XML de ObjectGrid devem corresponder. Se eles não possuem nomes de ObjectGrid e nomes de mapas correspondentes, ocorrem erros.

  Se a lista de backingMap em um arquivo XML de ObjectGrid não corresponder à lista de referências de mapas em um arquivo XML da política de implementação, ocorre um erro no servidor de catálogos.

  Por exemplo, o seguinte arquivo XML de ObjectGrid e arquivo XML da política de implementação são utilizados para iniciar um processo de contêiner. O arquivo da política de implementação possui mais referências de mapas que são listados no arquivo XML de ObjectGrid.

  ObjectGrid.xml - exemplo incorreto

```
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="accounting">
            <backingMap name="payroll" readOnly="false" />
        </objectGrid>
    </objectGrids>
</objectGridConfig>
```

  deploymentPolicy.xml - exemplo incorreto

```
<?xml version="1.0" encoding="UTF-8"?>
<deploymentPolicy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/deploymentPolicy ../deploymentPolicy.xsd"
 xmlns="http://ibm.com/ws/objectgrid/deploymentPolicy">
    <objectgridDeployment objectgridName="accounting">
        <mapSet name="mapSet1" numberOfPartitions="4" minSyncReplicas="1"
maxSyncReplicas="1" >"2" maxAsyncReplicas="1">
            <map ref="payroll"/>
            <map ref="ledger"/>
        </mapSet>
    </objectgridDeployment>
</deploymentPolicy>
```

Mensagens: Uma mensagem de erro ocorrerá no arquivo `SystemOut.log` quando a política de implementação for incompatível com o arquivo XML do ObjectGrid. Para o exemplo precedente, ocorre a seguinte mensagem:

```
CWOBJ3179E: A referência do ledger do mapa no mapSet mapSet1 do arquivo do descritor de implementação
de contabilidade do ObjectGrid
não faz referência a um mapa de retorno válido do XML do ObjectGrid
.
```

Se a política de implementação estiver sem referências de mapa para os backingMaps listados no arquivo XML do ObjectGrid, ocorrerá uma mensagem de erro no arquivo `SystemOut.log`. Por exemplo:

```
CWOBJ3178E: O ledger do mapa na contabilidade do ObjectGrid referido no XML do ObjectGrid
não foi localizado no arquivo do descritor de implementação.
```

Solução: Determine qual arquivo tem a lista correta e altere o código relevante de acordo.

- **Problema:** Nomes do ObjectGrid incorretos entre arquivos XML também causam um erro.

  O nome do ObjectGrid é referido no arquivo XML ObjectGrid e no arquivo XML da política de implementação.

  Mensagem: Uma ObjectGridException ocorre causada pela exceção de IncompatibleDeploymentPolicyException. A seguir, está um exemplo.

  Causado por:
  com.ibm.websphere.objectgrid.IncompatibleDeploymentPolicyException: O objectgridDeployment com "accountin" de objectGridName não possui um objectGrid correspondente no XML do ObjectGrid.

  O arquivo XML ObjectGrid é a lista principal dos nomes ObjectGrid. Ocorrerá um erro se uma política de implementação possuir um nome ObjectGrid que não está contido no arquivo XML ObjectGrid.

  Solução: Verifique detalhes, como a ortografia do nome do ObjectGrid. Remova quaisquer nomes extras ou inclua nomes ObjectGrid ausentes nos arquivos XML ObjectGrid ou da política de implementação. Na mensagem de exemplo, o objectGridName está escrito incorretamente como "accountin" em vez de "accounting".

- **Problema:** Alguns dos atributos no arquivo XML podem receber apenas alguns valores. Estes atributos possuem valores aceitáveis enumerados pelo esquema. A lista a seguir fornece alguns dos atributos:
  - atributo authorizationMechanism no elemento objectGrid
  - atributo copyMode no elemento backingMap
  - atributo lockStrategy no elemento backingMap
  - atributo ttlEvictorType no elemento backingMap
  - atributo type no elemento property
  - initialState no elemento objectGrid
  - evictionTriggers no elemento backingMap

  Se a um destes atributos for designado um valor inválido, a validação XML falhará. No arquivo XML de exemplo a seguir, é utilizado um valor incorreto de INVALID_COPY_MODE:

```
exemplo de INVALID_COPY_MODE
<?xml version="1.0" encoding="UTF-8"?>
<objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
 xmlns="http://ibm.com/ws/objectgrid/config">
    <objectGrids>
        <objectGrid name="accounting">
            <backingMap name="payroll" copyMode="INVALID_COPY_MODE"/>
        <objectGrid/>
   </objectGrids>
</objectGridConfig>
```

A mensagem a seguir aparece no log.

```
CWOBJ2403E: O arquivo XML é inválido. Foi detectado um problema com < null > na linha 5. A mensagem de erro
é cvc-enumeration-valid: O valor 'INVALID_COPY_MODE' não possui uma faceta válida com relação à enumeração'
[COPY_ON_READ_AND_COMMIT, COPY_ON_READ, COPY_ON_WRITE, NO_COPY,COPY_TO_BYTES]'.
Ela deve ser um valor a partir da enumeração.
```

- **Problema:** Atributos ou tags ausentes ou incorretos em um arquivo XML causa erros, como o seguinte exemplo em que, no arquivo XML do ObjectGrid, falta a tag final < /objectGrid >:

  atributos ausentes - XML de exemplo

  ```
  <?xml version="1.0" encoding="UTF-8"?>
  <objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
   xmlns="http://ibm.com/ws/objectgrid/config">
      <objectGrids>
          <objectGrid name="accounting">
              <backingMap name="payroll" />

     </objectGrids>
  </objectGridConfig>
  ```

  Mensagem:

  ```
  CWOBJ2403E: O arquivo XML é inválido. Foi detectado um
  problema com < null > na linha 7. A mensagem de erro
   é: The
  end-tag for element type "objectGrid" must end with a '>' delimiter.
  ```

  Ocorre uma ObjectGridException sobre o arquivo XMl inválido com o nome do arquivo XML.

  Solução: Certifique-se de que as tags e os atributos necessários apareçam nos arquivos XML com o formato correto.

- **Problema:** Se um arquivo XML estiver formatado com sintaxe incorreta ou ausente, o CWOBJ2403E aparecerá no log. Por exemplo, a mensagem a seguir é exibida quando uma aspa está ausente em um dos atributos XML

  ```
  CWOBJ2403E: O arquivo XML é inválido. Foi detectado
  um problema com < null > na linha 7. A mensagem de erro
   é:
  Open quote is expected for attribute "maxSyncReplicas"
  associated with an element type "mapSet".
  ```

  Uma ObjectGridException sobre o arquivo XML inválido também ocorre.

  Solução: Várias soluções podem ser usadas para um determinado erro de sintaxe XML. Consulte a documentação relevante sobre a gravação de script XML.

- **Problema:** Referência a uma coleção de plug-in inexistente torna um arquivo XML inválido. Por exemplo, ao usar o XML para definir um plug-ins BackingMap, o atributo pluginCollectionRef do elemento backingMap deve referenciar um backingMapPluginCollection. O atributo pluginCollectionRef deve corresponder aos elementos backingMapPluginCollection.

  Mensagem:

  Se o atributo pluginCollectionRef não corresponder a nenhum dos atributos de ID de algum dos elementos backingMapPluginConfiguration, uma mensagem semelhante à seguinte será exibida no log.

  ```
  [7/14/05 14:02:01:971 CDT] 686c060e XmlErrorHandl E CWOBJ9002E:
  This is an English only Error message: Invalid XML file. Line: 14; URI: null;
  Message: Key 'pluginCollectionRef' with
  value 'bookPlugins' not found for identity constraint of element 'objectGridConfig'.
  ```

  O arquivo XML a seguir é utilizado para produzir o erro. Observe que o nome do BackingMap book possui seu atributo pluginCollectionRef configurado como bookPlugins e o backingMapPluginCollection único possui um ID de collection1.

  Referenciando um XML de atributo não-existente - exemplo

  ```
  <?xml version="1.0" encoding="UTF-8"?>
  <objectGridConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://ibm.com/ws/objectgrid/config ../objectGrid.xsd"
  ```

```
 xmlns="http://ibm.com/ws/objectgrid/config">
   <objectGrids>
      <objectGrid name="bookstore">
        <backingMap name="book" pluginCollectionRef="bookPlugin" />
      </objectGrid>
   </objectGrids>
   <backingMapPluginCollections>
    <backingMapPluginCollection id="collection1">
     <bean id="Evictor"
       className="com.ibm.websphere.objectgrid.plugins.builtins.LRUEvictor" />
     </backingMapPluginCollection>
    </backingMapPluginCollections>
</objectGridConfig>
```

Solução:

Para corrigir o problema, certifique-se de que o valor de cada pluginCollectionRef corresponda ao ID de um dos elementos backingMapPluginCollection. Simplesmente altere o nome de pluginCollectionRef para collection1 para não receber este erro. Outras maneiras de corrigir o problema incluem a alteração do ID do backingMapPluginCollection existente para corresponder ao pluginCollectionRef ou a inclusão de um backingMapPluginCollection adicional com um ID que corresponda ao pluginCollectionRef.

- **Problema:** O IBM Software Development Kit (SDK) Versão 5 contém uma implementação de alguma função de Java API for XML Processing (JAXP) a ser usada para validação de XML com relação a um esquema. Ao utilizar um SDK que não contém esta implementação, as tentativas de validação poderão falhar.

  Ao tentar validar o XML com um SDK que não possui a implementação necessária, o log contém o seguinte erro:

```
A validação XML de XmlConfigBuild está ativada
SystemErr R com.ibm.websphere.objectgrid
SystemErr R at
com.ibm.ws.objectgrid.ObjectGridManagerImpl.getObjectGridConfigurations
 (ObjectGridManagerImpl.java:182)
SystemErr R at com.ibm.ws.objectgrid.ObjectGridManagerImpl.createObjectGrid(ObjectGridManagerImpl.java:309)
SystemErr R at com.ibm.ws.objectgrid.test.config.DocTest.main(DocTest.java:128)
SystemErr R Caused by: java.lang.IllegalArgumentException: No attributes are implemented
SystemErr R at org.apache.crimson.jaxp.DocumentBuilderFactoryImpl.setAttribute(DocumentBuilderFactoryImpl.java:93)
SystemErr R at com.ibm.ws.objectgrid.config.XmlConfigBuilder.<init>XmlConfigBuilder.java:133)
SystemErr R at com.ibm.websphere.objectgrid.ProcessConfigXML$2.runProcessConfigXML.java:99)...
```

  O SDK utilizado não contém uma implementação da função JAXP necessária para validar arquivos XML em um esquema.

  Solução: Se você desejar validar o XML usando um SDK que não contém a implementação JAXP, faça download do Apache Xerces e inclua seus arquivos Java archive (JAR) no caminho de classe. Para evitar este problema, depois de efetuar download do Xerces e incluir os arquivos JAR no caminho de classe,é possível validar o arquivo XML com êxito.

Resolvendo Problemas de Conflitos

As seções a seguir descrevem alguns dos cenários de conflitos mais comuns e sugestões sobre como evitá-los.

Antes de Iniciar

Implemente a manipulação de exceção no seu aplicativo. Consulte o "Implementando Manipulação de Exceção em Cenários de Bloqueio" na página 499 para obter informações adicionais.

A seguinte exceção é exibida como resultado:

`com.ibm.websphere.objectgrid.plugins.LockDeadlockException: Message`

Essa mensagem representa a cadeia que é transmitida como um parâmetro quando a exceção é criada e emitida.

Procedimento

- **Problema:** Exceção LockTimeoutException.

  Descrição: Quando uma transação ou cliente solicita que um bloqueio seja concedido para uma entrada de mapa específica, a solicitação sempre aguarda o cliente atual liberar o bloqueio antes que a solicitação seja enviada. Se a solicitação de bloqueio permanecer inativa por um longo período de tempo, e o bloqueio nunca for concedido, a exceção LockTimeoutException será criada para evitar um conflito, que é descrito com mais detalhes na seção a seguir. É mais provável que esta exceção seja exibida quando usar uma estratégia de bloqueio pessimista porque o bloqueio nunca é liberado antes que transação seja confirmada.

  Recuperar mais detalhes:

  A exceção LockTimeoutException contém o método getLockRequestQueueDetails, que retorna uma sequência. Este método pode ser usado para ver uma descrição detalhada da situação que aciona a exceção. A seguir há um exemplo de código que captura a exceção e exibe uma mensagem de erro.

```
try {
    ...
}
catch (LockTimeoutException lte) {
    System.out.println(lte.getLockRequestQueueDetails());
}
```

  O resultado da saída é:

```
lock request queue
->[TX:163C269E-0105-4000-E0D7-5B3B090A571D, state =
    Granted 5348 milli-seconds ago, mode = U]
->[TX:163C2734-0105-4000-E024-5B3B090A571D, state =
    Waiting for 5348 milli-seconds, mode = U]
->[TX:163C328C-0105-4000-E114-5B3B090A571D, state =
    Waiting for 1402 milli-seconds, mode = U]
```

  Se você receber a exceção em um bloco de captura uma exceção ObjectGridException, o código a seguir determinará a exceção e exibe os detalhes da fila. O método do utilitário findRootCause também é usado.

```
try {
...
}
catch (ObjectGridException oe) {
    Throwable Root = findRootCause( oe );
    if (Root instanceof LockTimeoutException) {
        LockTimeoutException lte = (LockTimeoutException)Root;
        System.out.println(lte.getLockRequestQueueDetails());
    }
}
```

  Solução: Uma uma exceção LockTimeoutException evita possíveis conflitos em seu aplicativo. Uma exceção desse tipo resulta quando a exceção aguarda uma quantidade de tempo configurada. É possível configurar a quantidade de tempo que a exceção aguarda usando o método setLockTimeout(int), que está disponível para o BackingMap. Se um conflito não existir realmente no aplicativo, ajuste o tempo limite de bloqueio para evitar a LockTimeoutException.

  O código a seguir mostra como criar um objeto ObjectGrid, definir um mapa e configurar seu valor LockTimeout para 30 segundos:

```
ObjectGrid objGrid = new ObjectGrid();
BackingMap bMap = objGrid.defineMap("MapName");
bMap.setLockTimeout(30);
```

Use o exemplo codificado permanentemente para configurar as propriedades do ObjectGrid e do mapa. Se você criar o ObjectGrid a partir de um arquivo XML, configure o atributo **LockTimeout** dentro do elemento backingMap. A seguir há um exemplo de um elemento backingMap que configura um valor LockTimeout do mapa para 30 segundos.

```
<backingMap name="MapName" lockStrategy="PESSIMISTIC" lockTimeout="30">
```

- **Problema:** Conflitos de chave única.

  Descrição: Os seguintes cenários descrevem como podem ocorrer conflitos quando uma única chave é acessada utilizando um bloqueio S e posteriormente atualizada. Quando isto acontece em duas transações simultaneamente, o resultado é um conflito.

Tabela 33. Cenário de conflitos de uma única chave

	Encadeamento 1	**Encadeamento 2**	
1	session.begin()	session.begin()	Cada encadeamento estabelece uma transação independente.
2	map.get(key1)	map.get(key1)	O bloqueio S é concedido a ambas as transações para key1.
3	map.update(Key1,v)		Nenhum bloqueio U. A atualização é executada no cache transacional.
4		map.update(key1,v)	Nenhum bloqueio U. A atualização é executada no cache transacional
5	session.commit()		Bloqueado: O bloqueio S para key1 não pode ser atualizado para um bloqueio X porque o Encadeamento 2 possui um bloqueio S.
6		session.commit()	Conflito: O bloqueio S para key1 não pode ser atualizado para um bloqueio X porque T1 possui um bloqueio S.

Tabela 34. Conflitos de uma única chave, continuação

	Encadeamento 1	**Encadeamento 2**	
1	session.begin()	session.begin()	Cada encadeamento estabelece uma transação independente.
2	map.get(key1)		Bloqueio S concedido para key1
3	map.getForUpdate(key1,v)		O bloqueio S é atualizado para um bloqueio U para key1.
4		map.get(key1)	Bloqueio S concedido para key1.
5		map.getForUpdate(key1,v)	Bloqueado: T1 já possui um bloqueio U.
6	session.commit()		Conflito: O bloqueio U para key1 não pode ser atualizado.
7		session.commit()	Conflito: O bloqueio S para key1 não pode ser atualizado.

Tabela 35. Conflitos de uma única chave, continuação

	Encadeamento 1	**Encadeamento 2**	
1	session.begin()	session.begin()	Cada encadeamento estabelece uma transação independente

Tabela 35. Conflitos de uma única chave, continuação (continuação)

	Encadeamento 1	Encadeamento 2	
2	map.get(key1)		Bloqueio S concedido para key1.
3	map.getForUpdate(key1,v)		O bloqueio S é atualizado para um bloqueio U para key1
4		map.get(key1)	O bloqueio S é concedido para key1.
5		map.getForUpdate(key1,v)	Bloqueado: O Encadeamento 1 já possui um bloqueio U.
6	session.commit()		Conflito: O bloqueio U para key1 não pode ser atualizado para um bloqueio X porque o Encadeamento 2 possui um bloqueio S.

Se ObjectMap.getForUpdate for utilizado para evitar o bloqueio S, o conflito será evitado:

Tabela 36. Conflitos de uma única chave, continuação

	Encadeamento 1	Encadeamento 2	
1	session.begin()	session.begin()	Cada encadeamento estabelece uma transação independente.
2	map.getForUpdate(key1)		Bloqueio U concedido para o encadeamento 1 para key1.
3		map.getForUpdate(key1)	O pedido do bloqueio U é bloqueado.
4	map.update(key1,v)	<blocked>	
5	session.commit()	<blocked>	O bloqueio U para key1 pode ser atualizado com êxito para um bloqueio X.
6		<liberado>	O bloqueio U é finalmente concedido para key1 para o encadeamento 2.
7		map.update(key2,v)	Bloqueio U concedido ao encadeamento 2 para key2.
8		session.commit()	O bloqueio U para key1 pode ser atualizado com êxito para um bloqueio X.

Soluções:

1. Use o método getForUpdate ao invés do método get para adquirir um bloqueio U ao invés de um bloqueio S.
2. Utilize um nível de isolamento de transação da leitura confirmada para evitar reter bloqueios S. Reduzir o nível de isolamento de transação aumenta a possibilidade de leituras não-repetíveis. No entanto, leituras não repetitivas de um cliente são possíveis apenas se o cache de transição estiver explicitamente invalidado pelo mesmo cliente.
3. Utilize a estratégia de bloqueio otimista. A utilização da estratégia de bloqueio optimistic requer a manipulação de exceções de colisão otimistas.

- **Problema:** Diversos conflitos de chaves solicitados.

  Descrição: Este cenário descreve o que acontece se duas transações tentarem atualizar a mesma entrada diretamente e manter bloqueios S com outras entradas.

Tabela 37. Cenário de conflito de múltiplas chaves em ordem

	Encadeamento 1	**Encadeamento 2**	
1	session.begin()	session.begin()	Cada encadeamento estabelece uma transação independente.
2	map.get(key1)	map.get(key1)	O bloqueio S é concedido a ambas as transações para key1.
3	map.get(key2)	map.get(key2)	Bloqueio S concedido para ambas as transações para key2.
4	map.update(key1,v)		Nenhum bloqueio U. Atualização executada no cache transacional.
5		map.update(key2,v)	Nenhum bloqueio U. A atualização é executada no cache transacional.
6.	session.commit()		Bloqueado: O bloqueio S para key 1 não pode ser atualizado para um bloqueio X porque o encadeamento 2 possui um bloqueio S.
7		session.commit()	Conflito: O bloqueio S para key 2 não pode ser atualizado porque o encadeamento 1 possui um bloqueio S.

É possível utilizar o método ObjectMap.getForUpdate para evitar o bloqueio S, assim, é possível evitar o bloqueio:

Tabela 38. Cenário de conflito de múltiplas chaves em ordem, continuação

	Encadeamento 1	**Encadeamento 2**	
1	session.begin()	session.begin()	Cada encadeamento estabelece uma transação independente.
2	map.getForUpdate(key1)		Bloqueio U concedido para a transação T1 para key1.
3		map.getForUpdate(key1)	O pedido do bloqueio U é bloqueado.
4	map.get(key2)	<blocked>	Bloqueio S concedido para T1 para key2.
5	map.update(key1,v)	<blocked>	
6	session.commit()	<blocked>	O bloqueio U para key1 pode ser atualizado com êxito para um bloqueio X.
7		<liberado>	O bloqueio U finalmente é concedido para key1 para T2
8		map.get(key2)	Bloqueio S concedido para T2 para key2.
9		map.update(key2,v)	Bloqueio U concedido para T2 para key2.
10		session.commit()	O bloqueio U para key1 pode ser atualizado com êxito para um bloqueio X.

Soluções:

1. Use o método getForUpdate ao invés do método get para adquirir um bloqueio U diretamente para a primeira chave. Esta estratégia funciona apenas se o método order for determinístico.
2. Utilize um nível de isolamento de transação da leitura confirmada para evitar reter bloqueios S. Esta solução é a mais fácil para implementar se o método order não for determinístico. Reduzir o nível de isolamento de

transação aumenta a possibilidade de leituras não-repetíveis. Entretanto, as leituras não-repetíveis são possíveis apenas se o cache de transição estiver explicitamente invalidado.

3. Utilize a estratégia de bloqueio otimista. A utilização da estratégia de bloqueio optimistic requer a manipulação de exceções de colisão otimistas.

- **Problema:** Fora de ordem com bloqueio U

  Descrição: Se a ordem na qual as chaves são solicitadas não puder ser garantida, um conflito ainda poderá ocorrer.

Tabela 39. Fora de ordem com cenário com bloqueio U

	Encadeamento 1	**Encadeamento 2**	
1	session.begin()	session.begin()	Cada encadeamento estabelece uma transação independente.
2	map.getforUpdate(key1)	map.getForUpdate(key2)	Bloqueios U concedidos com êxito para key1 e key2.
3	map.get(key2)	map.get(key1)	Bloqueio S concedido para key1 e key2.
4	map.update(key1,v)	map.update(key2,v)	
5	session.commit()		O bloqueio U não pode ser atualizado para um bloqueio X porque T2 possui um bloqueio S.
6		session.commit()	O bloqueio U não pode ser atualizado para um bloqueio X porque T1 possui um bloqueio S.

Soluções:

1. Quebre todo o trabalho com um bloqueio U global único (mutex). Este método reduz a simultaneidade, mas trata todos os cenários quando o acesso e a ordem são não-determinísticos.
2. Utilize um nível de isolamento de transação da leitura confirmada para evitar reter bloqueios S. Esta solução é a mais fácil para implementar se o método order não for determinístico e fornece a maior quantidade de simultaneidade. Reduzir o nível de isolamento de transação aumenta a possibilidade de leituras não-repetíveis. Entretanto, as leituras não-repetíveis são possíveis apenas se o cache de transição estiver explicitamente invalidado.
3. Utilize a estratégia de bloqueio otimista. A utilização da estratégia de bloqueio optimistic requer a manipulação de exceções de colisão otimistas.

Conceitos relacionados:

"Bloqueios" na página 493
Bloqueios têm ciclos de vida e os tipos diferentes de bloqueios são compatíveis com outros de várias maneiras. Os bloqueios devem ser manipulados na ordem correta para evitar cenários de conflito.

Resolução de Problemas de Exceções de Tempo Limite do Bloqueio para uma Transação Multipartição

Java

O cenário que é descrito é um exemplo de uma transação multipartição que está causando uma exceção de tempo limite de bloqueio. Dependendo do estado da transação, as soluções ilustram como você pode resolver esse problema manualmente.

Antes de Iniciar

Implemente a manipulação de exceção no seu aplicativo. Para obter informações adicionais, consulte "Implementando Manipulação de Exceção em Cenários de Bloqueio" na página 499.

A seguinte exceção é exibida como resultado:

```
Caused by: com.ibm.websphere.objectgrid.LockTimeoutException:
Local-40000139-DEF8-05EA-E000-64A856931719 timed out waiting
for lock mode S to be granted for map name: TS2_MapP, key: k
ey12 granted = X lock request queue
->[WXS-40000139-DEF6-FA84-E000-1CB456931719, state = Granted,
requested 73423 milli-seconds ago, marked to keep current mode
false, snapshot mode 0, mode = X, thread
name = xIOReplicationWorkerThreadPool : 29]
->[Local-40000139-DEF8-05EA-E000-64A856931719, state
= Waiting for 5000 milli-seconds, marked to keep current
mode false, snapshot mode 0, mode = S, thread
name = xIOWorkerThreadPool : 28]
dump of all locks for WXS-40000139-DEF6-FA84-E000-1CB456931719
Key: key12, map: TS2_MapP
strongest currently granted mode for key is X
->[WXS-40000139-DEF6-FA84-E000-1CB456931719, state
= Granted, requested  73423 milli-seconds ago, marked to
keep current mode false, snapshot mode 0, mode = X,
thread name = xIOReplicationWorkerThreadPool : 29]
dump of all locks for Local-40000139-DEF8-05EA-E000-64A856931719
```

Essa mensagem representa a cadeia que é transmitida como um parâmetro quando a exceção é criada e emitida.

Procedimento

Problema: Você vê uma exceção de tempo limite de bloqueio e o portador da trava é uma transação multipartição ou a pasta de log está aumentando com mensagens de log.
Diagnóstico:
Você verá uma mensagem de log repetidamente preenchendo a pasta de log como a seguir:

```
00000099 TransactionLog I  CWOBJ8705I:
Resolução automática da transação
WXS-40000139-DF01-216D-E002-1CB456931719 em RM:TestGrid:TestSet2:20
ainda está esperando por uma decisão.
Uma outra tentativa de resolver a transação ocorrerá em 30 segundos.
```

Determine qual tipo de transação está causando o bloqueio. Se o prefixo no identificador de transação é WXS-, isto indica transação multipartição. Se o prefixo no identificador de transação é Local-, isto indica que a transação é transação de partição única.
Causa: O aplicativo está provavelmente mantendo o bloqueio porque uma confirmação ou um retrocesso não ocorreu.
Solução: Determine o estado da transação e por quanto tempo ela estava nesse estado. Utilize o utilitário de comando **xscmd -c listindoubts** com a opção -d(para uma saída detalhada) ou utilize o MBean da transação.

Conceitos relacionados:

Java "Visão Geral do Processamento de Transações" na página 464
O WebSphere eXtreme Scale usa transações de acordo com seu mecanismo de interação com os dados.

Java "Two-phase Commit e Recuperação de Erro" na página 486
O protocolo two-phase commit coordena todas as partições que participam de uma transação distribuída para confirmar ou recuperar a transação.

Java "Estratégias de Bloqueio" na página 473
As estratégias de bloqueio incluem pessimista, otimista e nenhum. Para escolher uma estratégia de bloqueio, é necessário considerar questões como a porcentagem de cada tipo de operações que você tem, se você utiliza um utilitário de carga, entre outras.

Resolvendo Exceções de Tempo Limite do Bloqueio

Java

Usando o comando **xscmd -c listindoubt**, é possível visualizar o estado de uma transação e determinar um curso de ação.

Conceitos relacionados:

Java "Visão Geral do Processamento de Transações" na página 464
O WebSphere eXtreme Scale usa transações de acordo com seu mecanismo de interação com os dados.

Java "Two-phase Commit e Recuperação de Erro" na página 486
O protocolo two-phase commit coordena todas as partições que participam de uma transação distribuída para confirmar ou recuperar a transação.

Java "Estratégias de Bloqueio" na página 473
As estratégias de bloqueio incluem pessimista, otimista e nenhum. Para escolher uma estratégia de bloqueio, é necessário considerar questões como a porcentagem de cada tipo de operações que você tem, se você utiliza um utilitário de carga, entre outras.

Resolvendo Exceções de Tempo Limite de Bloqueio com o comando `xscmd -c listindoubts`

Procedimento

- Exiba a lista detalhada de transações em seu ambiente: `xscmd -c listindoubt -d`
  O comando pode retornar um dos seguintes estados:
  - Todas as transações confirmadas
  - Preparado
  - Um gerenciador de transações (TM) ausente
- Execute as ações apropriadas para resolver a transação. **Problema:** Todas as transações confirmadas

```
[1] WXS-40000139-DEF8-EF60-E002-1CB456931719
Timestamp                Partition    Role  State     Container   Resync  Attempts
------------------------------------------- ---------------------------------
2012-09-19 10:40:19.824  TestSet1:11  TM  COMMITT  MPTBasic2_C-0  Primary  0
2012-09-19 10:40:19.824  TestSet1:7  RM  PREPARED  MPTBasic0_C-1  Primary  0
2012-09-19 10:40:19.839  TestSet2:20  RM  PREPARED  MPTBasic2_C-0  Primary  0
2012-09-19 10:40:19.824  TestSet2:6  RM  PREPARED  MPTBasic0_C-1  Primary  0
```

  Solução: Confirme as partições do gerenciador de recursos (RM) e, em seguida, esqueça a transação.

1. Emita o seguinte comando para confirmar a partição do RM na transação WXS-40000139-DEF8-EF60-E002-1CB456931719: `xscmd -c listIndoubts -xid WXS-40000139-DEF8-EF60-E002-1CB456931719 -cm -rm`
2. Emita o seguinte comando para esquecer essa transação: `xscmd -c listIndoubts -xid WXS-40000139-DEF8-EF60-E002-1CB456931719 -f`

Problema: Transações preparadas

```
[1] WXS-40000139-DEF6-FA84-E000-1CB456931719

Timestamp               Partition    Role   State   Container     Resync Attempts
----------------------------------------------------------------- --------------
2012-09-19 10:38:11.603  TestSet1:10  RM  PREPARED  MPTBasic2_C-0  Primary  0
2012-09-19 10:38:11.588  TestSet1:5  TM  PREPARED  MPTBasic2_C-0  Primary  0
2012-09-19 10:38:11.603  TestSet2:11  RM  PREPARED  MPTBasic2_C-0  Primary  0
2012-09-19 10:38:11.619  TestSet2:13  RM  PREPARED  MPTBasic2_C-0  Primary  0
```

Solução: Recupere a partição do TM primeiro e, em seguida, recupere partições do RM subsequentes. Em seguida, esqueça a transação.

1. Emita o comando a seguir para recuperar a partição do TM na transação WXS-40000139-DEF6-FA84-E000-1CB456931719: `xscmd -c listIndoubts -xid WXS-40000139-DEF6-FA84-E000-1CB456931719 -r -tm`
2. Emita o comando a seguir para recuperar as partições do RM nesta transação: `xscmd -c listIndoubts -xid WXS-40000139-DEF6-FA84-E000-1CB456931719 -r -rm`
3. Emita o seguinte comando para esquecer essa transação: `xscmd -c listIndoubts -xid WXS-40000139-DEF6-FA84-E000-1CB456931719 -f`

Problema: Um TM ausente

```
[1] WXS-40000139-DEF8-EF31-E000-1CB456931719

Timestamp               Partition    Role   State   Container     Resync Attempts
----------------------------------------------------------------- --------------
2012-09-19 10:40:19.777  TestSet1:11  RM  PREPARED  MPTBasic2_C-0  Primary  0
2012-09-19 10:40:19.792  TestSet2:5  RM  PREPARED  MPTBasic2_C-0  Primary  0
2012-09-19 10:40:19.777  TestSet2:6  RM  PREPARED  MPTBasic2_C-1  Primary  0
```

Solução: Recupere as partições do RM.

– Emita o comando a seguir para recuperar as partições do RM na transação WXS-40000139-DEF8-EF31-E000-1CB456931719: `xscmd -c listIndoubts -xid WXS-40000139-DEF8-EF31-E000-1CB456931719 -r`

Resolução de Problemas de Segurança

Use estas informações para resolver problemas com sua configuração de segurança.

Procedimento

- **Problema:** A extremidade da conexão do cliente requer Secure Sockets Layer (SSL), com a configuração transportType definida para `SSL-Required`. No entanto, a extremidade da conexão do servidornão suporta SSL e possui a configuração transportType definida para `TCP/IP`. Como resultado, a exceção a seguir é encadeada para outra exceção nos arquivos de log:

```
java.net.ConnectException: connect: Address is invalid on local machine, or
port is not valid on remote machine
    at java.net.PlainSocketImpl.doConnect(PlainSocketImpl.java:389)
    at java.net.PlainSocketImpl.connectToAddress(PlainSocketImpl.java:250)
    at java.net.PlainSocketImpl.connect(PlainSocketImpl.java:237)
    at java.net.SocksSocketImpl.connect(SocksSocketImpl.java:385)
    at java.net.Socket.connect(Socket.java:540)
    at
com.ibm.rmi.transport.TCPTransportConnection.createSocket(TCPTransportConnection.java:155)
    at
com.ibm.rmi.transport.TCPTransportConnection.createSocket(TCPTransportConnection.java:167)
```

O endereço nessa seção pode ser um servidor de catálogo, um servidor de contêiner ou um cliente.

Solução: Consulte “Configurando Tipos de Transportes Seguros” na página 784 para obter uma tabela com as configurações de segurança válidas entre clientes e servidores.

- Quando o agente é usado, o cliente envia a chamada do agente para o servidor e o servidor envia a resposta de volta para o cliente para reconhecer a chamada do agente. Quando o agente conclui o processamento, o servidor inicia uma conexão para enviar os resultados do agente. Isso torna o servidor de contêiner um cliente a partir do ponto de vista de conexão. Portanto, se o TLS ou o SSL está configurado, certifique-se de que o certificado público do cliente seja importado no armazenamento confiável do servidor.
- **Problema:** Quando usuários estão autorizados a acessar uma grade de dados do WebSphere eXtreme Scale, esses usuários também podem ser autorizados a executar operações de gerenciamento usando o comando **xscmd** ou o comando **stopOgServer**. A maioria dos implementadores de grade de dados restringem o acesso administrativo apenas a um subconjunto dos usuários que podem acessar os dados da grade.

  Se você utilizar o comando a seguir para acessar a grade de dados, também poderá estar autorizado a desempenhar ações administrativas, como listAllJMXAddresses:

  ```
  ./xscmd.sh -user <user> -password <password> <other_parameters>
  ```

  Se esta operação funciona para este usuário, qualquer operação **xscmd** também pode ser executada pelo mesmo usuário.

  Resolução: Quando os componentes do eXtreme Scale são executados com o WebSphere Application Server, use o console administrativo do WebSphere Application Server para ativar o gerenciador de segurança. Clique em **Segurança** > **Segurança Global** e selecione as caixas de seleção, **Ativar Segurança Administrativa** e **Usar Java 2 Security**, para restringir acesso do aplicativo a recursos locais.

  O acesso às operações de gerenciamento é controlado pelo gerenciador de segurança do WebSphere Application Server e é concedido apenas aos usuários que pertencem à função de Administrador do WebSphere. O comando **xscmd** deve ser executado a partir do diretório WebSphere Application Server.

  Quando componentes do eXtreme Scale são executados em um ambiente independente, etapas adicionais são necessárias para implementar a segurança administrativa. Você deve executar os servidores de catálogos e servidores de contêiner usando o gerenciador de segurança Java, o que requer um arquivo de políticas.

  O arquivo de políticas é semelhante ao exemplo a seguir:

  Lembre-se: Geralmente também há entradas MapPermission, conforme documentado em “Tutorial de Segurança do Java SE - Etapa 5” na página 30.

```
grant codeBase "file:${objectgrid.home}/lib/*" {
permission java.security.AllPermission;
};

grant principal javax.security.auth.x500.X500Principal "CN=manager,O=acme,OU=OGSample" {
permission javax.management.MBeanPermission "*", "getAttribute,setAttribute,invoke,queryNames";
};
```

  Neste caso, apenas o proprietário do gerenciador está autorizado a executar operações administrativas utilizando o comando **xscmd**. Outras linhas podem ser incluídas conforme necessário para conceder permissões adicionais aos proprietários do MBean. Um tipo diferente de principal é necessário se você usa autenticação LDAP.

Digite o seguinte comando: UNIX Linux

```
startOgServer.sh <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config -Djava.security.manager
-Djava.security.policy="auth.policy" -Dobjectgrid.home=$OBJECTGRID_HOME
```

UNIX Linux 8.6+

```
startXsServer.sh <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config -Djava.security.manager
-Djava.security.policy="auth.policy" -Dobjectgrid.home=$OBJECTGRID_HOME
```

Windows

```
startOGServer.bat <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config -Djava.security.manager
-Djava.security.policy="auth.policy" -Dobjectgrid.home=%OBJCTGRID_HOME%
```

Windows 8.6+

```
startXsServer.bat <arguments> -jvmargs -Djava.security.auth.login.config=jaas.config -Djava.security.manager
-Djava.security.policy="auth.policy" -Dobjectgrid.home=%OBJCTGRID_HOME%
```

Especifique -Djava.security.policy neste caso, em vez de -Djava.security.auth.policy.

Solucionando Problemas de Configurações de Perfil do Liberty

Use essas informações para solucionar problemas comuns ocorridos com o perfil do Liberty.

Sobre Esta Tarefa

Para ajudar a identificar e solucionar os problemas, o produto tem um componente de criação de log unificado. Consulte “Analisando Dados de Log e de Rastreio” na página 865.

Os detalhes das restrições conhecidas que se aplicam na utilização do perfil do Liberty são fornecidos nos dois tópicos a seguir no Centro de Informações do WebSphere Application Server:

- Perfil do Liberty: Restrições conhecidas do ambiente de tempo de execução
- Perfil do Liberty: Restrições conhecidas das Ferramentas do Desenvolvedor

Procedimento

- **Problema:** Ocorreram problemas que não foram explicados prontamente.

  Solução: Verifique se seus Java development kits estão no Java Versão 6 ou posterior e se estão em um nível de serviço atual. Consulte o tópico Níveis mínimos suportados de Java no perfil do Liberty: Restrições conhecidas do ambiente de tempo de execução para obter informações adicionais.
- **Problema:** O erro de segurança a seguir é exibido quando você tenta acessar um aplicativo que é redirecionado a uma porta SSL e essa porta não está disponível:

  `CWWKS9105E: Não foi possível determinar a porta SSL para um redirecionamento automático`

  Solução: A porta pode não estar disponível devido a uma configuração de SSL ausente ou a algum erro na definição de configuração do SSL. Verifique a configuração de SSL no arquivo `server.xml` para certificar-se de que ela existe e está correta.

Coletando Dados com o IBM Support Assistant Data Collector

Execute o IBM Support Assistant Data Collector para coletar dados de determinação de problema a partir do seu ambiente do WebSphere eXtreme Scale. Usando esta ferramenta, é possível reduzir a quantidade de tempo que leva para reproduzir um problema com o conjunto de níveis de rastreio de RAS apropriado e reduzir o esforço necessário para enviar as informações de log apropriadas para o Suporte IBM.

Antes de Iniciar

Antes de executar a ferramenta, tenha as informações de configuração do sistema a seguir prontas para fornecer à ferramenta:

- Nome do arquivo para salvar os dados coletados
- Diretório do *java_home*
- Diretório do *wxs_home*
- Diretório ativo utilizado pelo WebSphere eXtreme Scale
- Local dos arquivos de scripts adicionais utilizados para iniciar os servidores

Sobre Esta Tarefa

Em liberações anteriores do WebSphere eXtreme Scale, a ferramenta IBM Support Assistant Lite era utilizada para reunir o log para determinação de problemas. A ferramenta IBM Support Assistant Lite continua sendo fornecida com o produto no diretório *wxs_home*/`isalite_wxs`. O IBM Support Assistant Data Collector é uma ferramenta mais interativa instalada com a Versão 8.6 e posterior. O IBM Support Assistant Data Collector aprimora a facilidade de uso da coleta de dados lembrando várias entradas, reduzindo a digitação repetitiva durante a entrada do console. Para obter mais informações, consulte IBM Support Assistant Data Collector.

Procedimento

1. Inicie a ferramenta. A ferramenta é executada no modo do console, iniciando o script de ativação a partir da linha de comandos. O script para a ferramenta está instalado no diretório *wxs_home*/`isalite_dc`.
   - Windows **`isadc.bat`**
   - Linux UNIX **`isadc.sh`**
2. Forneça suas informações do sistema para a ferramenta. Em cada etapa, as opções são apresentadas como listas numeradas e você deve inserir o número desejado e pressionar a tecla ENTER. Quando uma entrada é necessária, são exibidos prompts nos quais você insere sua resposta e pressiona a tecla ENTER. É possível localizar detalhes da coleção para cada tipo de problema em seus documentos MustGather correspondentes. Também é possível fornecer o nome do arquivo compactado e o local do diretório no qual você deseja salvar suas informações em um pacote configurável.
3. Pare a ferramenta coletora digitando a opção **`quit`** no modo do console.

Resultados

As informações relacionadas ao ambiente a seguir são empacotadas em um arquivo compactado que você nomeou para salvar os dados:

- Reunir arquivos de log

- Reunir informações de versão do eXtreme Scale
- Reunir informações de versão Java
- Reunir informações sobre a estrutura de diretório do *wxs_home*, incluindo quais arquivos estão atualmente armazenados em vários diretórios. Os arquivos reais não são salvos no arquivo compactado.
- Reunir os scripts atualmente no diretório `bin`.

O que Fazer Depois

Entre em contato com o suporte IBM e forneça o arquivo compactado que você gerou com o IBM Support Assistant Data Collector. Para obter informações adicionais, consulte "Entrando em Contato com o Suporte IBM" na página 851.

IBM Support Assistant for WebSphere eXtreme Scale

É possível usar o IBM Support Assistant para coletar dados, analisar sintomas e acessar informações do produto.

IBM Support Assistant Lite

O IBM Support Assistant Lite for WebSphere eXtreme Scale fornece uma coleta de dados automática e suporte à análise de sintomas para cenários de determinação de problemas.

O IBM Support Assistant Lite reduz o período de tempo que leva para reproduzir um problema com os níveis de rastreamento Reliability, Availability and Serviceability adequados configurados (os níveis de rastreamento são automaticamente configurados pela ferramenta) para simplificar a determinação de problemas. Se você precisar de assistência adicional, o IBM Support Assistant Lite também reduz o esforço necessário para enviar as informações de log apropriadas para o IBM Support.

O IBM Support Assistant Lite é incluído em cada instalação do WebSphere eXtreme Scale Versão 7.1.0

IBM Support Assistant

O IBM® Support Assistant (ISA) fornece acesso rápido a recursos do produto, de educação e de suporte que podem ajudar você a responder questões e resolver sozinho problemas com os produtos de software IBM, sem precisar entrar em contato com o IBM Support. Plug-ins diferentes específicos do produto permitem customizar o IBM Support Assistant para os produtos particulares que você instalou. O IBM Support Assistant também podem coletar dados do sistema, arquivos de log e outras informações para ajudar o IBM Support a determinar a causa de um problema particular.

O IBM Support Assistant é um utilitário a ser instalado em sua estação de trabalho, não diretamente no sistema do servidor WebSphere eXtreme Scale em si. Os requisitos de memória e de recurso para o Assistant podem afetar negativamente o desempenho do sistema do servidor WebSphere eXtreme Scale. Os componentes de diagnóstico móveis incluídos são projetados para um impacto mínimo para a operação normal de um servidor.

É possível usar o IBM Support Assistant para ajudá-lo das seguintes maneiras:

- Para pesquisar em fontes de conhecimento e de informações IBM e não IBM em vários produtos IBM para responder uma questão ou resolver um problema
- Para localizar informações adicionais por meio de recursos da web específicos do produto; incluindo páginas iniciais do produto e de suporte, grupos de notícias e fóruns de clientes, qualificações e recursos de treinamento e informações sobre como resolver problemas e as perguntas mais comuns
- Para aumentar sua capacidade para diagnosticar problemas específicos do produto com as ferramentas de diagnóstico de destino disponíveis no Support Assistant
- Para simplificar a coleta de dados de diagnóstico para ajudar você e a IBM a resolver seus problemas (coletar dados gerais ou dados específicos do produto/sintoma)
- Para ajudar no relatório de incidentes de problemas ao IBM Support por meio de uma interface online customizada, incluindo a capacidade de conectar os dados de diagnóstico mencionados acima ou qualquer outra informação a incidentes novos ou existentes

Finalmente, é possível usar o recurso Updater integrado para obter suporte para produtos de software e recursos adicionais assim que eles forem disponibilizados. Para configurar o IBM Support Assistant para ser usado com o WebSphere eXtreme Scale, primeiro instale o IBM Support Assistant usando os arquivos fornecidos na imagem transferida por download da página da web Visão Geral do IBM Support em: http://www-947.ibm.com/support/entry/portal/Overview/Software/Other_Software/IBM_Support_Assistant. A seguir, use o IBM Support Assistant para localizar e instalar qualquer atualização do produto. Também é possível optar por instalar plug-ins disponíveis para outro software IBM em seu ambiente. Mais informações e a versão mais recente do IBM Support Assistant estão disponíveis a partir da página da web do IBM Support Assistant em: http://www.ibm.com/software/support/isa/.

Avisos

Referências nesta publicação a produtos, programas ou serviços IBM não significam que a IBM pretende torná-los disponíveis em todos os países onde opera. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. A avaliação e verificação da operação em conjunto com outros produtos, exceto aqueles expressamente designados pela IBM, são de inteira responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não garante ao Cliente nenhum direito sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Licenciados deste programa que desejam obter mais informações sobre este assunto com objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) a utilização mútua das informações trocadas, devem entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146,
Botafogo
Rio de Janeiro, RJ
CEP 22290-240
Brasil

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo, em alguns casos, o pagamento de uma taxa.

Marcas Registradas

IBM, o logotipo IBM e ibm.com são marcas registradas da International Business Machines Corp., registrada em várias jurisdições pelo mundo. Outros nomes de produtos e serviços podem ser marcas registradas da IBM ou de outras empresas. Uma lista atual de marcas registradas IBM está disponível na Web em "Copyright and trademark information" em www.ibm.com/legal/copytrade.shtml.

Java e todas as marcas registradas e logotipos baseados em Java são marcas ou marcas registradas da Oracle e/ou suas afiliadas.

Linux é uma marca registrada da Linus Torvalds nos Estados Unidos e/ou em outros países.

Microsoft, Windows, Windows NT e o logotipo do Windows são marcas registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.

Outros nomes de empresas, produtos e serviços podem ser marcas registradas ou marcas de serviços de terceiros.

Índice Remissivo

Caracteres Especiais

A

B

C

D

E

F

G

H

I

J

L

M

O

P

R

S

T

U

V

W

X

Impresso no Brasil