IBM SOA
Policy Gateway Pattern

Índice

Capítulo 1. Visão Geral de SOA Policy

O gerenciamento de política desempenha uma função-chave no controle de políticas de uma forma estruturada e consistente. As políticas podem ser usadas para permitir melhor controle em qualquer ambiente orientado a serviços. As práticas de Arquitetura Orientada a Serviços (SOA) ajudam as empresas a identificar e focalizar os serviços principais dos negócios. Incluindo políticas, nós incluímos pontos de controle e agilidade para os negócios e a tecnologia da informação. Como resultado, o SOA é mais consumível, melhorando o tempo de maturação para os usuários de negócios com custos reduzidos para seus projetos, e acelera a adoção de soluções SOA.

Uma política é um elemento independente que pode ser aplicado a um ou vários recursos, incluindo serviços diferentes. A designação da política e quaisquer metadados associados, especialmente em um ambiente distribuído, pode ocorrer em vários pontos de execução e pontos de decisão.

A Arquitetura SOA Policy

A arquitetura SOA Policy descreve a interação de Policy Authoring Point (PAP), Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Information Point (PIP) e Policy Monitoring Point (PMP). Nesse padrão, o PAP é atingido usando o WSRR e o PEP é atingido usando o WebSphere DataPower.

A organização da arquitetura de política básica e a definição desses pontos principais são:

- **Policy Authoring Point** - Fornece recursos de política para a criação de uma política, gerenciamento e controle da política e sua designação a recursos e administração dos resultados da política durante o tempo de execução. Inclui um repositório para armazenar políticas. Nesse padrão, isso é alcançado usando o WSRR.
- **Policy Enforcement Point** - É um ponto funcional que é executado no middleware que:
  - Impinge políticas.
  - Recebe atualizações de política de execução e as deixa prontas ou as converte para uso.
  - Fornece métricas de execução para o Policy Monitoring Point.
  - Fornece resultados e analítica da política de execução para o Policy Administration Point e os Policy Monitoring Points.
  - Altera os locais em que as políticas são realmente aplicadas e impingidas dependendo do estágio do ciclo de vida:
    - Durante o tempo de design, o registro e repositório de serviço em si é o ponto de execução.
    - Durante o tempo de execução, as políticas são geralmente impingidas pelo sistema intermediário subjacente (middleware) que conecta os provedores de serviços aos clientes.

  Neste padrão, isso é alcançado usando o WebSphere DataPower.
- **Policy Decision Point** - Avalia as solicitações dos participantes com relação a políticas ou contratos e atributos relevantes. Ele renderiza uma decisão de autorização, elegibilidade ou validação para fornecer resultados calculados.

- **Policy Information Point** - Fornece informações externas para o Policy Decision Point, como informações sobre os atributos LDAP ou os resultados de um banco de dados com informações que devem ser avaliadas para tomar uma decisão de política.
- **Policy Monitoring Point** - Um componente funcional que fornece a função de monitoramento de política detalhada para a arquitetura geral; por exemplo, a visão geral da política no ambiente distribuído. Isso inclui:
  - Receber atualizações de política de monitoramento e deixá-las prontas ou convertê-las para uso.
  - Capturar a coleção em tempo real e a análise de estatísticas para exibição.
  - Correlacionar, analisar e visualizar os dados alimentados pelos vários coletores em tempo real, incluindo Policy Enforcement Points.
  - Um console de gerenciamento que fornece visibilidade no gerenciamento da rede distribuída de pontos de execução de política e o status dessas execuções.
  - Criar log, agregar medidas e destacar eventos significantes conforme especificado pela política de monitoramento.
  - Fornecer analítica de política de monitoramento para o Policy Administration Point e os Policy Enforcement Points.

  Nota: O monitoramento não está incluso neste padrão.

O consumidor e o provedor interagem com o middleware, que, por sua vez, interage com o repositório e qualquer software de monitoramento.

Como a Arquitetura SOA Policy Funciona Junto

O fluxo de padrão acionável de SOA Policy é mostrado em Figura 1 na página 3 e descrito abaixo.

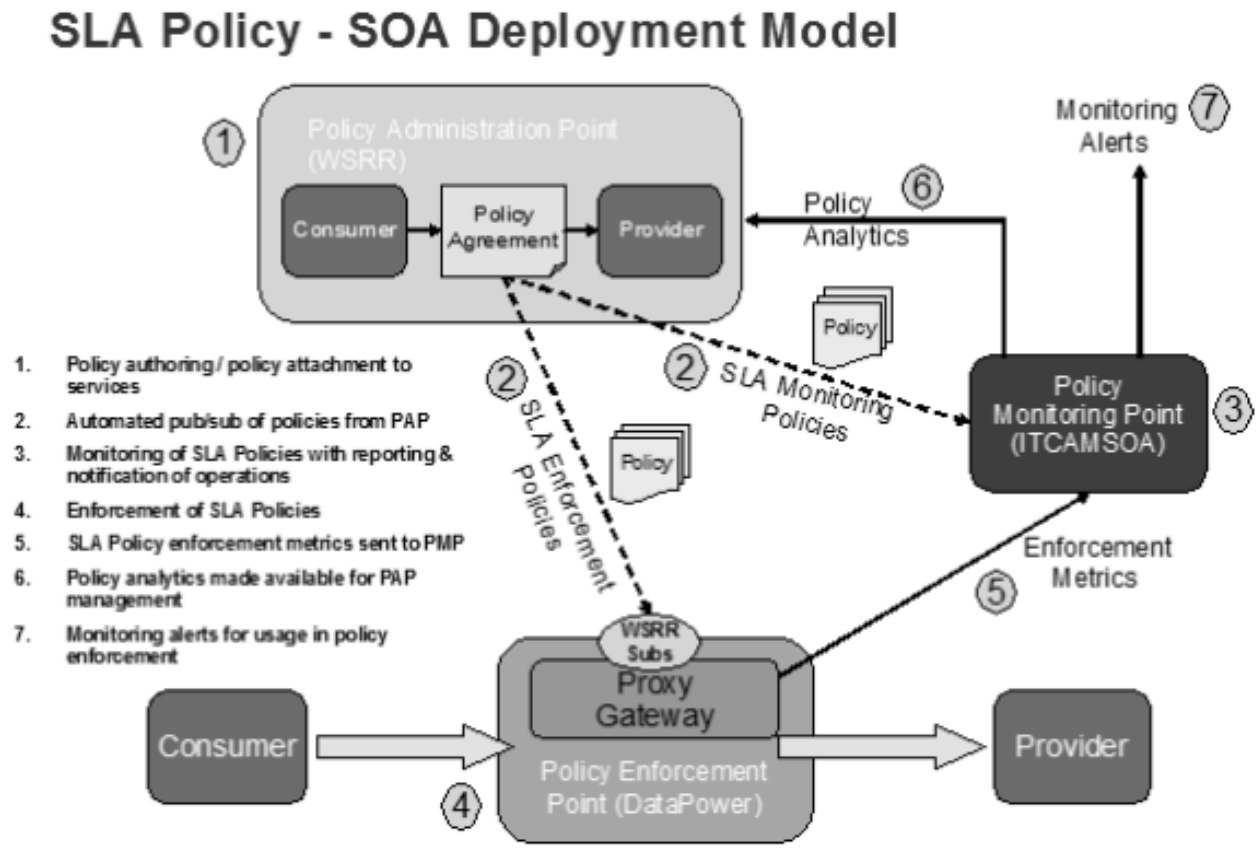


Figura 1. Política de Acordo de Nível de Serviço (SLA) - O Modelo de Implementação SOA

1. As políticas são criadas e, em seguida, anexadas a serviços que requerem dessa política. Geralmente, isto segue a ordem a seguir:
   a. O conjunto de serviços é carregado ou criado no repositório de serviço. Isto é uma parte do Policy Authoring Point.
   b. O conjunto de políticas necessárias é criado no Policy Authoring Point usando o ciclo de vida de política:
      1) As políticas são anexadas aos serviços que requerem essas políticas – no nível de serviço, operação ou terminal, conforme necessário.
2. A pub/sub automatizada de políticas do Policy Authoring Point aos Policy Enforcement Points e ao Policy Monitoring Point.

   Nota: O monitoramento usando o ITCAM for SOA não é incluído neste padrão.
   a. Como parte da configuração, o ITCAM for SOA assina a política de monitoramento a partir do WSRR. Isso ocorre apenas uma vez.
   b. Como parte da configuração, os gateways de proxy são criados em cada dispositivo WebSphere Data Power que possui transações de serviço com execução de política. Isso ocorre apenas uma vez e é incluso ou alterado conforme necessário.
   c. Como parte da configuração, cada gateway de proxy no dispositivo assina políticas do WSRR para serviços pelos quais ele é responsável. Isso ocorre apenas uma vez e é incluso ou alterado conforme necessário.

d. Como parte da configuração, o WebSphere DataPower é configurado de modo que as políticas possam ser compartilhadas por outros dispositivos em um cluster. Isso ocorre apenas uma vez e é incluso ou alterado conforme necessário.
e. O ITCAM for SOA faz download das políticas de monitoramento conforme elas são publicadas.
f. O ITCAM for SOA converte as políticas para a representação interna, chamadas de políticas de situação.
g. O WebSphere DataPower faz download dos WSDLs para os serviços pelos quais ele é responsável por transacionar.
h. O WebSphere DataPower faz download das políticas para os serviços pelos quais ele responsável quando notificado pelo WSRR.
i. O WebSphere DataPower converte as políticas para a representação interna do WebSphere DataPower na forma de objetos SLM.

3. Monitoramento de políticas SOA com relatório e notificação de operações:
   a. As políticas de monitoramento estão ativas no ITCAM para a Política de Situação SOA.
   b. O ITCAM for SOA recebe informações de monitoramento e coloca essas informações em áreas de trabalho.

   Nota: O monitoramento não é fornecido neste padrão.
4. Execução de Políticas SOA:
   a. As políticas de execução estão ativas nos vários dispositivos WebSphere DataPower.
   b. O WebSphere DataPower recebe transações de serviço e aplica políticas para esse serviço de cliente e serviço de provedor.
5. O Policy Enforcement Point envia estatísticas de SOA Policy Enforcement para o Policy Monitoring Point.

   Nota: O monitoramento não está incluso neste padrão.
6. O Policy Monitoring Point envia eventos de monitoramento ao Policy Authoring Point:
   a. Os eventos são configurados no Policy Authoring Point que precisam ser monitorados a partir do Policy Monitoring Point. Isso ocorre apenas uma vez e é incluso ou alterado conforme necessário.
   b. À medida que as políticas de situação são avaliadas como verdadeiras, os eventos são enviados ao Policy Authoring Point a partir do Policy Monitoring Point.

   Nota: O monitoramento não está incluso neste padrão.
7. Monitoramento de alertas:
   a. As políticas de situação são executadas periodicamente e tomam uma ação operacional, conforme especificado na política. O padrão é a cada 5 minutos.

O Ciclo de Vida de SOA Policy

As políticas de mediação são controladas usando o ciclo da Política SOA. Isso faz com que a política seja inicialmente identificada, até ser implementada na produção e, finalmente, descontinuada quando não for mais necessária.

Para obter mais informações sobre as transições do ciclo de vida e os estados no ciclo de vida da Política SOA, consulte Centro de Informações do IBM® WebSphere Service Registry and Repository Versão 8.0 - SOA policy lifecycle.

Padrões de Política

Os grupos de comunidade técnica da web, W3C e OASIS, criaram padrões para atender à necessidade de definir a política aplicável a serviços da web.

- **WS-Policy**: O domínio Web Services Mediation Policy 1.0 define um conjunto de asserções de política para descrever os requisitos de mediação para um serviço.
- **Web Services Policy 1.5 - Framework**: Define uma estrutura e um modelo para expressar políticas que se referem a recursos específicos do domínio, requisitos e características gerais de entidades em um sistema baseado em serviços da web.

Exemplos de especificações que definem asserções de política específica do domínio:

- WS-MediationPolicy
- WS-SecurityPolicy
- WS-ReliableMessaging e WS-ReliableMessagingPolicy
- WS-SecureConversation
- WS-Security
- WS-Transactions
- WS-Trust

Para obter informações adicionais sobre WS-MediationPolicy, consulte ftp://public.dhe.ibm.com/software/solutions/soa/pdfs/WSMediationPolicy1.6-20120124.pdf.

O Modelo de Dados WS-Policy inclui:

- **Política**: Uma coleção não ordenada de “alternativas de política”.
- **Alternativa de Política**: Uma alternativa de política é uma coleção de “asserções de política”.
- **Asserção de Política**: Representa uma preferência individual; por exemplo, um requisito ou um recurso.
- **Parâmetros de Política**: A carga útil opaca de uma “asserção de política”.
- **Assunto de Política**: Uma entidade à qual uma expressão de política pode estar ligada. Isto é usado em um documento WS-PolicyAttachment.

O exemplo a seguir, Figura 2 na página 6, mostra uma expressão de política de segurança usando asserções definidas em WS-Security e WS-SecurityPolicy:

```
(01) <wsp:Policy
   xmlns:sp=http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702
   xmlns:wsp=http://www.w3.org/ns/ws-policy
   xmlns:wsu=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
   wsu:Id="SecureMessages">  <!-- expressão de política -->
(02)   <wsp:ExactlyOne>
(03)     <wsp:All>    <!-- alternativa de política nº1 -->
(04)       <sp:SignedParts>;   <!-- asserção de política -->
(05)         <sp:Body>   <!-- parâmetro de asserção de política -->
(06)       </sp:SignedParts>
(07)     </wsp:All>
(08)     <wsp:All>    <!-- alternativa de política nº2 -->
(09)       <sp:EncryptedParts> <!-- asserção de política -->
(10)         <sp:Body/>   <!-- parâmetro de asserção de política -->
(11)       </sp:EncryptedParts>
(12)     </wsp:All>
(13)   </wsp:ExactlyOne>
(14) </wsp:Policy>
```

As linhas (03-07) representam uma alternativa de política para assinar um corpo de mensagem.

As linhas (08-12) representam uma segunda alternativa de política para criptografar um corpo de mensagem.

As linhas (02-13) mostram o operador de política `ExactlyOne`. Os operadores de política agrupam asserções de política em alternativas de política. Uma interpretação válida da política acima seria que uma chamada de um serviço da web assinará ou criptografará o corpo da mensagem, mas não ambos.

Figura 2. Uso de Web Services Policy com Asserções de Política de Segurança.

Figura 3 mostra uma definição de política.

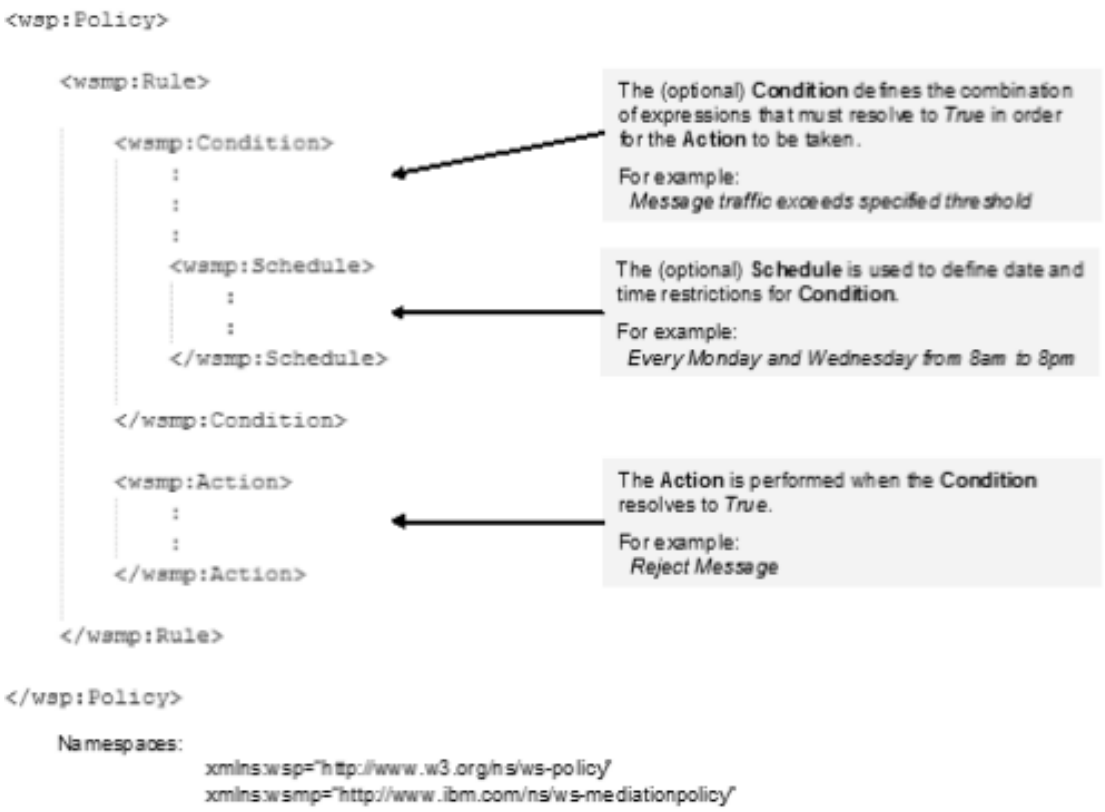


Figura 3. Visão Geral da Estrutura de Política

Anexo sobre a Política

A função Documentar de Anexo sobre a Política é associar um conjunto de políticas WS-Policy a um ponto de anexo de serviço específico para execução, como um ponto de anexo de serviços da web.

Por exemplo, as plataformas de serviços da web podem suportar pontos de anexo com base em:

- Elementos de WSDL Element URI 1.1
- Elementos de WS-Addressing

A sintaxe é definida na especificação WS-PolicyAttachment:

```
<wsp:PolicyAttachment>
    <wsp:AppliesTo>


    </wsp:AppliesTo>
    <wsp:Policy>


    </wsp:Policy>
</wsp:PolicyAttachment>
```

Figura 4. Especificação WS-PolicyAttachment

O WSRR expõe interfaces REST para adquirir os anexos sobre a política apropriados em um modelo SLA. As informações sobre o par Consumidor/ Provedor ao qual a política se aplica são passadas para o ESB no formato WS-PolicyAttachment. A sintaxe é definida na especificação WS-PolicyAttachment: Filtros de Conteúdo da Mensagem.

A política pode ser especificada para um serviço de provedor apenas, para um par de consumidor/provedor específico ou para consumidores Anônimos. Os consumidores anônimos fornecem uma maneira de definir uma política padrão que se aplica apenas aos consumidores para os quais nenhuma outra políticas se aplica.

No Figura 4, o assunto da política específica do domínio ao qual a política de aplica (o provedor) está contido na seção `<wsp:AppliesTo>` seguida pelo filtro de contexto do consumidor ao qual a política se aplica (consumidor). Em seguida, na seção `<wsp:Policy>`, a política ou políticas são declaradas ou referenciadas.

Capítulo 2. Visão Geral de Padrão

O IBM SOA Policy Gateway Pattern é um conjunto de padrões de sistema virtual que fornece um ponto de execução de política e um ponto de administração da política. O ponto de administração de política é fornecido por padrões de sistema virtual que provisionam o WSRR em uma arquitetura multicamada, oferecendo um ambiente de produção e de temporariedade. O ponto de execução de política é fornecido pelo dispositivo WebSphere DataPower no qual um domínio é criado durante a implementação do padrão do sistema virtual.

Há exemplos de política em muitos, se não todos os ambientes de Arquitetura Orientada a Serviços (SOA). Os produtores e consumidores de serviço concordam com os recursos, desempenho e características do serviço durante a fase de design. Para fazer isso, é possível usar as Service Level Definitions (SLDs) e os Acordos de Nível de Serviço (SLAs). Esse padrão permite definir políticas para SLDs e SLAs de uma maneira eficientemente administrada, definida, controlada e utilizada. Os tipos de política usados nesse padrão incluem os seguintes:

- **Políticas de Mediação** -
  - Rejeição - Rejeita ou regula solicitações que chegam em uma taxa maior que a definida.
  - Registro - Cria uma mensagem de log com o ponto de execução de política quando um serviço é chamado.
  - Transformação.
  - Validação - Valida a chamada de serviço com relação à definição de serviço.
  - Roteamento - Com base na mensagem, roteia para um terminal específico.
- **Políticas de Segurança**: Na amostra, demonstramos os meios para forçar as políticas de segurança de controle de acesso do XACML. Esses meios não são controlados dentro do ponto de administração da política neste momento.

O padrão IBM SOA Policy Gateway Pattern contém os padrões a seguir do sistema virtual:

- SOA Policy Gateway Basic Runtime Sample
- SOA Policy Gateway Governance Master
- SOA Policy Gateway Basic Runtime
- SOA Policy Gateway Advanced Runtime

O quatro padrões de sistema virtual funcionam juntos para fornecer um ambiente de controle de serviços de vários estágios. O IBM SOA Policy Gateway Pattern também fornece o recurso para provisionar vários domínios do DataPower configurados para o ambiente de controle durante a implementação do padrão. Combinadas, as seguintes topologias de implementação são fornecidas:

- Implementação Independente
- Implementação Piloto
- Implementação de Produção Integral

Para obter informações adicionais sobre Política SOA, consulte Capítulo 1, “Visão Geral de SOA Policy”, na página 1.

É possível configurar manualmente o padrão de sistema virtual implementado para incluir monitoramento com o ITCAM for SOA Versão 7. Isto fornece o monitoramento básico de eventos e expande o suporte de política para incluir políticas de monitoramento que permitem que situações de eventos sejam definidas dentro do Policy Authoring Point (PAP) e conectadas a uma definição de serviço, permitindo que o monitor pare de atuar quando a situação de evento ocorre.

Conceitos relacionados:

Capítulo 1, “Visão Geral de SOA Policy”, na página 1
O gerenciamento de política desempenha uma função-chave no controle de políticas de uma forma estruturada e consistente. As políticas podem ser usadas para permitir melhor controle em qualquer ambiente orientado a serviços. As práticas de Arquitetura Orientada a Serviços (SOA) ajudam as empresas a identificar e focalizar os serviços principais dos negócios. Incluindo políticas, nós incluímos pontos de controle e agilidade para os negócios e a tecnologia da informação. Como resultado, o SOA é mais consumível, melhorando o tempo de maturação para os usuários de negócios com custos reduzidos para seus projetos, e acelera a adoção de soluções SOA.

“SOA Policy Gateway Basic Runtime” na página 21
O SOA Policy Gateway Basic Runtime fornece um meio simples de fornecer um tempo de execução que pode ser usado independente ou integrado a um padrão SOA Policy Gateway Governance Master implementado. O padrão SOA Policy Gateway Basic Runtime suporta a implementação de um domínio do DataPower que é configurado para se comunicar com o servidor de runtime WSRR aprovisionado no padrão.

“SOA Policy Gateway Basic Runtime Sample” na página 18
O SOA Policy Gateway Basic Runtime Sample aprovisiona um SOA Policy Gateway Basic Runtime com uma interface de amostra e um aplicativo que demonstra as políticas atualmente suportadas nesta liberação.

“SOA Policy Gateway Governance Master” na página 20
O padrão SOA Policy Gateway Governance Master fornece um ambiente de controle em cluster para criar e gerenciar serviços e políticas. O ambiente é aprovisionado com o Perfil de Ativação de Controle padrão do WSRR configurado. O Perfil de Ativação de Controle padrão suporta dois destinos de promoção, Temporariedade e Produção.

“SOA Policy Gateway Advanced Runtime” na página 23
O SOA Policy Gateway Advanced Runtime inclui mais opções de alta disponibilidade e deve ser usado com o SOA Policy Gateway Governance Master.

Capítulo 3. Introdução ao IBM SOA Policy Gateway Pattern

Este padrão usa o WebSphere DataPower para controlar mensagens usando políticas controladas e definições de serviço no WSRR. Revise os tópicos nesta seção para entender o que é abrangido neste cenário, as razões pelas quais uma empresa pode desejar seguir o cenário, as funções de usuário envolvidas e uma visão geral do recurso entregue com o produto.

Antes de Iniciar

É possível usar o IBM IBM SOA Policy Gateway Pattern no IBM PureApplication System ou no dispositivo IBM Workload Deployer.

Procedimento

Para usar o IBM SOA Policy Gateway Pattern, conclua as etapas a seguir:

1. Faça download e instale o IBM SOA Policy Gateway Pattern. Para obter informações adicionais sobre como fazer download dos pacotes a partir do Passport Advantage, consulte “Fazendo Download e Instalando os Padrões” na página 12.
2. Opcional: Configure o acesso de usuário. Para obter informações adicionais, consulte “Configurando o Acesso de Usuário” na página 14.
3. Configure e implemente o padrão
   a. Aceite as licenças de imagem do sistema virtual importadas do WSRR.
   b. Aceite todos os contratos de licença no DB2 Enterprise.
   c. Implemente o padrão:
      1) Decida sobre a topologia de implementação. Para obter informações adicionais, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Topologias de Implementação.
      2) Se estiver usando uma topologia de implementação independente, implemente um único padrão Basic Runtime sem a promoção configurada.
      3) Para outras topologias, primeiro implemente o padrão SOA Policy Gateway Governance Master. Isso fornece um ambiente de controle para serviços e políticas.
      4) Depois que o padrão Governance Master for implementado com sucesso, escolha o tipo de ambiente de tempo de execução necessário. Para um ambiente de teste ou de temporariedade, um Basic Runtime geralmente será suficiente. Para um ambiente de produção, escolha o ambiente Advanced Runtime. Os tempos de execução podem ser registrados com a configuração da promoção do perfil de ativação de controle para o Governance Master. As opções de promoção incluem produção, temporariedade ou para não promoção para configuração de promoção manual.

      Para obter informações adicionais, consulte “Implementando Padrões” na página 61.
   d. Verifique a implementação. Consulte o “Verificando a Implementação” na página 67.

e. Proteja o ambiente do WSRR. Para obter mais informações sobre o planejamento e a configuração da segurança do WSRR, consulte o Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0.

f. Configure o domínio do DataPower provisionado. Para obter informações adicionais, consulte "Gerenciamento da Segurança" na página 54.

4. Use a instância implementada. Para obter informações adicionais, consulte Capítulo 6, "Trabalhando com a Instância Implementada", na página 91.

Fazendo Download e Instalando os Padrões

O IBM SOA Policy Gateway Pattern para uso com o IBM Workload Deployer Versão 3.1.0.2 ou o IBM PureApplication System é empacotado para download a partir do Passport Advantage.

Antes de Iniciar

Assegure-se de que existam 10 GB de espaço disponíveis para o arquivo `CI9G9ML.tar.gz` e um adicional de 10 - 14 GB para os arquivos extraídos.

O arquivo `CI9G9ML.tar.gz` deve ser transferido por download para um sistema que esteja executando Linux ou Microsoft Windows. O Java™ Runtime Environment (JRE) Versão 6 também deve ser instalado antes de iniciar a instalação do padrão. É possível fazer download dessa versão para Linux no endereço a seguir: http://www.ibm.com/developerworks/java/jdk/linux/download.html.

Sobre Esta Tarefa

O IBM SOA Policy Gateway Pattern está empacotado no arquivo `CI9G9ML.tar.gz`. Esse archive contém os arquivos open virtual archive (OVA), arquivos de pacote de scripts e arquivos de definição de padrão.

Procedimento

Para fazer download das imagens do IBM SOA Policy Gateway Pattern a partir do Passport Advantage, conclua as etapas a seguir:

1. Acesse o website do Passport Advantage: Passport Advantage.
2. Faça download do archive que contém as imagens, os padrões de scripts e os padrões a serem usados. O arquivo é nomeado `CI9G9ML.tar.gz`.
3. Abra um terminal no Linux ou uma janela de prompt de comandos no Windows e navegue para o diretório no qual o arquivo `CI9G9ML.tar.gz` foi transferido por download.
4. Extraia o conteúdo do arquivo `CI9G9ML.tar.gz` em seu sistema de arquivos local. No Linux, o comando de extração é: No Linux, o comando de extração é:

```
tar xvzf CI9G9ML.tar.gz
```

   No Windows, use o software de extração do archive adicional para extrair o conteúdo de `CI9G9ML.tar.gz`.
5. Assegure-se de que os arquivos extraídos a seguir tenham permissão de execução nos sistemas Linux:
   - `chmod a+x installer/installer`
   - `chmod a+x installer/deployer.cli/bin/deployer`
   - `chmod a+x installer/deployer.cli/bin/3.1.0.2-20120531075842/deployer`
6. Altere para o diretório `installer`:

```
cd installer
```

7. Para instalar o IBM SOA Policy Gateway Pattern no dispositivo em Nuvem, execute o instalador. O nome do comando é `installer.bat` no Microsoft Windows ou `installer` no Linux. Insira o comando a seguir: `installer -h <host> -u <username> -p <password>` em que `<host>` é o Dispositivo em Nuvem e username e password são as credenciais do Administrador em Nuvem. Por exemplo:

```
./installer -h apiliwd.rchland.ibm.com -u cbadmin -p cbadmin
```

8. Quando solicitado, aceite a licença do IBM SOA Policy Gateway Pattern.
   a. No Microsoft Windows: depois de aceitar o contrato de licença, se uma nova linha no terminal exibir `>>>`, digite `quit()` e pressione a tecla Enter. Repita a etapa 7.
9. Os padrões são importados. À medida que cada padrão é instalado, uma mensagem é exibida no instalador para indicar que ele foi instalado com êxito. Por exemplo:

```
Importando o Padrão "SOA Policy Gateway 2.0.0.0 - Governance Master" ...
Importação do padrão "SOA Policy Gateway 2.0.0.0 - Governance Master" bem-sucedida.
```

Resultados

Os padrões e scripts são carregados e os padrões de Sistema Virtual são criados.

Nota: Se um padrão de sistema virtual na versão correta usada no IBM SOA Policy Gateway Pattern já existir no catálogo, ele será sobrescrito.

O que Fazer Depois

Aceite licenças no dispositivo IBM Workload Deployer ou no IBM PureApplication System.

Para validar a instalação, consulte “Verificar o Padrão Instalado”.

Verificar o Padrão Instalado

É possível verificar se o padrão é instalado com êxito e aceitar as licenças necessárias para usar o padrão.

Antes de Iniciar

Assegure-se de que todas as etapas de “Fazendo Download e Instalando os Padrões” na página 12 estejam concluídas.

Sobre Esta Tarefa

Depois de instalar o padrão, é possível verificar a instalação do padrão. Para pode usar qualquer imagem virtual, você deve aceitar a licença necessária para ela.

Procedimento

Para verificar a instalação do IBM SOA Policy Gateway Pattern, conclua as etapas a seguir:

1. Efetue login no console do IPAS ou no console do IWD no host em que o padrão foi instalado.

2. Verifique as Imagens Virtuais navegando para `Catálogo -> Imagens Virtuais` e localize: DB2 9.7.5.0 e WebSphere Service Registry and Repository 8.0.0.1. Se uma licença não fora ceita, o ícone de imagem conterá uma caixa vermelha com uma cruz.
   a. Para aceitar uma licença, clique na imagem para visualizar seus detalhes. O status atual é exibido. Clique em **Aceitar** para o Contrato de Licença e, em seguida, clique em qualquer uma das licenças que devem ser aceitas antes que a imagem virtual possa ser usada. O status atual exibirá Somente Leitura e o Contrato de Licença exibirá Aceito quando concluído.
3. `Navegue para Catálogo -> Pacotes de Scripts` e localize:
   - SOA Policy Gateway 2.0.0.0 - Domínio do DataPower
   - SOA Policy Gateway 2.0.0.0 - Promoção
   - SOA Policy Gateway 2.0.0.0 - Amostra
   - SOA Policy Gateway 2.0.0.0 - Segurança

   Esses pacotes de scripts estão todos presentes em uma instalação bem-sucedida.
4. `Navegue para Padrões -> Sistemas Virtuais` e localize:
   - SOA Policy Gateway 2.0.0.0 - Advanced Runtime
   - SOA Policy Gateway 2.0.0.0 - Basic Runtime
   - SOA Policy Gateway 2.0.0.0 - Basic Runtime Sample
   - SOA Policy Gateway 2.0.0.0 - Governance Master

   Esses padrões estão todos presentes em uma instalação bem-sucedida.

Resultados

Você verificou a instalação do IBM SOA Policy Gateway Pattern.

O que Fazer Depois

Se você tiver uma instalação bem-sucedida, será possível acessar Capítulo 5, “Trabalhando com o IBM SOA Policy Gateway Pattern”, na página 51. Se sua instalação não foi bem-sucedida, repita a partir da etapa 7 do tópico “Fazendo Download e Instalando os Padrões” na página 12.

Configurando o Acesso de Usuário

Para permitir que os usuários acessem as imagens e os padrões no dispositivo, o administrador do dispositivo deve primeiro permitir o acesso de usuário. É possível criar os usuários primeiro e incluí-los no grupo ou criar o grupo primeiro e, em seguida, criar os usuários e incluí-los no grupo.

Sobre Esta Tarefa

Os usuários administrativos, geralmente o administrador do dispositivo, podem incluir outros usuários para acessar e administrar os padrões.

Procedimento

Para configurar o acesso de usuário, conclua as etapas a seguir:

1. Escolha uma das opções a seguir para configurar usuários e, opcionalmente, grupos de usuários:
   - Incluir e configurar um usuário a partir da janela Usuários da interface.

a. No menu, clique em **Sistema** > **Usuários**.
b. Clique no ícone **Incluir**.
c. Forneça um nome de usuário abreviado, bem como o nome real do usuário, endereço de email e senhas e clique em **OK**.
d. Selecione o usuário que você incluiu no painel Usuários para configurar o acesso. Configure o acesso e as ações do usuário que você selecionou.
e. Inclua o usuário em um ou mais grupos de usuários no campo **Grupos de Usuários**.

- Criar um grupo de usuários.
  a. No menu, clique em **Sistema** > **Grupos de Usuários**.
  b. Clique no ícone **Incluir**.Forneça um nome e uma descrição para o grupo.
  c. Selecione o grupo que você incluiu no painel Grupos de Usuários para configurar o acesso.
  d. Inclua os membros no campo **Membros do Grupo** e forneça as permissões para aplicar ao grupo.

2. Opcional: Se você já tiver incluído as imagens virtuais, forneça acesso às imagens virtuais para os usuários ou grupo. No menu, clique em **Catálogo** > **Imagens Virtuais** para abrir a janela Imagens Virtuais. Selecione uma imagem virtual do IBM SOA Policy Gateway Pattern do painel esquerdo e, em seguida, inclua os usuários ou grupo no painel direito.

O que Fazer Depois

Se você ainda não tiver incluído as imagens virtuais, inclua-as e, em seguida, forneça aos usuários ou grupo o acesso a elas.

Informações relacionadas:

IBM PureApplication System: Gerenciando Usuários e Grupos

IBM Workload Deployer: Gerenciando Usuários e Grupos

Capítulo 4. Padrões, Partes e Pacotes de Scripts

As partes do IBM SOA Policy Gateway Pattern são os componentes funcionais do padrão. Cada parte representa uma única máquina virtual. Um padrão fornece uma definição de topologia para implementação repetida que pode ser compartilhada.

Os padrões descrevem a função fornecida por cada máquina virtual em um sistema virtual. Cada função é identificada como uma parte no padrão. Os padrões herdam as características de suas partes associadas. Por exemplo, quando uma parte do WSRR é colocada em um padrão, que é, então, implementado, o resultado é uma máquina virtual que possui uma instância do WSRR em execução.

Partes

As partes descrevem os componentes que estão configurados em uma máquina virtual. Cada parte tem um conjunto de propriedades (parâmetros) que são usadas durante a implementação para ajudar a definir a configuração geral do sistema virtual. Quando você carrega as imagens do IBM SOA Policy Gateway Pattern no IBM Workload Deployer, as partes estão inclusas.

Padrões

O padrão IBM SOA Policy Gateway Pattern contém quatro padrões:

- SOA Policy Gateway Basic Runtime
- SOA Policy Gateway Basic Runtime Sample
- SOA Policy Gateway Advanced Runtime
- SOA Policy Gateway Governance Master

Para obter informações detalhadas sobre como usar o IBM Workload Deployer para acessar padrões existentes ou criar padrão customizado, consulte http://publib.boulder.ibm.com/infocenter/worlodep/v3r0m0/topic/com.ibm.worlodep.doc/welcome.html.

Padrões

Quando as imagens virtuais tiverem sido carregadas no IBM Workload Deployer ou IBM PureApplication System e o acesso adequado tiver sido designado aos usuários, os usuários podem começar a trabalhar com os padrões das imagens.

Os padrões fornecem uma topologia repetida que pode ser implementada em uma nuvem. Os padrões implementados são sistemas virtuais em execução na nuvem. Os padrões, quer sejam predefinidos ou criados, contêm partes. Algumas partes são necessárias para que o padrão funcione quando implementado na nuvem como um sistema virtual.

SOA Policy Gateway Basic Runtime

O SOA Policy Gateway Basic Runtime contém as partes necessárias a seguir:

- DB2 Enterprise
- Servidor Independente do WSRR

SOA Policy Gateway Basic Runtime Sample

O SOA Policy Gateway Basic Runtime Sample contém as partes necessárias a seguir:

- DB2 Enterprise
- Servidor Independente do WSRR

SOA Policy Gateway Advanced Runtime

O SOA Policy Gateway Advanced Runtime contém as partes necessárias a seguir:

- Gerenciador de Implementação do WSRR
- HADR Primário do DB2 Enterprise
- HADR de Espera do DB2 Enterprise
- Nó Customizado do WSRR

SOA Policy Gateway Governance Master

O SOA Policy Gateway Governance Master contém as partes necessárias a seguir:

- Gerenciador de Implementação do WSRR
- HADR Primário do DB2 Enterprise
- HADR de Espera do DB2 Enterprise
- Nó Customizado do WSRR

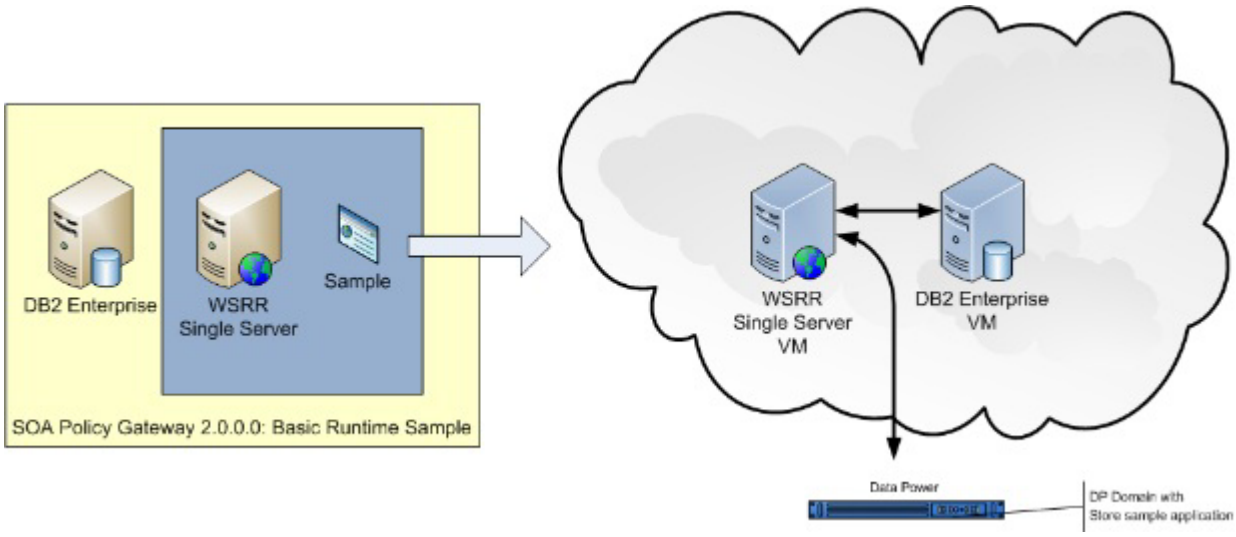
SOA Policy Gateway Basic Runtime Sample

O SOA Policy Gateway Basic Runtime Sample aprovisiona um SOA Policy Gateway Basic Runtime com uma interface de amostra e um aplicativo que demonstra as políticas atualmente suportadas nesta liberação.

O padrão SOA Policy Gateway Basic Runtime Sample requer as partes a seguir:

- Servidor Independente do WSRR
- DB2 Enterprise

O padrão SOA Policy Gateway Basic Runtime Sample instala um aplicativo de amostra no ambiente implementado. Ele instala o domínio de amostra no DataPower que implementa um serviço simples, instala o WSDL e políticas de amostra no WSRR para o serviço e fornece um aplicativo de teste para demonstrar as políticas forçadas. Para obter informações adicionais sobre o aplicativo de amostra, consulte “O Aplicativo de Amostra” na página 70. Ele instala o domínio de amostra no DataPower, instala o WSDL e Políticas de amostra no WSRR e demonstra várias políticas com relação a um serviço.



As políticas implementadas incluem:

Tabela 1. Políticas Inclusas no Basic Runtime com Padrão Sample

Tipo de política	Descrição
Criação de log	Com base em um ID de contexto de solicitações, registra a solicitação no DataPower.
Roteamento	Com base em um ID de contexto de solicitações, roteia a solicitação para um terminal especificado.
Validação	Valida a solicitação com relação ao WSDL de implementações de serviço.
Rejeição	Controla solicitações para um serviço com base na contagem de mensagens com as ações: rejeitar, enfileirar e outras.
Segurança AAA	Controla o acesso ao serviço usando autorização de usuário baseada em XACML. O XACML não é armazenado no WSRR.
Edição de Dados de Segurança	Edita dados de partes da mensagem de resposta com base no XACML. O XACML não é armazenado no WSRR.

Scripts e Opções Avançadas

O padrão SOA Policy Gateway Basic Runtime requer os scripts a seguir.

Na parte do Servidor Independente do WSRR:

- SOA Policy Gateway 2.0.0.0 - Amostra

Visualize a parte e os parâmetros de script:

- "Parâmetros de Configuração da Parte do DB2 Enterprise para o Padrão SOA Policy Gateway Basic Runtime Sample" na página 28
- "Parâmetros de Configuração da Parte de Servidor Independente do WSRR para o Padrão SOA Policy Gateway Basic Runtime Sample" na página 36
- "SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Amostra para o Padrão SOA Policy Gateway Basic Runtime Sample" na página 46

Conceitos relacionados:

"Parte do DB2 Enterprise" na página 26
A parte do DB2 Enterprise fornece algumas opções de configuração.

"Parte do Servidor Independente do WSRR" na página 35
A parte do Servidor Independente do WSRR fornece algumas opções de configuração.

"Script: SOA Policy Gateway 2.0.0.0 - Amostra" na página 44
O script de Amostra configura os parâmetros do aplicativo de amostra para serem usados com o padrão SOA Policy Gateway Basic Runtime Sample.

"O Aplicativo de Amostra" na página 70
O aplicativo de amostra é um Domínio do DataPower configurável e um conjunto de Artefatos do WSRR que podem ser usados para demonstrar os recursos do padrão.

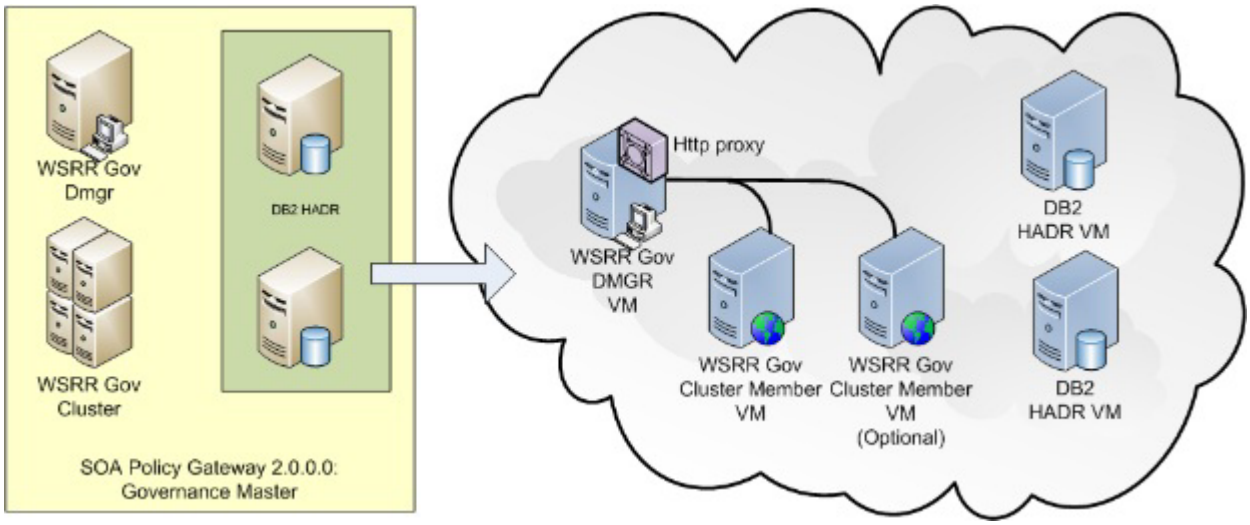
SOA Policy Gateway Governance Master

O padrão SOA Policy Gateway Governance Master fornece um ambiente de controle em cluster para criar e gerenciar serviços e políticas. O ambiente é aprovisionado com o Perfil de Ativação de Controle padrão do WSRR configurado. O Perfil de Ativação de Controle padrão suporta dois destinos de promoção, Temporariedade e Produção.

O padrão SOA Policy Gateway Governance Master requer as partes a seguir:

- HADR Primário do DB2
- HADR de Espera do DB2
- Gerenciador de Implementação do WSRR
- Nós Customizados do WSRR

Nota: O padrão Governance Master deve ser implementado antes de os padrões de tempo de execução serem implementados. Os parâmetros usados para configurar o padrão Governance Master são usados pelos padrões de tempo de execução para configurar ele mesmo com o Governance Master. Somente o padrão SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime pode ser configurado no Governance Master.



Scripts e Opções Avançadas

O padrão SOA Policy Gateway Governance Master requer os scripts a seguir:

- SOA Policy Gateway 2.0.0.0 - Segurança
- SOA Policy Gateway 2.0.0.0 - Promoção
- SOA Policy Gateway 2.0.0.0 - Domínio do DataPower

Visualize a parte e os parâmetros de script:

- "Parâmetros de Configuração da Parte de HADR Primário do DB2 Enterprise para o Padrão SOA Policy Gateway Governance Master pattern" na página 31
- "Parâmetros de Configuração da Parte de HADR de Espera do DB2 Enterprise para o Padrão SOA Policy Gateway Governance Master" na página 34
- "Parâmetros de Configuração da Parte de Gerenciador de Implementação do WSRR para o Padrão SOA Policy Gateway Governance Master" na página 38
- "Parâmetros de Configuração da Parte de Nós Customizados do WSRR para o Padrão SOA Policy Gateway Governance Master" na página 40

Usando o Padrão Governance como um Controle Principal

O padrão SOA Policy Gateway Governance Master é implementado com o Perfil de Ativação de Controle do WSRR padrão que inclui dois estágios de promoção, Temporariedade e Produção. Para obter informações adicionais sobre o Perfil de Ativação de Controle no WSRR, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Governance Enablement Profile. Os padrões SOA Policy Gateway Basic Runtime e SOA Policy Gateway Advanced Runtime podem ser implementados nessa integração como destinos de promoção. Para obter informações adicionais sobre como configurar isso, consulte "Cenário: Incluindo um Tempo de Execução Adicional ao Padrão" na página 68.

Conceitos relacionados:

"Parte de HADR Primário do DB2 Enterprise" na página 29
A parte de HADR Primário do DB2 Enterprise fornece algumas opções de configuração.

"Parte de HADR de Espera do DB2 Enterprise" na página 32
A parte de HADR de Espera do DB2 Enterprise fornece algumas opções de configuração.

"Parte do Gerenciador de Implementação do WSRR" na página 37
A parte do Gerenciador de Implementação do WSRR fornece algumas opções de configuração.

"Parte de Nós Customizados do WSRR" na página 39
A parte de Nós Customizados do WSRR fornece algumas opções de configuração.

Informações relacionadas:

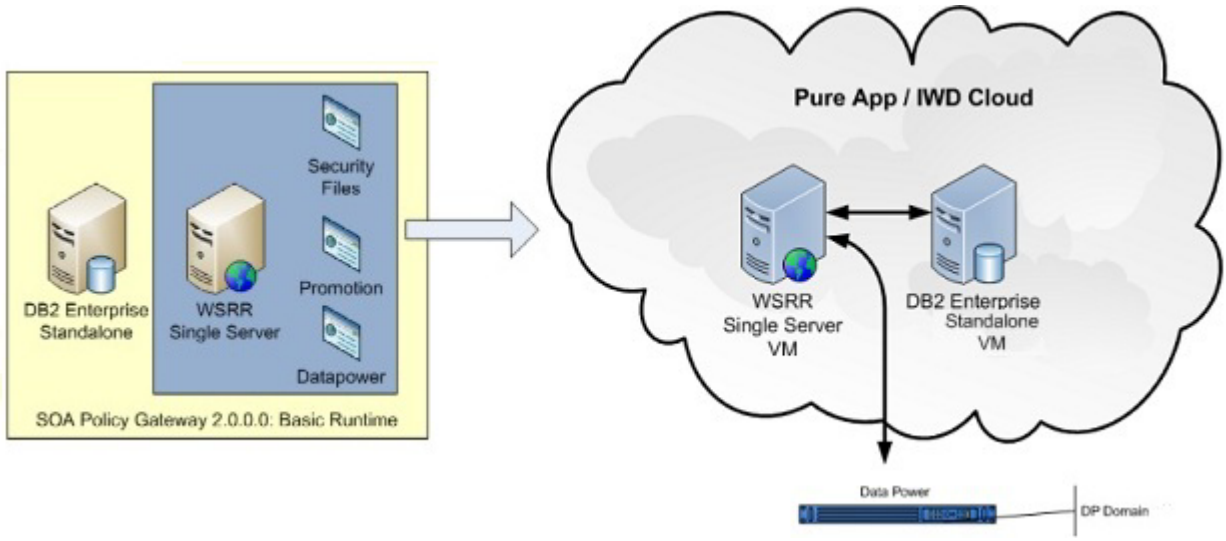
Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Governance Enablement Profile

SOA Policy Gateway Basic Runtime

O SOA Policy Gateway Basic Runtime fornece um meio simples de fornecer um tempo de execução que pode ser usado independente ou integrado a um padrão SOA Policy Gateway Governance Master implementado. O padrão SOA Policy Gateway Basic Runtime suporta a implementação de um domínio do DataPower que é configurado para se comunicar com o servidor de runtime WSRR aprovisionado no padrão.

O padrão SOA Policy Gateway Basic Runtime requer as partes a seguir:

- Servidor Independente do WSRR
- DB2 Enterprise



Scripts e Opções Avançadas

O padrão SOA Policy Gateway Basic Runtime requer os scripts a seguir.

Na parte do Servidor Independente do WSRR:

- SOA Policy Gateway 2.0.0.0 - Segurança
- SOA Policy Gateway 2.0.0.0 - Promoção
- SOA Policy Gateway 2.0.0.0 - Domínio do DataPower

Visualize a parte e os parâmetros de script:

- "Parâmetros de Configuração da Parte de Servidor Independente do WSRR para o Padrão SOA Policy Gateway Basic Runtime" na página 36
- "Parâmetros de Configuração da Parte do DB2 Enterprise para o Padrão SOA Policy Gateway Basic Runtime" na página 27
- "SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Segurança para o Padrão SOA Policy Gateway Basic Runtime" na página 48
- "SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Promoção para o Padrão SOA Policy Gateway Basic Runtime" na página 43
- "SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Domínio do DataPower para o Padrão SOA Policy Gateway Basic Runtime" na página 41

Promovendo o SOA Policy Gateway Basic Runtime a um Governance Runtime

Quando um padrão Advanced Runtime é configurado com um padrão Governance Master, ocorre o seguinte:

- A segurança de célula cruzada é configurada
- O arquivo `promotion.xml` no Governance Master é atualizado com os dados da implementação do Basic Runtime.

Para configurar a promoção, você deve escolher uma das opções de estágio a seguir:

- produção
- temporariedade
- outro ou Não Configurado

Essas opções são alinhadas com os níveis fornecidos pelo Perfil de Ativação de Controle no WSRR. Se o perfil de controle for diferente, "outro" será escolhido quando o perfil de controle Controles Principais for alterado. Para obter informações adicionais sobre o Perfil de Ativação de Controle no WSRR, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Governance Enablement Profile.

Conceitos relacionados:

"O Aplicativo de Amostra" na página 70
O aplicativo de amostra é um Domínio do DataPower configurável e um conjunto de Artefatos do WSRR que podem ser usados para demonstrar os recursos do padrão.

"Parte do DB2 Enterprise" na página 26
A parte do DB2 Enterprise fornece algumas opções de configuração.

"Parte do Servidor Independente do WSRR" na página 35
A parte do Servidor Independente do WSRR fornece algumas opções de configuração.

"Script: SOA Policy Gateway 2.0.0.0 - Segurança" na página 47
O script de Segurança copia as informações de segurança, contidas em um arquivo ZIP, necessárias para a comunicação com um dispositivo DataPower na máquina do Dmgr ou do WSRR a partir de um servidor de arquivos externo que suporta o secure copy program (SCP) do Linux.

"Script: SOA Policy Gateway 2.0.0.0 - Promoção" na página 43
O script de Promoção permite que um padrão SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime seja integrado com um padrão SOA Policy Gateway Governance Master pré-implementado. Ele estabelece uma segurança de célula cruzada entre os padrões Runtime e Governance, enquanto configura opcionalmente a promoção do WSRR no controle principal.

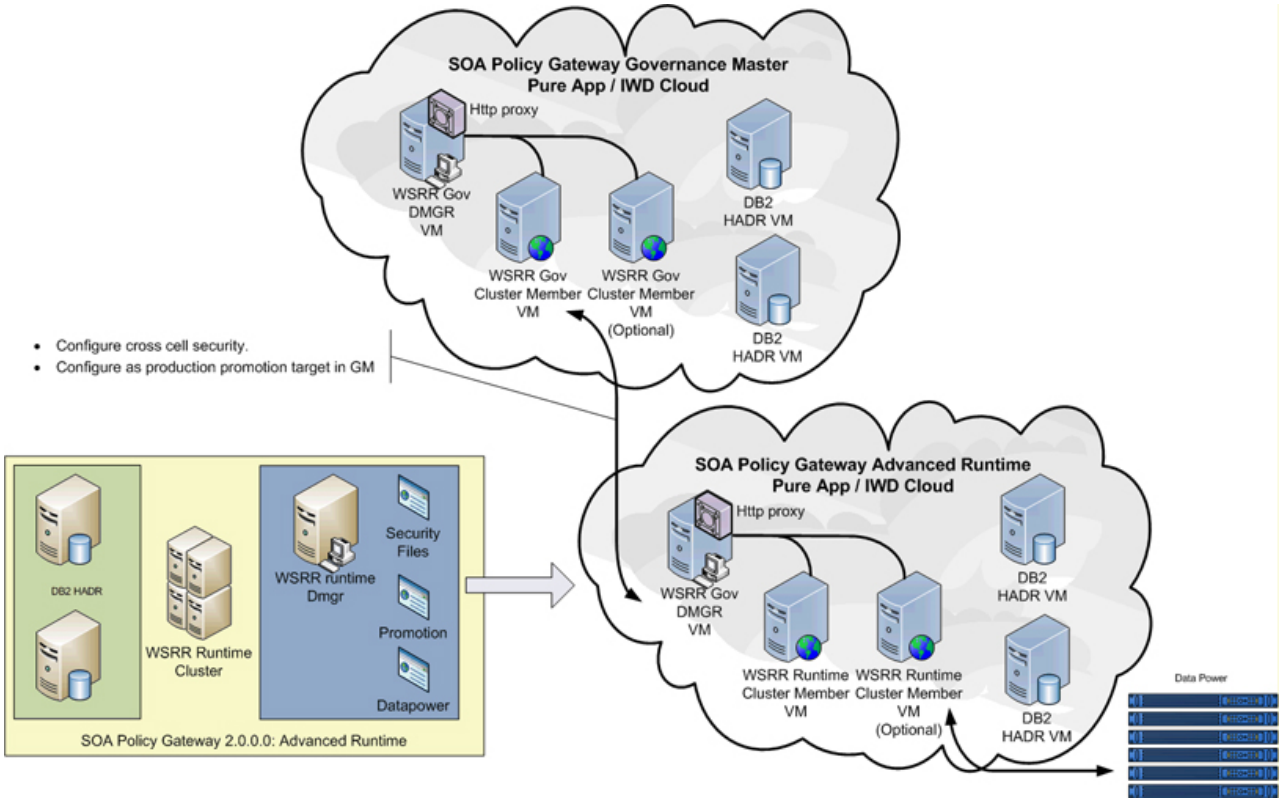
"Script: SOA Policy Gateway 2.0.0.0 - Domínio do DataPower" na página 41
O script de Domínio do DataPower aprovisiona o domínio do DataPower durante a implementação. O script configura a conexão entre um único domínio do DataPower e o tempo de execução do WSRR. Um script de Domínio do DataPower separado é necessário para cada domínio do DataPower que está conectado ao tempo de execução do WSRR.

SOA Policy Gateway Advanced Runtime

O SOA Policy Gateway Advanced Runtime inclui mais opções de alta disponibilidade e deve ser usado com o SOA Policy Gateway Governance Master.

O padrão SOA Policy Gateway Advanced Runtime requer as partes a seguir:

- HADR Primário do DB2
- HADR de Espera do DB2
- Gerenciador de Implementação do WSRR
- Nós Customizados do WSRR



Scripts e Opções Avançadas

O padrão SOA Policy Gateway Governance Master requer os scripts a seguir na parte do WSRR Deployment Manager:

- SOA Policy Gateway 2.0.0.0 - Segurança
- SOA Policy Gateway 2.0.0.0 - Promoção
- SOA Policy Gateway 2.0.0.0 - Domínio do DataPower (um por domínio do DataPower)

Visualize a parte e os parâmetros de script:

- "Parâmetros de Configuração da Parte de HADR Primário do DB2 Enterprise para o Padrão SOA Policy Gateway Advanced Runtime pattern" na página 30
- "Parâmetros de Configuração da Parte de HADR de Espera do DB2 Enterprise para o Padrão SOA Policy Gateway Advanced Runtime" na página 33
- "Parâmetros de Configuração da Parte de Gerenciador de Implementação do WSRR para o Padrão SOA Policy Gateway Advanced Runtime" na página 38
- "Parâmetros de Configuração da Parte de Nós Customizados do WSRR para o Padrão SOA Policy Gateway Advanced Runtime" na página 39
- "SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Segurança para o Padrão SOA Policy Gateway Advanced Runtime" na página 49
- "SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Promoção para o Padrão SOA Policy Gateway Advanced Runtime" na página 44
- "SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Domínio do DataPower para o Padrão SOA Policy Gateway Advanced Runtime" na página 42

Promovendo o SOA Policy Gateway Advanced Runtime a um Governance Runtime

Quando um padrão Advanced Runtime é configurado com um padrão Governance Master, ocorre o seguinte:

- A segurança de célula cruzada é configurada
- O arquivo `promotion.xml` no Governance Master é atualizado com os dados da implementação do Advanced Runtime.

Para configurar a promoção, você deve escolher uma das opções de estágio a seguir:

- produção
- temporariedade
- outro ou “Não Configurado”

Essas opções são alinhadas com os níveis fornecidos pelo Perfil de Ativação de Controle no WSRR. Se o perfil de controle no Governance Master foi alterado, use “outros” como o nível de promoção. Para obter informações adicionais sobre o Perfil de Ativação de Controle no WSRR, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Governance Enablement Profile.

Conceitos relacionados:

"Parte de HADR Primário do DB2 Enterprise" na página 29
A parte de HADR Primário do DB2 Enterprise fornece algumas opções de configuração.

"Parte de HADR de Espera do DB2 Enterprise" na página 32
A parte de HADR de Espera do DB2 Enterprise fornece algumas opções de configuração.

"Parte do Gerenciador de Implementação do WSRR" na página 37
A parte do Gerenciador de Implementação do WSRR fornece algumas opções de configuração.

"Parte de Nós Customizados do WSRR" na página 39
A parte de Nós Customizados do WSRR fornece algumas opções de configuração.

"Script: SOA Policy Gateway 2.0.0.0 - Segurança" na página 47
O script de Segurança copia as informações de segurança, contidas em um arquivo ZIP, necessárias para a comunicação com um dispositivo DataPower na máquina do Dmgr ou do WSRR a partir de um servidor de arquivos externo que suporta o secure copy program (SCP) do Linux.

"Script: SOA Policy Gateway 2.0.0.0 - Promoção" na página 43
O script de Promoção permite que um padrão SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime seja integrado com um padrão SOA Policy Gateway Governance Master pré-implementado. Ele estabelece uma segurança de célula cruzada entre os padrões Runtime e Governance, enquanto configura opcionalmente a promoção do WSRR no controle principal.

"Script: SOA Policy Gateway 2.0.0.0 - Domínio do DataPower" na página 41
O script de Domínio do DataPower aprovisiona o domínio do DataPower durante a implementação. O script configura a conexão entre um único domínio do DataPower e o tempo de execução do WSRR. Um script de Domínio do DataPower separado é necessário para cada domínio do DataPower que está conectado ao tempo de execução do WSRR.

Partes

As partes a seguir constituem o IBM SOA Policy Gateway Pattern.

Parte do DB2 Enterprise

A parte do DB2 Enterprise fornece algumas opções de configuração.

Os parâmetros configuráveis da imagem do sistema virtual do DB2 Enterprise 9.7.5 são descritos na tabela a seguir:

Tabela 2. Parâmetros Configuráveis

Nome do parâmetro	Descrição
CPUs virtuais	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	A quantia de memória alocada para essa máquina virtual, em megabytes.
Senha (db2inst1)	A senha para o ID do usuário db2inst1 do sistema operacional. Esse ID do usuário é usado como o proprietário da instalação da instância do DB2 e como o proprietário dos bancos de dados e esquemas.
Verificar senha	Verifica a senha do db2inst1.

Tabela 2. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Descrição
Senha (db2fenc1)	A senha para o ID do usuário usada para executar funções definidas pelo usuário (UDFs) e procedimentos armazenados fora do espaço de endereço usado pelo banco de dados DB2. O usuário protegido é um usuário sob o qual alguns procedimentos armazenados (procedimentos armazenados "protegidos") podem ser executados com autoridade de sistema operacional reduzida. Isso pode ajudar a evitar que procedimentos armazenados protegidos sobrescrevam arquivos de instância porque o sistema operacional evitará isso.
Verificar senha	Verifica a senha do db2fenc1.
Senha (dasusr1)	O ID do usuário para o usuário do DB2 Administration Server que é usado para executar o DB2 Administration Server em seu sistema. O usuário padrão é dasusr1 e o grupo padrão é dasadm1. O ID do usuário também é usado pelas ferramentas da GUI do DB2 para executar tarefas de administração com relação a bancos de dados e instâncias de bancos de dados do servidor local.
Verificar senha	Verifica a senha do dasusr1.
Senha (raiz)	A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Verifica a senha raiz.
Senha (virtuser)	A senha para o ID do usuário virtuser do sistema operacional. Esse ID do usuário é usado como um ID de usuário não raiz para a máquina virtual.
Verificar senha	Verifica a senha do virtuser.

Outros parâmetros são herdados do padrão de sistema virtual base e são bloqueados.

Parâmetros de Configuração da Parte do DB2 Enterprise para o Padrão SOA Policy Gateway Basic Runtime

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 3. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
CPUs virtuais	Sim	1	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	Sim	2048	A quantia de memória alocada para essa máquina virtual, em megabytes.
Senha (db2inst1)	Sim		A senha para o ID do usuário db2inst1 do sistema operacional. Esse ID do usuário é usado como o proprietário da instalação da instância do DB2 e como o proprietário dos bancos de dados e esquemas.
Verificar senha	Sim		Verifica a senha do db2inst1.

Tabela 3. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Necessário	Valor padrão	Descrição
Senha (db2fenc1)	Sim		A senha para o ID do usuário usada para executar funções definidas pelo usuário (UDFs) e procedimentos armazenados fora do espaço de endereço usado pelo banco de dados DB2. O usuário protegido é um usuário sob o qual alguns procedimentos armazenados (procedimentos armazenados "protegidos") podem ser executados com autoridade de sistema operacional reduzida. Isso pode ajudar a evitar que procedimentos armazenados protegidos sobrescrevam arquivos de instância porque o sistema operacional evitará isso.
Verificar senha	Sim		Verifica a senha do db2fenc1.
Senha (dasusr1)	Sim		O ID do usuário para o usuário do DB2 Administration Server que é usado para executar o DB2 Administration Server em seu sistema. O usuário padrão é dasusr1 e o grupo padrão é dasadm1. O ID do usuário também é usado pelas ferramentas da GUI do DB2 para executar tarefas de administração com relação a bancos de dados e instâncias de bancos de dados do servidor local.
Verificar senha	Sim		Verifica a senha do dasusr1.
Senha (raiz)	Sim		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Sim		Verifica a senha raiz.
Senha (virtuser)	Sim		A senha para o ID do usuário virtuser do sistema operacional. Esse ID do usuário é usado como um ID de usuário não raiz para a máquina virtual.
Verificar senha	Sim		Verifica a senha do virtuser.

Parâmetros de Configuração da Parte do DB2 Enterprise para o Padrão SOA Policy Gateway Basic Runtime Sample

No SOA Policy Gateway Basic Runtime Sample, os valores padrão são pré-configurados para todos os parâmetros.

Tabela 4. Parâmetros Configurados

Nome do parâmetro	Necessário	Valor padrão	Descrição
CPUs virtuais	Sim	1	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	Sim	2048	A quantia de memória alocada para essa máquina virtual, em megabytes.

Tabela 4. Parâmetros Configurados (continuação)

Nome do parâmetro	Necessário	Valor padrão	Descrição
Senha (db2inst1)	Sim	password	A senha para o ID do usuário db2inst1 do sistema operacional. Esse ID do usuário é usado como o proprietário da instalação da instância do DB2 e como o proprietário dos bancos de dados e esquemas.
Verificar senha	Sim	password	Verifica a senha do db2inst1.
Senha (db2fenc1)	Sim	password	A senha para o ID do usuário usada para executar funções definidas pelo usuário (UDFs) e procedimentos armazenados fora do espaço de endereço usado pelo banco de dados DB2. O usuário protegido é um usuário sob o qual alguns procedimentos armazenados (procedimentos armazenados "protegidos") podem ser executados com autoridade de sistema operacional reduzida. Isso pode ajudar a evitar que procedimentos armazenados protegidos sobrescrevam arquivos de instância porque o sistema operacional evitará isso.
Verificar senha	Sim	password	Verifica a senha do db2fenc1.
Senha (dasusr1)	Sim	password	O ID do usuário para o usuário do DB2 Administration Server que é usado para executar o DB2 Administration Server em seu sistema. O usuário padrão é dasusr1 e o grupo padrão é dasadm1. O ID do usuário também é usado pelas ferramentas da GUI do DB2 para executar tarefas de administração com relação a bancos de dados e instâncias de bancos de dados do servidor local.
Verificar senha	Sim	password	Verifica a senha do dasusr1.
Senha (raiz)	Sim	password	A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Sim	password	Verifica a senha raiz.
Senha (virtuser)	Sim	password	A senha para o ID do usuário virtuser do sistema operacional. Esse ID do usuário é usado como um ID de usuário não raiz para a máquina virtual.
Verificar senha	Sim	password	Verifica a senha do virtuser.

Parte de HADR Primário do DB2 Enterprise

A parte de HADR Primário do DB2 Enterprise fornece algumas opções de configuração.

Os parâmetros configuráveis da parte de HADR Primário do DB2 Enterprise são descritos na tabela a seguir:

Tabela 5. Parâmetros Configuráveis

Nome do parâmetro	Descrição
CPUs virtuais	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	A quantia de memória alocada para essa máquina virtual, em megabytes.
Senha (db2inst1)	A senha para o ID do usuário db2inst1 do sistema operacional. Esse ID do usuário é usado como o proprietário da instalação da instância do DB2 e como o proprietário dos bancos de dados e esquemas.
Verificar senha	Verifica a senha do db2inst1.
Senha (db2fenc1)	A senha para o ID do usuário usada para executar funções definidas pelo usuário (UDFs) e procedimentos armazenados fora do espaço de endereço usado pelo banco de dados DB2. O usuário protegido é um usuário sob o qual alguns procedimentos armazenados (procedimentos armazenados "protegidos") podem ser executados com autoridade de sistema operacional reduzida. Isso pode ajudar a evitar que procedimentos armazenados protegidos sobrescrevam arquivos de instância porque o sistema operacional evitará isso.
Verificar senha	Verifica a senha do db2fenc1.
Senha (dasusr1)	A senha do ID do usuário para o usuário do DB2 Administration Server que é usado para executar o DB2 Administration Server em seu sistema. O usuário padrão é dasusr1 e o grupo padrão é dasadm1. O ID do usuário também é usado pelas ferramentas da GUI do DB2 para executar tarefas de administração com relação a bancos de dados e instâncias de bancos de dados do servidor local.
Verificar senha	Verifica a senha do dasusr1.
Senha (raiz)	A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Verifica a senha raiz.
Senha (virtuser)	A senha para o ID do usuário virtuser do sistema operacional. Esse ID do usuário é usado como um ID de usuário não raiz para a máquina virtual.
Verificar senha	Verifica a senha do virtuser.

Outros parâmetros são herdados do padrão de sistema virtual base e são bloqueados.

Parâmetros de Configuração da Parte de HADR Primário do DB2 Enterprise para o Padrão SOA Policy Gateway Advanced Runtime pattern

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 6. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
CPUs virtuais	Sim	1	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	Sim	2048	A quantia de memória alocada para essa máquina virtual, em megabytes.
Senha (db2inst1)	Sim		A senha para o ID do usuário db2inst1 do sistema operacional. Esse ID do usuário é usado como o proprietário da instalação da instância do DB2 e como o proprietário dos bancos de dados e esquemas.
Verificar senha	Sim		Verifica a senha do db2inst1.

Tabela 6. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Necessário	Valor padrão	Descrição
Senha (db2fenc1)	Sim		A senha para o ID do usuário usada para executar funções definidas pelo usuário (UDFs) e procedimentos armazenados fora do espaço de endereço usado pelo banco de dados DB2. O usuário protegido é um usuário sob o qual alguns procedimentos armazenados (procedimentos armazenados "protegidos") podem ser executados com autoridade de sistema operacional reduzida. Isso pode ajudar a evitar que procedimentos armazenados protegidos sobrescrevam arquivos de instância porque o sistema operacional evitará isso.
Verificar senha	Sim		Verifica a senha do db2fenc1.
Senha (dasusr1)	Sim		A senha do ID do usuário para o usuário do DB2 Administration Server que é usado para executar o DB2 Administration Server em seu sistema. O usuário padrão é dasusr1 e o grupo padrão é dasadm1. O ID do usuário também é usado pelas ferramentas da GUI do DB2 para executar tarefas de administração com relação a bancos de dados e instâncias de bancos de dados do servidor local.
Verificar senha	Sim		Verifica a senha do dasusr1.
Senha (raiz)	Sim		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Sim		Verifica a senha raiz.
Senha (virtuser)	Sim		A senha para o ID do usuário virtuser do sistema operacional. Esse ID do usuário é usado como um ID de usuário não raiz para a máquina virtual.
Verificar senha	Sim		Verifica a senha do virtuser.

Parâmetros de Configuração da Parte de HADR Primário do DB2 Enterprise para o Padrão SOA Policy Gateway Governance Master pattern

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 7. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
CPUs virtuais	Sim	1	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	Sim	2048	A quantia de memória alocada para essa máquina virtual, em megabytes.

Tabela 7. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Necessário	Valor padrão	Descrição
Senha (db2inst1)	Sim		A senha para o ID do usuário db2inst1 do sistema operacional. Esse ID do usuário é usado como o proprietário da instalação da instância do DB2 e como o proprietário dos bancos de dados e esquemas.
Verificar senha	Sim		Verifica a senha do db2inst1.
Senha (db2fenc1)	Sim		A senha para o ID do usuário usada para executar funções definidas pelo usuário (UDFs) e procedimentos armazenados fora do espaço de endereço usado pelo banco de dados DB2. O usuário protegido é um usuário sob o qual alguns procedimentos armazenados (procedimentos armazenados "protegidos") podem ser executados com autoridade de sistema operacional reduzida. Isso pode ajudar a evitar que procedimentos armazenados protegidos sobrescrevam arquivos de instância porque o sistema operacional evitará isso.
Verificar senha	Sim		Verifica a senha do db2fenc1.
Senha (dasusr1)	Sim		A senha do ID do usuário para o usuário do DB2 Administration Server que é usado para executar o DB2 Administration Server em seu sistema. O usuário padrão é dasusr1 e o grupo padrão é dasadm1. O ID do usuário também é usado pelas ferramentas da GUI do DB2 para executar tarefas de administração com relação a bancos de dados e instâncias de bancos de dados do servidor local.
Verificar senha	Sim		Verifica a senha do dasusr1.
Senha (raiz)	Sim		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Sim		Verifica a senha raiz.
Senha (virtuser)	Sim		A senha para o ID do usuário virtuser do sistema operacional. Esse ID do usuário é usado como um ID de usuário não raiz para a máquina virtual.
Verificar senha	Sim		Verifica a senha do virtuser.

Parte de HADR de Espera do DB2 Enterprise

A parte de HADR de Espera do DB2 Enterprise fornece algumas opções de configuração.

Tabela 8. Parâmetros Configuráveis

Nome do parâmetro	Descrição
CPUs virtuais	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	A quantia de memória alocada para essa máquina virtual, em megabytes.
Senha (db2inst1)	A senha para o ID do usuário db2inst1 do sistema operacional. Esse ID do usuário é usado como o proprietário da instalação da instância do DB2 e como o proprietário dos bancos de dados e esquemas.
Verificar senha	Verifica a senha do db2inst1.
Senha (db2fenc1)	A senha para o ID do usuário usada para executar funções definidas pelo usuário (UDFs) e procedimentos armazenados fora do espaço de endereço usado pelo banco de dados DB2. O usuário protegido é um usuário sob o qual alguns procedimentos armazenados (procedimentos armazenados "protegidos") podem ser executados com autoridade de sistema operacional reduzida. Isso pode ajudar a evitar que procedimentos armazenados protegidos sobrescrevam arquivos de instância porque o sistema operacional evitará isso.
Verificar senha	Verifica a senha do db2fenc1.
Senha (dasusr1)	A senha do ID do usuário para o usuário do DB2 Administration Server que é usado para executar o DB2 Administration Server em seu sistema. O usuário padrão é dasusr1 e o grupo padrão é dasadm1. O ID do usuário também é usado pelas ferramentas da GUI do DB2 para executar tarefas de administração com relação a bancos de dados e instâncias de bancos de dados do servidor local.
Verificar senha	Verifica a senha do dasusr1.
Senha (raiz)	A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Verifica a senha raiz.
Senha (virtuser)	A senha para o ID do usuário virtuser do sistema operacional. Esse ID do usuário é usado como um ID de usuário não raiz para a máquina virtual.
Verificar senha	Verifica a senha do virtuser.

Outros parâmetros são herdados do padrão de sistema virtual base e são bloqueados.

Parâmetros de Configuração da Parte de HADR de Espera do DB2 Enterprise para o Padrão SOA Policy Gateway Advanced Runtime

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 9. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
CPUs virtuais	Sim	1	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	Sim	2048	A quantia de memória alocada para essa máquina virtual, em megabytes.
Senha (db2inst1)	Sim		A senha para o ID do usuário db2inst1 do sistema operacional. Esse ID do usuário é usado como o proprietário da instalação da instância do DB2 e como o proprietário dos bancos de dados e esquemas.
Verificar senha	Sim		Verifica a senha do db2inst1.

Tabela 9. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Necessário	Valor padrão	Descrição
Senha (db2fenc1)	Sim		A senha para o ID do usuário usada para executar funções definidas pelo usuário (UDFs) e procedimentos armazenados fora do espaço de endereço usado pelo banco de dados DB2. O usuário protegido é um usuário sob o qual alguns procedimentos armazenados (procedimentos armazenados "protegidos") podem ser executados com autoridade de sistema operacional reduzida. Isso pode ajudar a evitar que procedimentos armazenados protegidos sobrescrevam arquivos de instância porque o sistema operacional evitará isso.
Verificar senha	Sim		Verifica a senha do db2fenc1.
Senha (dasusr1)	Sim		A senha do ID do usuário para o usuário do DB2 Administration Server que é usado para executar o DB2 Administration Server em seu sistema. O usuário padrão é dasusr1 e o grupo padrão é dasadm1. O ID do usuário também é usado pelas ferramentas da GUI do DB2 para executar tarefas de administração com relação a bancos de dados e instâncias de bancos de dados do servidor local.
Verificar senha	Sim		Verifica a senha do dasusr1.
Senha (raiz)	Sim		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Sim		Verifica a senha raiz.
Senha (virtuser)	Sim		A senha para o ID do usuário virtuser do sistema operacional. Esse ID do usuário é usado como um ID de usuário não raiz para a máquina virtual.
Verificar senha	Sim		Verifica a senha do virtuser.

Parâmetros de Configuração da Parte de HADR de Espera do DB2 Enterprise para o Padrão SOA Policy Gateway Governance Master

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 10. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
CPUs virtuais	Sim	1	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	Sim	2048	A quantia de memória alocada para essa máquina virtual, em megabytes.

Tabela 10. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Necessário	Valor padrão	Descrição
Senha (db2inst1)	Sim		A senha para o ID do usuário db2inst1 do sistema operacional. Esse ID do usuário é usado como o proprietário da instalação da instância do DB2 e como o proprietário dos bancos de dados e esquemas.
Verificar senha	Sim		Verifica a senha do db2inst1.
Senha (db2fenc1)	Sim		A senha para o ID do usuário usada para executar funções definidas pelo usuário (UDFs) e procedimentos armazenados fora do espaço de endereço usado pelo banco de dados DB2. O usuário protegido é um usuário sob o qual alguns procedimentos armazenados (procedimentos armazenados "protegidos") podem ser executados com autoridade de sistema operacional reduzida. Isso pode ajudar a evitar que procedimentos armazenados protegidos sobrescrevam arquivos de instância porque o sistema operacional evitará isso.
Verificar senha	Sim		Verifica a senha do db2fenc1.
Senha (dasusr1)	Sim		A senha do ID do usuário para o usuário do DB2 Administration Server que é usado para executar o DB2 Administration Server em seu sistema. O usuário padrão é dasusr1 e o grupo padrão é dasadm1. O ID do usuário também é usado pelas ferramentas da GUI do DB2 para executar tarefas de administração com relação a bancos de dados e instâncias de bancos de dados do servidor local.
Verificar senha	Sim		Verifica a senha do dasusr1.
Senha (raiz)	Sim		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Sim		Verifica a senha raiz.
Senha (virtuser)	Sim		A senha para o ID do usuário virtuser do sistema operacional. Esse ID do usuário é usado como um ID de usuário não raiz para a máquina virtual.
Verificar senha	Sim		Verifica a senha do virtuser.

Parte do Servidor Independente do WSRR

A parte do Servidor Independente do WSRR fornece algumas opções de configuração.

Os parâmetros configuráveis da parte do Servidor Independente do WSRR são descritos na tabela a seguir:

Tabela 11. Parâmetros Configurados

Nome do parâmetro	Descrição
CPUs virtuais	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	A quantia de memória alocada para essa máquina virtual, em megabytes.
Senha (raiz)	A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Verifica a entrada do usuário para Senha (raiz).
Nome de usuário administrativo do WebSphere	O nome de usuário administrativo do ambiente WebSphere.
Senha administrativa do WebSphere	A senha de usuário administrativo do ambiente WebSphere.
Verificar senha	Verifica a entrada do usuário para a senha administrativa do WebSphere.
Reservar memória física	A memória física reservada para uso exclusivo por essa máquina virtual.

Outros parâmetros são herdados do padrão de sistema virtual base e são bloqueados.

Parâmetros de Configuração da Parte de Servidor Independente do WSRR para o Padrão SOA Policy Gateway Basic Runtime

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 12. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
CPUs virtuais	Sim	1	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	Sim	4096	A quantia de memória alocada para essa máquina virtual, em megabytes.
Reservar memória física	Sim	Falso	A memória física reservada para uso exclusivo por essa máquina virtual.
Nome da célula	Sim	SOAPolicyBasicCell	O nome da célula do WebSphere na máquina virtual no padrão Basic Runtime.
Nome do Nó	Sim	SOAPolicyBasicNode	O nome do nó do WebSphere na máquina virtual no padrão Basic Runtime.
Senha (raiz)	Sim		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Sim		Verifica a entrada do usuário para Senha (raiz).
Nome de usuário administrativo do WebSphere	Sim	virtuser	O nome de usuário administrativo do ambiente WebSphere.
Senha administrativa do WebSphere	Sim		A senha de usuário administrativo do ambiente WebSphere.
Verificar senha	Sim		Verifica a entrada do usuário para a senha administrativa do WebSphere.

Parâmetros de Configuração da Parte de Servidor Independente do WSRR para o Padrão SOA Policy Gateway Basic Runtime Sample

No SOA Policy Gateway Basic Runtime Sample, os valores padrão são pré-configurados para todos os parâmetros.

Tabela 13. Parâmetros Configurados

Nome do parâmetro	Necessário	Valor padrão	Descrição
CPUs virtuais	Sim	1	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	Sim	4096	A quantia de memória alocada para essa máquina virtual, em megabytes.
Reservar memória física	Sim	Falso	A memória física reservada para uso exclusivo por essa máquina virtual.
Senha (raiz)	Sim	password	A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Sim	password	Verifica a entrada do usuário para Senha (raiz).
Nome de usuário administrativo do WebSphere	Sim	virtuser	O nome de usuário administrativo do ambiente WebSphere.
Senha administrativa do WebSphere	Sim	password	A senha de usuário administrativo do ambiente WebSphere.
Verificar senha	Sim	password	Verifica a entrada do usuário para a senha administrativa do WebSphere.

Parte do Gerenciador de Implementação do WSRR

A parte do Gerenciador de Implementação do WSRR fornece algumas opções de configuração.

Os parâmetros configuráveis da parte do Gerenciador de Implementação do WSRR são descritos na tabela a seguir:

Tabela 14. Parâmetros Configuráveis

Nome do parâmetro	Descrição
CPUs virtuais	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	A quantia de memória alocada para essa máquina virtual, em megabytes.
Reservar CPUs físicas	As CPUs físicas reservadas para uso exclusivo por essa máquina virtual.
Reservar memória física	A memória física reservada para uso exclusivo por essa máquina virtual.
Nome da célula	O nome da célula do WebSphere para o padrão Advanced Runtime.
Nome do Nó	O nome do nó para o nó do WebSphere que reside na máquina virtual do Gerenciador de Implementação no padrão Advanced Runtime.
Senha (raiz)	A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Verifica a entrada do usuário para Senha (raiz).
Nome de usuário administrativo do WebSphere	O nome de usuário administrativo do ambiente WebSphere.
Senha administrativa do WebSphere	A senha de usuário administrativo do ambiente WebSphere.
Verificar senha	Verifica a entrada do usuário para a senha administrativa do WebSphere.

Outros parâmetros são herdados do padrão de sistema virtual base e são bloqueados.

Parâmetros de Configuração da Parte de Gerenciador de Implementação do WSRR para o Padrão SOA Policy Gateway Advanced Runtime

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 15. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
CPUs virtuais	Sim	1	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	Sim	2048	A quantia de memória alocada para essa máquina virtual, em megabytes.
Reservar CPUs físicas	Sim	Falso	As CPUs físicas reservadas para uso exclusivo por essa máquina virtual.
Reservar memória física	Sim	Falso	A memória física reservada para uso exclusivo por essa máquina virtual.
Nome da célula	Sim	SOAPolicyAdvancedCell	O nome da célula do WebSphere para o padrão Advanced Runtime.
Nome do Nó	Sim	SOAPolicyAdvancedNode	O nome do nó para o nó do WebSphere que reside na máquina virtual do Gerenciador de Implementação no padrão Advanced Runtime.
Senha (raiz)	Sim		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Sim		Verifica a entrada do usuário para Senha (raiz).
Nome de usuário administrativo do WebSphere	Sim	virtuser	O nome de usuário administrativo do ambiente WebSphere.
Senha administrativa do WebSphere	Sim		A senha de usuário administrativo do ambiente WebSphere.
Verificar senha	Sim		Verifica a entrada do usuário para a senha administrativa do WebSphere.

Parâmetros de Configuração da Parte de Gerenciador de Implementação do WSRR para o Padrão SOA Policy Gateway Governance Master

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 16. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
CPUs virtuais	Sim	1	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	Sim	2048	A quantia de memória alocada para essa máquina virtual, em megabytes.
Reservar CPUs físicas	Sim	Falso	As CPUs físicas reservadas para uso exclusivo por essa máquina virtual.
Reservar memória física	Sim	Falso	A memória física reservada para uso exclusivo por essa máquina virtual.
Nome da célula	Sim	SOAPolicyGMCell	O nome da célula do WebSphere para o padrão Advanced Runtime.

Tabela 16. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Necessário	Valor padrão	Descrição
Nome do Nó	Sim	SOAPolicyGMNode	O nome do nó para o nó do WebSphere que reside na máquina virtual do Gerenciador de Implementação no padrão Advanced Runtime.
Senha (raiz)	Sim		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Sim		Verifica a entrada do usuário para Senha (raiz).
Nome de usuário administrativo do WebSphere	Sim	virtuser	O nome de usuário administrativo do ambiente WebSphere.
Senha administrativa do WebSphere	Sim		A senha de usuário administrativo do ambiente WebSphere.
Verificar senha	Sim		Verifica a entrada do usuário para a senha administrativa do WebSphere.

Parte de Nós Customizados do WSRR

A parte de Nós Customizados do WSRR fornece algumas opções de configuração.

Os parâmetros configuráveis da parte de Nós Customizados do WSRR são descritos na tabela a seguir:

Tabela 17. Parâmetros Configuráveis

Nome do parâmetro	Descrição
CPUs virtuais	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	A quantia de memória alocada para essa máquina virtual, em megabytes.
Reservar CPUs físicas	As CPUs físicas reservadas para uso exclusivo por essa máquina virtual.
Reservar memória física	A memória física reservada para uso exclusivo por essa máquina virtual.
Nome da célula	O valor do nome da célula na configuração da parte de Nó Customizado é ignorado. O nome da célula especificado na configuração da parte do Gerenciador de Implementação é usado.
Nome do Nó	O nome do nó para o nó do WebSphere que reside na máquina virtual do Nó Customizado no padrão Advanced Runtime.
Senha (raiz)	A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Verifica a entrada do usuário para Senha (raiz).
Nome de usuário administrativo do WebSphere	O nome de usuário administrativo do ambiente WebSphere.
Senha administrativa do WebSphere	A senha de usuário administrativo do ambiente WebSphere.
Verificar senha	Verifica a entrada do usuário para a senha administrativa do WebSphere.

Outros parâmetros são herdados do padrão de sistema virtual base e são bloqueados.

Parâmetros de Configuração da Parte de Nós Customizados do WSRR para o Padrão SOA Policy Gateway Advanced Runtime

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 18. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
CPUs virtuais	Sim	2	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	Sim	4096	A quantia de memória alocada para essa máquina virtual, em megabytes.
Reservar CPUs físicas	Sim	Falso	As CPUs físicas reservadas para uso exclusivo por essa máquina virtual.
Reservar memória física	Sim	Falso	A memória física reservada para uso exclusivo por essa máquina virtual.
Nome do Nó	Sim	SOAPolicyAdvancedNode	O nome do nó para o nó do WebSphere que reside na máquina virtual do Nó Customizado no padrão Advanced Runtime.
Senha (raiz)	Sim		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Sim		Verifica a entrada do usuário para Senha (raiz).
Nome de usuário administrativo do WebSphere	Sim	virtuser	O nome de usuário administrativo do ambiente WebSphere.
Senha administrativa do WebSphere	Sim		A senha de usuário administrativo do ambiente WebSphere.
Verificar senha	Sim		Verifica a entrada do usuário para a senha administrativa do WebSphere.

Parâmetros de Configuração da Parte de Nós Customizados do WSRR para o Padrão SOA Policy Gateway Governance Master

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 19. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
CPUs virtuais	Sim	2	O número de processadores virtuais alocados para a máquina virtual representada por essa parte.
Tamanho da memória (MB)	Sim	4096	A quantia de memória alocada para essa máquina virtual, em megabytes.
Reservar CPUs físicas	Sim	Falso	As CPUs físicas reservadas para uso exclusivo por essa máquina virtual.
Reservar memória física	Sim	Falso	A memória física reservada para uso exclusivo por essa máquina virtual.
Nome do Nó	Sim	SOAPolicyGMNode	O nome do nó para o nó do WebSphere que reside na máquina virtual do Nó Customizado no padrão Advanced Runtime.
Senha (raiz)	Sim		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual representada por esta parte no padrão.
Verificar senha	Sim		Verifica a entrada do usuário para Senha (raiz).

Tabela 19. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Necessário	Valor padrão	Descrição
Nome de usuário administrativo do WebSphere	Sim	virtuser	O nome de usuário administrativo do ambiente WebSphere.
Senha administrativa do WebSphere	Sim		A senha de usuário administrativo do ambiente WebSphere.
Verificar senha	Sim		Verifica a entrada do usuário para a senha administrativa do WebSphere.

Pacotes de Scripts

Há 4 pacotes de scripts fornecidos com o IBM SOA Policy Gateway Pattern.

Os pacotes de scripts inclusos com este padrão são:

- SOA Policy Gateway 2.0.0.0 - Domínio do DataPower
- SOA Policy Gateway 2.0.0.0 - Promoção
- SOA Policy Gateway 2.0.0.0 - Amostras
- SOA Policy Gateway 2.0.0.0 - Segurança

Script: SOA Policy Gateway 2.0.0.0 - Domínio do DataPower

O script de Domínio do DataPower aprovisiona o domínio do DataPower durante a implementação. O script configura a conexão entre um único domínio do DataPower e o tempo de execução do WSRR. Um script de Domínio do DataPower separado é necessário para cada domínio do DataPower que está conectado ao tempo de execução do WSRR.

Parâmetros

Tabela 20. Parâmetros Configuráveis

Nome do parâmetro	Descrição
DataPower_hostname	O nome do host do dispositivo DataPower no qual o aplicativo de amostra será instalado.
DataPower_XML_mgmt_port	A porta usada para a Interface de Gerenciamento XML do DataPower, geralmente 5550.
Datapower_admin_id	O ID de usuário administrador com permissões apropriadas para usar a Interface de Gerenciamento XML.
DataPower_admin_password	A senha para o DataPower_admin_id.
Verificar senha	Verifica a entrada do usuário para DataPower_admin_password.
New_DataPower_domain	O novo nome de domínio a ser criado no dispositivo DataPower. Ele não deve corresponder a nenhum domínio existente ou ocorrerá falha ou saída do pacote de scripts. O valor não pode conter espaços.
securityFileCleanUp	Determina se o arquivo `DomainZipFile.zip` e o Certificado do WSRR transferido por upload para DataPower são excluídos da instância do WSRR em que os pacotes de scripts são executados. Se esse arquivo não for removido, será uma exposição de segurança se os certificados continuarem na instância.

SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Domínio do DataPower para o Padrão SOA Policy Gateway Basic Runtime

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 21. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
DataPower_hostname	Sim		O nome do host do dispositivo DataPower no qual o aplicativo de amostra será instalado.
DataPower_XML_mgmt_port	Sim	5550	A porta usada para a Interface de Gerenciamento XML do DataPower, geralmente 5550.
Datapower_admin_id	Sim		O ID de usuário administrador com permissões apropriadas para usar a Interface de Gerenciamento XML.
DataPower_admin_password	Sim		A senha para o DataPower_admin_id.
Verificar senha	Sim		Verifica a entrada do usuário para DataPower_admin_password.
New_DataPower_domain	Sim		O novo nome de domínio a ser criado no dispositivo DataPower. Ele não deve corresponder a nenhum domínio existente ou ocorrerá falha ou saída do pacote de scripts. O valor não pode conter espaços.
Remove_security_files	Sim	true	Determina se o arquivo `DomainZipFile.zip` e o Certificado do WSRR transferido por upload para DataPower são excluídos da instância do WSRR em que os pacotes de scripts são executados. Se esse arquivo não for removido, será uma exposição de segurança se os certificados continuarem na instância.

SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Domínio do DataPower para o Padrão SOA Policy Gateway Advanced Runtime

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 22. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
DataPower_hostname	Sim		O nome do host do dispositivo DataPower no qual o aplicativo de amostra será instalado.
DataPower_XML_mgmt_port	Sim	5550	A porta usada para a Interface de Gerenciamento XML do DataPower, geralmente 5550.
Datapower_admin_id	Sim		O ID de usuário administrador com permissões apropriadas para usar a Interface de Gerenciamento XML.
DataPower_admin_password	Sim		A senha para o DataPower_admin_id.
Verificar senha	Sim		Verifica a entrada do usuário para DataPower_admin_password.
New_DataPower_domain	Sim		O novo nome de domínio a ser criado no dispositivo DataPower. Ele não deve corresponder a nenhum domínio existente ou ocorrerá falha ou saída do pacote de scripts. O valor não pode conter espaços.

Tabela 22. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Necessário	Valor padrão	Descrição
Remove_security_files	Sim	true	Determina se o arquivo `DomainZipFile.zip` e o Certificado do WSRR transferido por upload para DataPower são excluídos da instância do WSRR em que os pacotes de scripts são executados. Se esse arquivo não for removido, será uma exposição de segurança se os certificados continuarem na instância.

Script: SOA Policy Gateway 2.0.0.0 - Promoção

O script de Promoção permite que um padrão SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime seja integrado com um padrão SOA Policy Gateway Governance Master pré-implementado. Ele estabelece uma segurança de célula cruzada entre os padrões Runtime e Governance, enquanto configura opcionalmente a promoção do WSRR no controle principal.

Parâmetros

Tabela 23. Parâmetros Configuráveis

Nome do parâmetro	Descrição
WSRR_GOV_DMGR_hostname	O nome do host do Dmgr para o Cluster do WSRR.
WSRR_GOV_DMGR_cellname	O Nome da Célula do WebSphere para o Cluster do WSRR.
WSRR_GOV_admin_user	O ID de Administrador para a Célula de Controle do WebSphere WSRR.
WSRR_GOV_admin_password	A senha do ID de Administrador para a Célula de Controle do WebSphere WSRR.
Verificar senha	Verifica a entrada do usuário para WSRR_GOV_admin_password.
Promotion_environment	Deve ser temporariedade, produção ou Não configurado. Esses valores fazem distinção entre maiúsculas e minúsculas e devem corresponder exatamente.
LTPA_key_password	Uma Chave LTPA é exportada e usada durante o Pacote de Scripts que é do Governance Master e é usada entre todas as CÉLULAS no ambiente de promoção. Esta é a senha usada ao exportar essa chave LTPA.
Verificar senha	Verifica a entrada do usuário para LTPA_key_password.

SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Promoção para o Padrão SOA Policy Gateway Basic Runtime

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 24. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
WSRR_GOV_DMGR_hostname	Sim		O nome do host do Dmgr para o Cluster do WSRR.
WSRR_GOV_DMGR_cellname	Sim		O Nome da Célula do WebSphere para o Cluster do WSRR.
WSRR_GOV_admin_user	Sim		O ID de Administrador para a Célula de Controle do WebSphere WSRR.
WSRR_GOV_admin_password	Sim		A senha do ID de Administrador para a Célula de Controle do WebSphere WSRR.
Verificar senha	Sim		Verifica a entrada do usuário para WSRR_GOV_admin_password.

Tabela 24. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Necessário	Valor padrão	Descrição
Promotion_environment	Sim		Deve ser temporariedade, produção ou Não configurado. Esses valores fazem distinção entre maiúsculas e minúsculas e devem corresponder exatamente.
LTPA_key_password	Sim		Uma Chave LTPA é exportada e usada durante o Pacote de Scripts que é do Governance Master e é usada entre todas as CÉLULAS no ambiente de promoção. Esta é a senha usada ao exportar essa chave LTPA.
Verificar senha	Sim		Verifica a entrada do usuário para LTPA_key_password.

SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Promoção para o Padrão SOA Policy Gateway Advanced Runtime

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 25. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
WSRR_GOV_DMGR_hostname	Sim		O nome do host do Dmgr para o Cluster do WSRR.
WSRR_GOV_DMGR_cellname	Sim		O Nome da Célula do WebSphere para o Cluster do WSRR.
WSRR_GOV_admin_user	Sim		O ID de Administrador para a Célula de Controle do WebSphere WSRR.
WSRR_GOV_admin_password	Sim		A senha do ID de Administrador para a Célula de Controle do WebSphere WSRR.
Verificar senha	Sim		Verifica a entrada do usuário para WSRR_GOV_admin_password.
Promotion_environment	Sim		Deve ser temporariedade, produção ou Não configurado. Esses valores fazem distinção entre maiúsculas e minúsculas e devem corresponder exatamente.
LTPA_key_password	Sim		Uma Chave LTPA é exportada e usada durante o Pacote de Scripts que é do Governance Master e é usada entre todas as CÉLULAS no ambiente de promoção. Esta é a senha usada ao exportar essa chave LTPA.
Verificar senha	Sim		Verifica a entrada do usuário para LTPA_key_password.

Script: SOA Policy Gateway 2.0.0.0 - Amostra

O script de Amostra configura os parâmetros do aplicativo de amostra para serem usados com o padrão SOA Policy Gateway Basic Runtime Sample.

Parâmetros

Nota: Qualquer parâmetro que requeira o valor Não Configurado faz distinção entre maiúsculas e minúsculas.

Tabela 26. Parâmetros Configuráveis

Nome do parâmetro	Descrição
SCP_host	O nome do host do Servidor SCP que contém o `DomainZipFile.zip`.
SCP_user	O nome de usuário a ser usado para se conectar ao Servidor SCP.
SCP_password	A senha a ser usada para efetuar login no Servidor SCP.
Verificar senha	Verifica a entrada do usuário para SCP_password.
SCP_zip_location	O local de URI do `DomainZipFile.zip`. Por exemplo, `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	O nome do Arquivo de Certificados do PEM usado para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Use o valor “Não Configurado” apenas para Autenticação de Servidor e não para usar o SSL.
CLIENT_PUBLIC _KEY_password	A senha para o Certificado Público usado para se conectar à porta Interface de Gerenciamento XML de Dispositivos DataPower. O valor será “Não Configurado” se nenhuma senha for usada.
Verificar senha	Verifica a entrada do usuário para CLIENT_PUBLIC_KEY_password.
CLIENT_PRIVATE_KEY_file	O nome do Arquivo-chave do PEM usado para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Isto é requerido para Autenticação Mútua. Use o valor “Não Configurado” apenas para Autenticação de Servidor e não para usar o SSL.
CLIENT_PRIVATE_KEY_password	A senha do arquivo-chave usada para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Isto é requerido para Autenticação Mútua. O valor será “Não Configurado” se nenhuma senha for usada.
Verificar senha	Verifica a entrada do usuário para CLIENT_PRIVATE_KEY_password.
CLI_FILE_file	O nome do arquivo de CLI contido no arquivo `DomainZipFile.zip`. Essa CLI é executada no final da instalação do Domínio e da Configuração do WSRR Server.
Verificar senha	Verifica a entrada do usuário para LTPA_KEY_password.
DataPower_hostname	O nome do host do dispositivo DataPower no qual o aplicativo de amostra será instalado.
DataPower_XML_mgmt_port	A porta usada para a Interface de Gerenciamento XML do DataPower.
DataPower_admin_id	O ID de usuário administrador com permissões apropriadas para usar a Interface de Gerenciamento XML.
DataPower_admin_password	A senha para o DataPower_admin_id.
Verificar senha	Verifica a entrada do usuário para DataPower_admin_password.
SOAPolicySample_DataPower_domain	O nome de domínio da amostra. Ele não deve corresponder a nenhum domínio existente no dispositivo DataPower.
SamplePolicySample_starting_port	O aplicativo requer 5 portas livres, que serão usadas sequencialmente a partir desse valor. Por exemplo, se o valor for 62000, as portas 62000-62004 serão usadas. Nenhuma verificação é feita pelo script para saber se portas estão livres.
LDAP_hostname	A amostra usa um servidor LDAP, este é o nome do host desse servidor.
LDAP_port	A porta não segura do servidor LDAP. Geralmente, 389.
LDAP_password	A senha usada na ligação com o LDAP_DN.

Tabela 26. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Descrição
Verificar senha	Verifica a entrada do usuário para LDAP_password.
LDAP_DN	O nome distinto usado para ligação com o LDAP. POr exemplo, cn=root,dc=ibm.com.

SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Amostra para o Padrão SOA Policy Gateway Basic Runtime Sample

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Nota: Qualquer parâmetro que requeira o valor Não Configurado faz distinção entre maiúsculas e minúsculas.

Tabela 27. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
SCP_host	Sim		O nome do host do Servidor SCP que contém o `DomainZipFile.zip`.
SCP_user	Sim		O nome de usuário a ser usado para se conectar ao Servidor SCP.
SCP_password	Sim		A senha a ser usada para efetuar login no Servidor SCP.
Verificar senha	Sim		Verifica a entrada do usuário para SCP_password.
SCP_zip_location	Sim		O local de URI do `DomainZipFile.zip`. Por exemplo, `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	Sim		O nome do Arquivo de Certificados do PEM usado para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Use o valor “Não Configurado” apenas para Autenticação de Servidor e não para usar o SSL.
CLIENT_PUBLIC _KEY_password	Sim		A senha para o Certificado Público usado para se conectar à porta Interface de Gerenciamento XML de Dispositivos DataPower. O valor será “Não Configurado” se nenhuma senha for usada.
Verificar senha	Sim		Verifica a entrada do usuário para CLIENT_PUBLIC_KEY_password.
CLIENT_PRIVATE_KEY_file	Sim		O nome do Arquivo-chave do PEM usado para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Isto é requerido para Autenticação Mútua. Use o valor “Não Configurado” apenas para Autenticação de Servidor e não para usar o SSL.
CLIENT_PRIVATE_KEY_password	Sim		A senha do arquivo-chave usada para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Isto é requerido para Autenticação Mútua. O valor será “Não Configurado” se nenhuma senha for usada.

Tabela 27. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Necessário	Valor padrão	Descrição
Verificar senha	Sim		Verifica a entrada do usuário para CLIENT_PRIVATE_KEY_password.
DataPower_hostname	Sim		O nome do host do dispositivo DataPower no qual o aplicativo de amostra será instalado.
DataPower_XML_mgmt_port	Sim	5550	A porta usada para a Interface de Gerenciamento XML do DataPower.
DataPower_admin_id	Sim		O ID de usuário administrador com permissões apropriadas para usar a Interface de Gerenciamento XML.
DataPower_admin_password	Sim		A senha para o DataPower_admin_id.
Verificar senha	Sim		Verifica a entrada do usuário para DataPower_admin_password.
SOAPolicySample_DataPower_domain	Sim	SOAPolicySample	O nome de domínio da amostra. Ele não deve corresponder a nenhum domínio existente no dispositivo DataPower.
SOAPolicySample_starting_port	Sim	62001	O aplicativo requer 5 portas livres, que serão usadas sequencialmente a partir desse valor. Por exemplo, se o valor for 62000, as portas 62000-62004 serão usadas. Nenhuma verificação é feita pelo script para saber se portas estão livres.
LDAP_hostname	Sim		A amostra usa um servidor LDAP, este é o nome do host desse servidor.
LDAP_port	Sim	389	A porta não segura do servidor LDAP. Geralmente, 389.
LDAP_password	Sim		A senha usada na ligação com o LDAP_DN.
Verificar senha	Sim		Verifica a entrada do usuário para LDAP_password.
LDAP_DN	Sim		O nome distinto usado para ligação com o LDAP. POr exemplo, cn=root,dc=ibm.com.

Script: SOA Policy Gateway 2.0.0.0 - Segurança

O script de Segurança copia as informações de segurança, contidas em um arquivo ZIP, necessárias para a comunicação com um dispositivo DataPower na máquina do Dmgr ou do WSRR a partir de um servidor de arquivos externo que suporta o secure copy program (SCP) do Linux.

O arquivo de segurança que é copiado contém o seguinte:

- Certificado de Acesso ao DPC
- Certificado Público de Acesso ao DPC
- Chave Privada do DPC
- Script de CLI do DP
- Pasta de cadeia de certificados

O script da interface de linha de comandos (CLI) para o DataPower permite configurar um domínio implementado durante a fase de implementação do padrão.

Nota: Certificados de segurança confidenciais devem ser excluídos do servidor de arquivos externo após a implementação.

Parâmetros

Tabela 28. Parâmetros Configuráveis

Nome do parâmetro	Descrição
SCP_host	O nome do host do Servidor SCP que contém o arquivo `DomainZipFile.zip`.
SCP_user	O nome de usuário a ser usado para se conectar ao Servidor SCP.
SCP_password	A senha a ser usada para efetuar login no Servidor SCP.
Verificar senha	Verifica a entrada do usuário para SCP_password.
SCP_zip_location	O local de URI do arquivo `DomainZipFile.zip`; por exemplo, `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	O nome do Arquivo de Certificado do PEM usado para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower.
CLIENT_PUBLIC_KEY_password	A senha do certificado de cliente usada para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Isto é requerido se disponível para Autenticação Mútua. Esse valor pode ser "Não Configurado" se nenhuma senha for usada.
CLIENT_PRIVATE_KEY_file	O nome do Arquivo-chave do PEM usado para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Isto é necessário para Autenticação Mútua.
CLIENT_PRIVATE_KEY_password	A senha do arquivo-chave usada para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Isto é requerido para Autenticação Mútua. Esse valor pode ser "Não Configurado" se nenhuma senha for usada.
CLI_file	O nome do arquivo de CLI contido no `DomainZipFile.zip`. Essa CLI é executada no final da instalação do Domínio e da Configuração do WSRR Server.

SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Segurança para o Padrão SOA Policy Gateway Basic Runtime

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 29. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
SCP_host	Sim		O nome do host do Servidor SCP que contém o arquivo `DomainZipFile.zip`.
SCP_user	Sim		O nome de usuário a ser usado para se conectar ao Servidor SCP.
SCP_password	Sim		A senha a ser usada para efetuar login no Servidor SCP.
Verificar senha	Sim		Verifica a entrada do usuário para SCP_password.
SCP_zip_location	Sim		O local de URI do arquivo `DomainZipFile.zip`; por exemplo, `/files/DomainZipFile.zip`.
CLIENT_PUBLIC_KEY_file	Sim		O nome do Arquivo de Certificado do PEM usado para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower.

Tabela 29. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Necessário	Valor padrão	Descrição
CLIENT_PUBLIC_KEY_password	Sim		A senha do certificado de cliente usada para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Isto é requerido se disponível para Autenticação Mútua. Esse valor pode ser "Não Configurado" se nenhuma senha for usada.
CLIENT_PRIVATE_KEY_file	Sim		O nome do Arquivo-chave do PEM usado para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Isto é necessário para Autenticação Mútua.
CLIENT_PRIVATE_KEY_password	Sim		A senha do arquivo-chave usada para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Isto é requerido para Autenticação Mútua. Esse valor pode ser "Não Configurado" se nenhuma senha for usada.
CLI_file	Sim	Não Configurado	O nome do arquivo de CLI contido no `DomainZipFile.zip`. Essa CLI é executada no final da instalação do Domínio e da Configuração do WSRR Server.

SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Segurança para o Padrão SOA Policy Gateway Advanced Runtime

Os parâmetros necessários sem um valor padrão devem ser configurados antes que o padrão possa ser implementado.

Tabela 30. Parâmetros Configuráveis

Nome do parâmetro	Necessário	Valor padrão	Descrição
SCP_zip_location	Sim		O local de URI do arquivo `DomainZipFile.zip`; por exemplo, `/files/DomainZipFile.zip`.
SCP_host	Sim		O nome do host do Servidor SCP que contém o arquivo `DomainZipFile.zip`.
SCP_user	Sim		O nome de usuário a ser usado para se conectar ao Servidor SCP.
SCP_password	Sim		A senha a ser usada para efetuar login no Servidor SCP.
Verificar senha	Sim		Verifica a entrada do usuário para SCP_password.
CLIENT_PUBLIC_KEY_file	Sim		O nome do Arquivo de Certificado do PEM usado para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower.
CLIENT_PUBLIC_KEY_password	Sim		A senha do certificado de cliente usada para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Isto é requerido se disponível para Autenticação Mútua. Esse valor pode ser "Não Configurado" se nenhuma senha for usada.

Tabela 30. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Necessário	Valor padrão	Descrição
CLIENT_PRIVATE_KEY_file	Sim		O nome do Arquivo-chave do PEM usado para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Isto é necessário para Autenticação Mútua.
CLIENT_PRIVATE_KEY_password	Sim		A senha do arquivo-chave usada para se conectar à porta da Interface de Gerenciamento XML de Dispositivos DataPower. Isto é requerido para Autenticação Mútua. Esse valor pode ser "Não Configurado" se nenhuma senha for usada.
CLI_file	Sim	Não Configurado	O nome do arquivo de CLI contido no `DomainZipFile.zip`. Essa CLI é executada no final da instalação do Domínio e da Configuração do WSRR Server.

Capítulo 5. Trabalhando com o IBM SOA Policy Gateway Pattern

O IBM SOA Policy Gateway Pattern fornece uma definição de padrão para implementação repetida da topologia que compõe o produto. Cada padrão fornece uma função específica no IBM SOA Policy Gateway Pattern e contém diversas imagens para suportar cada padrão. Os padrões devem ser configurados antes da implementação com base nas necessidades de negócios.

Como parte do processo de implementação, configure os parâmetros de parte. Para obter informações adicionais, consulte "Implementando Padrões" na página 61.

Tarefas relacionadas:

Capítulo 3, "Introdução ao IBM SOA Policy Gateway Pattern", na página 11
Este padrão usa o WebSphere DataPower para controlar mensagens usando políticas controladas e definições de serviço no WSRR. Revise os tópicos nesta seção para entender o que é abrangido neste cenário, as razões pelas quais uma empresa pode desejar seguir o cenário, as funções de usuário envolvidas e uma visão geral do recurso entregue com o produto.

Planejando a Configuração do Padrão e Pré-requisitos do Padrão

O IBM SOA Policy Gateway Pattern fornece um meio de provisionar de forma rápida e confiável um ambiente para controlar definições de serviço e políticas e aplicar essas políticas. Determine os requisitos de controle e os recursos necessários.

Para implementar o ambiente, preparar o dispositivo DataPower para administração remota e coletar os recursos necessários para se comunicar com segurança com o dispositivo. O teste do ambiente pode ser realizado implementando o SOA Policy Gateway Basic Runtime Sample. Isso confirma que o ambiente está corretamente configurado para implementação e demonstra o cumprimento das políticas. Depois da validação do ambiente, a configuração desejada de tempo de execução e controle do IBM SOA Policy Gateway Pattern é decidida usando as melhores práticas do WSRR. A implementação do padrão inicia com o Governance Master, seguido pelos padrões de Tempo de Execução correspondidos para a configuração desejada.

Preparando e Implementando o IBM SOA Policy Gateway Pattern

Prepare o DataPower e colete os arquivos de segurança:

1. Prepare o dispositivo DataPower para administração remota. Para obter informações adicionais, consulte "Configurando o DataPower para as IBM SOA Policy Gateway Patterns" na página 53.
2. Se o dispositivo DataPower estiver protegido, leia a seção de segurança do DataPower e, em seguida, colete os arquivos de segurança do DataPower necessários para se comunicar com ele.
3. Confirme se um sistema DataPower no ambiente de nuvem pode se comunicar com o dispositivo e que o dispositivo pode se comunicar com um sistema implementado.

O SOA Policy Gateway Basic Runtime Sample pode ser usado para demonstrar os recursos do padrão antes de você criar uma implementação de produção. Se o uso do Basic Runtime Sample for necessário, conclua as etapas a seguir:

1. Forneça um servidor SCP no Linux acessível a partir de um sistema implementado dentro da nuvem. SCP é o comando de cópia segura. O servidor SCP fornece um meio para hospedar os arquivos de segurança externos ao padrão, para que o padrão não precise ser alterado para cada configuração de segurança.
2. Forneça um servidor LDAP para hospedar os IDs de segurança usados pelo aplicativo de amostra implementado no DataPower. Para obter informações adicionais, consulte "Configurando o LDAP para a Amostra" na página 60.
3. Implemente o padrão do SOA Policy Gateway Basic Runtime Sample para validar a infraestrutura. Para obter informações adicionais, consulte "Implementando o Padrão SOA Policy Gateway Basic Runtime Sample" na página 62.
4. Quando o uso da amostra estiver concluído, o servidor LDAP não será necessário.

Prepare para implementação da produção:

1. Decida a escala necessária para a implementação. Decida os tamanhos de cluster para o Governance Master e as implementações de tempos de execução.

   Nota: Quando um cluster é implementado, não pode ser estendido com outro membro do cluster.
2. Defina o nome da célula e o ID do usuário administrativo e a senha do usuário administrativo do Governance Master.
3. Hospede o arquivo `DomainZipFile.zip` de segurança do DataPower em um servidor SCP. Para obter informações adicionais, consulte "Criando o `DomainZipFile.zip` de Segurança" na página 54.

Implemente o Governance Master para o ambiente de produção:

1. Implemente um padrão do SOA Policy Gateway Governance Master. Aguarde a conclusão da implementação antes de implementar padrões de tempo de execução do ambiente de produção. Para obter informações adicionais, consulte "Implementando o Padrão SOA Policy Gateway Governance Master" na página 63.

Implemente os padrões de tempo de execução do ambiente de produção:

1. Decida se um ambiente em cluster ou independente é necessário.
2. Se mais de um domínio de DataPower for necessário, clone o padrão Basic Runtime ou Advanced Runtime e inclua pacotes de scripts DataPower no clone para cada domínio necessário.

   Nota: Domínios adicionais do DataPower não podem ser incluídos depois que essa configuração foi concluída.
   Para obter informações adicionais, consulte "Implementando com Vários Domínios DataPower" na página 70.
3. Configure o padrão de tempo de execução com as informações de padrão do Governance Master. Para obter informações adicionais, consulte "Informações de Implementação do SOA Policy Gateway Governance Master" na página 64.
4. Decida se o tempo de execução será temporariedade, produção ou outros.
5. Implemente o padrão Basic Runtime ou Advanced Runtime. Para obter informações adicionais, consulte "Implementando o Padrão SOA Policy

Gateway Advanced Runtime" na página 66 ou "Implementando o Padrão SOA Policy Gateway Basic Runtime" na página 65.

6. Aguarde até que esteja totalmente implementado antes de implementar outro tempo de execução

.

Quando a implementação dos tempos de execução está concluída:

1. O servidor de arquivos SCP não é mais necessário.
2. A segurança do WSRR e do WebSphere pode ser atualizada a partir da configuração de segurança padrão. Para obter informações adicionais, consulte "Gerenciamento da Segurança" na página 54.
3. O domínio do DataPower está pronto para a configuração de gateway.

Configurando o DataPower para as IBM SOA Policy Gateway Patterns

Conclua as etapas de configuração do DataPower antes de executar os scripts SOAPolicy.

Procedimento

1. Efetue login no dispositivo DataPower suportado como um Administrador.
2. Procure `Interface de Gerenciamento XML`.
3. Certifique-se de que seu estado esteja ativado.
4. Certifique-se de que os itens a seguir estejam ativos e corretamente protegidos:
   - URI de Gerenciamento do SOAP
   - Gerenciamento de Configuração do SOAP
   - Gerenciamento de Configuração do SOAP (v2004)
   - Terminal AMP
   - Terminal SLM
   - Terminal WS-Management
   - Terminal WSDM
   - Assinatura do UDDI
   - Assinatura do WSRR

Segurança para os Padrões IBM SOA Policy Gateway Pattern

Os clientes requerem diferentes níveis de segurança entre o WSRR e o DataPower, particularmente na área de SSL. O IBM SOA Policy Gateway Pattern suporta 3 níveis de comunicação SSL entre os scripts de configuração e os padrões DataPower ao usar o SOA Policy Gateway Basic Runtime, SOA Policy Gateway Basic Runtime Sample e SOA Policy Gateway Advanced Runtime.

Se SSL Não For Necessário

Se não for necessário usar SSL, a chave pública e as chaves privadas para o cliente curl não serão fornecidas e deixadas como "Não Configurado".

Nota: Se nenhum SSL for usado, todos os dados enviados ao DataPower serão decriptografados, incluindo informações de usuário e senha. Isso apresenta uma vulnerabilidade de segurança. As senhas usadas em chamadas SOMA para o DataPower não suportam criptografia e, portanto, são transportadas para o

dispositivo DataPower não criptografados. Portanto, use a autenticação do lado do servidor em um mínimo para assegurar a segurança.

Autenticação Mútua entre os Aplicativos DataPower e os Scripts nos Padrões Basic e Advanced

Se for requerida a autenticação mútua entre os aplicativos do DataPower e os scripts nos padrões Basic e Advanced:

- A chave pública e as chaves privadas para o cliente curl devem ser fornecidas.

Gerenciamento da Segurança

As imagens do WSRR e as imagens do WebSphere Application Server usadas nos padrões têm apenas a segurança padrão no lugar. Para produzir um ambiente realmente seguro, você precisa protegê-lo com Técnicas padrão de Segurança do WebSphere.

Consulte o Centro de Informações do WebSphere Network Deployment Versão 8.0 nos links a seguir:

- WebSphere Application Server, Network Deployment (plataformas distribuídas e Windows), Versão 8.0: Centro de Informações do IBM WebSphere Application Server, Network Deployment (Plataformas Distribuídas e Windows), Versão 8.0
- Segurança do aplicativo: Centro de Informações do IBM WebSphere Application Server, Network Deployment (Plataformas Distribuídas e Windows), Versão 8.0 - Protegendo Aplicativos e Seus Ambientes
- Caminhos de ponta a ponta para segurança: Centro de Informações do IBM WebSphere Application Server, Network Deployment (Plataformas Distribuídas e Windows), Versão 8.0 - Protegendo Aplicativos e Seus Ambientes

Criando o `DomainZipFile.zip` de Segurança

Crie o `DomainZipFile.zip` de Segurança para o padrão SOA Policy Gateway Basic Runtime, o padrão SOA Policy Gateway Advanced Runtime e o padrão SOA Policy Gateway Basic Runtime Sample.

Procedimento

Crie o `DomainZipFile.zip` usando as regras a seguir:

1. A Estrutura do `DomainZipFile.zip` deve ser como a seguir:

   Nota: Somente a estrutura de diretório é necessária, os nomes dos arquivos individuais podem seguir a nomenclatura de sua escolha. No entanto, todos os arquivos de certificado e de chave devem estar no formato PEM.

   Nota: O uso do Nome do Host do DataPower no caminho permite que diferentes certificados sejam usados para diferentes dispositivos DataPower.

Tabela 31. Arquivos Necessários para os Padrões Basic e Advanced

Nome do arquivo, local relativo ao diretório-raiz	Notas
`CurlClientPublicKeyFile.crt`	Necessário apenas se a Autenticação Mútua for usada. Apenas formato PEM.
`CurlClientPrivateKeyFile.key`	Necessário apenas se a Autenticação Mútua for usada.

Tabela 31. Arquivos Necessários para os Padrões Basic e Advanced (continuação)

Nome do arquivo, local relativo ao diretório-raiz	Notas
/*dataPowerHostName*/certificate1.crt	Os certificados do DataPower a serem transferidos por upload para o WSRR. Requer que a Cadeia de Certificados inteira esteja no formato PEM. Certificados do DataPower a serem transferidos por upload para o WSRR. Ele deve incluir apenas o conteúdo a seguir: ------BEGINCERTIFICATE---- to -----END CERTIFICATE----- A extensão do arquivo deve ser .crt ou .pem.
/*dataPowerHostName*/certificate2.crt	A extensão do arquivo deve ser .crt ou .pem.
/*dataPowerHostName*/certificate3.crt	A extensão do arquivo deve ser .crt ou .pem.

2. Apenas para o padrão SOA Policy Gateway Advanced Runtime, inclua o arquivo cli a ser executado (opcional):

Tabela 32. Arquivos Adicionais Necessários para o Padrão Advanced

Nome do arquivo, local relativo ao diretório-raiz	Notas
/cli.cli	Um único arquivo CLI que será executado no final da Configuração de Domínio do DataPower

3. Coloque o DomainZipFile.zip em seu local do servidor SCP. Devido à natureza sensível dos arquivos, é recomendado que você exclua o arquivo após a configuração. Os scripts de configuração de padrão excluirão quaisquer arquivos obtidos do DomainZipFile.zip, bem como a cópia do DomainZipFile.zip que é criada usando SCP, de seu ambiente SCP.
4. Anote as informações do Servidor SCP a seguir:
   - O Nome do Host do SCP
   - O caminho do SCP para o DomainZipFile.zip
   - O Usuário e Senha do SCP

Usando o Arquivo DomainZipFile

Use casos do arquivo DomainZipFile para diferentes níveis de segurança em padrões.

O arquivo DomainZipFile.zip pode ser usado nos padrões Basic Runtime, Basic Runtime Sample e Advanced Runtime.

O SSL não é necessário para conectar os pacotes de scripts padrão para o dispositivo DataPower. Se você não usar o SSL, será necessário criar um arquivo DomainZipFile.zip, a menos que você requeira um script cli para customizar o domínio do DataPower criado pelo padrão. Nesse caso, se você não usar autenticação de servidor como um mínimo, os dados não serão criptografados. Este é um risco de segurança, pois as informações de usuário e senha são transmitidas para o DataPower durante o cliente de script em uma conexão http, e este é protegido pelos certificados no arquivo DomainZipFile.zip.

Se o host do DataPower não estiver configurado para validar o certificado do cliente, você não precisará usar Autenticação Mútua entre o cliente de script e o dispositivo DataPower. É recomendável usar, no mínimo, a Autenticação de Servidor.

Os cenários de caso neste tópico descrevem níveis diferentes de segurança.

O produto suporta os cenários de caso a seguir:

Caso 1: Nenhum SSL é necessário

Caso 2: Nenhum SSL é necessário, mas um script cli é necessário para customizar o domínio

Caso 3: A autenticação do servidor do Certificado do DataPower pelo cliente de Script é necessária

Caso 4: A Autenticação Mútua com o Dispositivo DataPower é Necessário

Caso 1: Nenhum SSL é necessário

É recomendável pelos motivos de segurança descritos que esta opção seja usada apenas para cenários de desenvolvimento. Caso o uso de SSL não seja requerido:

1. Configure os parâmetros para SCP_host como "Unset". Se você estiver usando os Padrões Basic Runtime ou Advanced Runtime, o SCP_host estará no SOA Policy Gateway 2.0.0.0 - Script do Pacote de Segurança. Se você estiver usando o padrão Basic Runtime Sample, SCP_host estará no script SOA Policy Gateway 2.0.0.0. Isso configura o script no padrão, de forma que ele não recupere o arquivo `DomainZipFile.zip` usando o SCP.
2. Configure os parâmetros a seguir como "Não Configurado" nos mesmos pacotes de scripts da etapa 1:
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - Verificar senha
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - Verificar senha

Caso 2: Nenhum SSL é necessário, mas um script cli é necessário para customizar o domínio

É recomendável pelos motivos de segurança descritos que esta opção seja usada apenas para cenários de desenvolvimento. Se você não desejar usar SSL, mas requerer um script cli:

1. Configure os parâmetros para SCP_host como "Unset". Se você estiver usando os Padrões Basic ou Advanced Runtime, o SCP_host estará no SOA Policy Gateway 2.0.0.0 - Script do Pacote de Segurança. Se você estiver usando o padrão Basic Runtime Sample, SCP_host estará no script SOA Policy Gateway 2.0.0.0. Isso configura o script no padrão, de forma que ele não recupere o arquivo `DomainZipFile.zip` usando o SCP.
2. Configure os parâmetros a seguir como Não Configurado nos mesmos pacotes de scripts da etapa 1:
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - Verificar senha
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - Verificar senha

   Nota: Se SCP_host for "Não Configurado", não será necessário um arquivo `DomainZipFile.zip`, a menos que você tenha um script cli que deseje executar nos padrões Basic Runtime e Advanced Runtime.

3. Coloque o arquivo de script cli que você deseja usar na raiz do arquivo `DomainZipFile.zip`. Um exemplo de estrutura do arquivo `DomainZipFile.zip` é o seguinte:

   ```
   /cli.cli
   ```

   Esse arquivo é executado no fim do pacote de scripts de Domínio do DataPower. `cli.cli` é um exemplo de nome do arquivo. O nome do arquivo não deve conter nenhum espaço.

Caso 3: A autenticação do servidor do Certificado do DataPower pelo cliente de Script é necessária

Você deve fornecer todos os Certificados da cadeia de Certificados do DataPower que protege a Interface de Gerenciamento XML. Para localizá-los, conclua as etapas a seguir:

1. Examine o perfil proxy SSL para a Interface de Gerenciamento XML e localize o CryptoProfile. O Perfil Crypto conterá as credenciais de identificação que contêm os certificados usados para proteger a Interface de Gerenciamento XML.
2. Inclua esses certificados no arquivo `DomainZipFile.zip`.

   O formato é:

   - dataPowerHostName/certificateChainMember1.crt
   - dataPowerHostName/certificateChainMember2.pem
   - dataPowerHostName/certificateChainMember(n).crt

   Se você estiver usando o cenário de vários domínios, o arquivo poderá ter dois diretórios `dataPowerHostName` diferentes com os arquivos a seguir para cada Cadeia de Certificados do DataPower:

   - clientCertificate.crt clientKeyFile.key
   - dataPowerHostName/certificateChainMember1.crt
   - dataPowerHostName/certificateChainMember2.pem
   - dataPowerHostName/certificateChainMember(n).crt
   - dataPowerHostName2/certificateChainMember1a.crt
   - dataPowerHostName2/certificateChainMember2a.pem
   - dataPowerHostName2/certificateChainMember2(n).crt

   Nota: Os arquivos da cadeia de certificados do DataPower devem ser do tipo `.crt` ou `.pem` e devem conter apenas o certificado em si. Os nomes de arquivo `.crt` ou `.pem` usados aqui são exemplos. O nome do arquivo não deve conter nenhum espaço.
3. Opcional: Se você requerer apenas Autenticação de Servidor para o SOA Policy Gateway 2.0.0.0 - Script do Pacote de Segurança usado pelos Padrões Basic Runtime e Advanced Runtime ou o SOA Policy Gateway 2.0.0.0 - Script de amostra no padrão Basic Runtime Sample, use “Não Configurado” como o valor para os parâmetros a seguir nesses scripts:

   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - Verificar senha
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - Verificar senha
4. Opcional: Se um script cli for necessário:

Coloque o arquivo de script cli que você deseja usar na raiz do arquivo `DomainZipFile.zip`. Um exemplo de estrutura do arquivo `DomainZipFile.zip` é o seguinte:

`/cli.cli`

Esse arquivo é executado no fim do pacote de scripts de Domínio do DataPower. `cli.cli` é um exemplo de nome do arquivo. O nome do arquivo não deve conter nenhum espaço.

Caso 4: A Autenticação Mútua com o Dispositivo DataPower é Necessário

Neste caso, o cliente e o DataPower Server requerem validação dos outros certificados. Isso é necessário apenas se o Host do DataPower é configurado no Perfil Proxy SSL para a Interface de Gerenciamento XML para validar os certificados dos clientes.

1. Inclua esses certificados no arquivo `DomainZipFile.zip`.

   O formato é:

   - clientCertificate.crt
   - clientKeyFile.key
   - dataPowerHostName/certificateChainMember1.crt
   - dataPowerHostName/certificateChainMember2.pem
   - dataPowerHostName/certificateChainMember(n).crt
   - dataPowerHostName2/certificateChainMember1a.crt
   - dataPowerHostName2/certificateChainMember2a.pem
   - dataPowerHostName2/certificateChainMember2(n).crt

   Nota: Os arquivos da cadeia de certificados do DataPower devem ser do tipo `.crt` ou `.pem` e devem conter apenas o certificado em si. Os nomes de arquivo `.crt` ou `.pem` usados aqui são exemplos. O nome do arquivo não deve conter nenhum espaço.

   O certificado de cliente e o arquivo-chave de cliente podem conter os dados no certificado ou no arquivo-chave antes da linha no arquivo que lê: `-----BEGIN CERTIFICATE-----`.
2. Opcional: Se você requerer Autenticação de Servidor para o SOA Policy Gateway 2.0.0.0 - Script do Pacote de Segurança usado pelos Padrões Basic Runtime e Advanced Runtime ou o SOA Policy Gateway 2.0.0.0 - Script de amostra no padrão Basic Runtime Sample, use “Não Configurado” como o valor para os parâmetros a seguir nesses scripts:
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - Verificar senha
3. Se não houver senha para o arquivo de Chaves Públicas, o valor dos scripts a seguir podem ser “Não Configurado”:
   - CLIENT_PUBLIC_KEY_password
   - Verificar senha
4. Os comandos curl usados pelos pacotes de scripts assumem que o tipo de arquivo seja `.pem`, de modo que **--key-type** e **--cert-type** sejam configurados

para PEM por padrão. O certificado e os arquivos- chave podem conter este conteúdo antes de `-----BEGIN CERTIFICATE-----` no certificado específico ou no arquivo-chave.

5. Opcional: Se um script cli for necessário, usando os padrões Basic Runtime ou Advanced Runtime:

   Coloque o arquivo de script cli que você deseja usar na raiz do arquivo `DomainZipFile.zip`. Um exemplo de estrutura do arquivo `DomainZipFile.zip` é o seguinte:

   ```
   /cli.cli
   ```

   Esse arquivo é executado no fim do pacote de scripts de Domínio do DataPower. `cli.cli` é um exemplo de nome do arquivo. O nome do arquivo não deve conter nenhum espaço.

Ao selecionar um caso, você terá configurado o nível de segurança apropriado, com ou sem usar o arquivo `DomainZipFile.zip`.

Certificados do DataPower a Serem Transferidos por Upload para o WSRR

É possível fornecer um diretório de certificados no diretório `dataPowerHostName` do arquivo `DomainZipFile.zip`. Isso pode ser transferido por upload para o WSRR Server Dmgr ou servidor independente WSRR.

Fornecendo seu Próprio Mecanismo para Fazer Download do Arquivo `DomainZipFile.zip`

É possível fornecer seu próprio `DomainZipFile.zip` sem usar o servidor SCP no Pacote de Scripts de Segurança.

Procedimento

Para usar outros meios para colocar o arquivo no ambiente, você deve executar o seguinte:

1. O parâmetro **`SCP_host`** deve ser configurado como Unset.
2. Você deve criar um pacote de scripts customizados para criar o `DomainZipFile.zip` no diretório `/tmp` antes de executar qualquer um dos Scripts de Padrão de Gateway SOA.
3. Para padrões Advanced, crie o arquivo `DomainZipFile.zip` no diretório `/tmp/security/RetrieveDomainFiles`.
4. Para padrões Basic com Sample, crie o arquivo `DomainZipFile.zip` no diretório `/installSample/Retrieve_Domain_Files`.

   Nota: Se o arquivo `DomainZipFile.zip` não estiver presente, o script poderá falhar se os parâmetros indicarem que certificados ou chaves são usados.

Valores CN em Certificados

Os Certificados fornecidos como parte do arquivo `DomainZipFile.zip` devem considerar o valor CN no certificado.

A Verificação de HostName está sempre ativa quando você escolhe usar SSL, portanto, é necessário levar em consideração o seguinte quando o Certificado é usado no Pacote de Scripts:

- Para Certificados de Cliente (Público e Privado/Chave), você não tem como saber o host exato em que o WSRR Server ou o WSRR Dmgr que executa o script estará presente. Portanto, o valor de CN deve ser genérico o suficiente

para executar em qualquer host do cliente em potencial no ambiente do IBM Workload Deployer; por exemplo, `*clientname*.yourcompany.com`.

- Os certificados para as máquinas DataPower estão em diretórios individuais no arquivo `DomainZipFile.zip`; por exemplo:

```
dpHost1/cert1.crt
dpHost2/certb.crt
dpHost2/certbc.pem
```

- O valor de CN para o certificado (o certificado final na cadeia do host do DataPower) deve ser válido para esse nome de host; por exemplo, `dp1.yourcompany.com` ou `*dp*.yourcompany.com`.

Configurando o LDAP para a Amostra

A amostra requer um protocolo LDAP com algumas entradas específicas.

Sobre Esta Tarefa

Os elementos e as propriedades devem ser definidos ao configurar o LDAP.

Nota: Não altere estas senhas.

Como uma alternativa para as etapas de configuração manual, extraia o conteúdo do arquivo `.zip` a seguir, que contém dois arquivos LDIF com os detalhes da configuração fornecidos nesta tarefa, e use esses arquivos para atualizar o servidor LDAP: soaSamples.zip.

Procedimento

Crie um LDAP com os elementos a seguir:

1. Defina o sufixo:

```
dc=ibm.com
```

2. Defina o domínio `dc=ibm.com` com as propriedades a seguir:

```
dn: dc=ibm.com
dc: ibm.com
objectclass: domain
objectclass: top
```

3. Defina os contêineres:
   a. Defina os grupos de contêineres:

```
dn: cn=groups,dc=ibm.com
objectclass: container
objectclass: top
cn: groups
```

   b. Defina os usuários do contêiner:

```
dn: cn=users,dc=ibm.com
objectclass: container
objectclass: top
cn: users
```

4. Defina os usuários a seguir:
   a. Usuário ConsumerA com as propriedades a seguir:

```
dn: uid=ConsumerA,cn=users,dc=ibm.com
uid: ConsumerA
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
sn: ConsumerA
cn: ConsumerA
userpassword: passw0rd
```

   b. Usuário ConsumerB com as propriedades a seguir:

```
dn: uid=ConsumerB,cn=users,dc=ibm.com
uid: ConsumerB
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
sn: ConsumerB
cn: ConsumerB
userpassword: passw0rd
```

c. Usuário ConsumerX com as propriedades a seguir:

```
dn: uid=ConsumerX,cn=users,dc=ibm.com
uid: ConsumerX
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
sn: ConsumerX
cn: ConsumerX
userpassword: passw0rd
```

5. Defina os grupos a seguir:
   a. Defina o grupo MANAGER com as propriedades a seguir:

```
dn: cn=MANAGER,cn=groups,dc=ibm.com
objectclass: groupOfNames
objectclass: top
cn: MANAGER
member: uid=ConsumerX,cn=users,dc=ibm.com
```

   b. Defina o grupo Clerk com as propriedades a seguir:

```
dn: cn=Clerk,cn=groups,dc=ibm.com
objectclass: groupOfNames
objectclass: top
cn: Clerk
member: uid=ConsumerA,cn=users,dc=ibm.com
```

   c. Defina o grupo Customer com as propriedades a seguir:

```
dn: cn=Customer,cn=groups,dc=ibm.com
objectclass: groupOfNames
objectclass: top
cn: Customer
member: uid=ConsumerB,cn=users,dc=ibm.com
```

6. Certifique-se de coletar as informações a seguir sobre o LDAP antes de executar a amostra:
   - O nome distinto (DN); por exemplo, `cn=root`.
   - A senha; por exemplo, `passw0rd`.
   - A porta não segura; por exemplo, 389.
   - O nome do Host LDAP; por exemplo, `ldap.customer.com`.

Implementando Padrões

A implementação de padrões som o IBM Workload Deployer 3.1.0.2 ou IBM SOA Policy Gateway Pattern na nuvem fornece um ambiente do IBM PureApplication System. É possível implementar os padrões predefinidos disponíveis com as imagens do IBM SOA Policy Gateway Pattern ou implementar padrões que você criou.

Antes de Iniciar

Para implementar um padrão, você deve primeiro ter um padrão predefinido ou um novo padrão que esteja completo, com todas as partes necessárias configuradas.

Sobre Esta Tarefa

A implementação de um padrão cria um sistema virtual, ou um ambiente de tempo de execução do IBM SOA Policy Gateway Pattern recém-aprovisionado, que esteja em execução na nuvem.

Procedimento

Para implementar os IBM SOA Policy Gateway Patterns para executar em sua nuvem privada, conclua as etapas a seguir:

1. Na lista de padrões na janela Padrões de Sistema Virtual, selecione o padrão a ser implementado.
2. Clique no ícone **Implementar**.
3. Preencha os campos obrigatórios para implementar o padrão. Na janela, insira um nome para o sistema virtual e quaisquer outras informações necessárias. Uma marca de seleção ao lado de cada item indica que ele não requer configuração adicional. É possível alterar os parâmetros para partes configuradas, antes de implementar o padrão, clicando no nome da parte para abrir o editor para a parte. As máquinas virtuais são criadas na ordem necessária e, em seguida, iniciadas.

Resultados

O processo de implementação cria e inicia máquinas virtuais para as partes definidas e fornece links para consoles necessários. O tempo para a implementação depende da complexidade do padrão que está sendo implementado. Um padrão implementado é um sistema virtual ou um ambiente de tempo de execução do IBM SOA Policy Gateway Pattern recém-aprovisionado.

O que Fazer Depois

É possível visualizar o status de sua instância, para ver quando a implementação está concluída e começar a administrá-la, a partir da janela Instâncias de Sistema Virtual.

Informações relacionadas:

IBM Workload Deployer: Gerenciando Padrões de Sistema Virtual

IBM PureApplication System: Gerenciando Padrões de Sistema Virtual

Implementando o Padrão SOA Policy Gateway Basic Runtime Sample

A implementação do padrão SOA Policy Gateway Basic Runtime Sample cria uma instância de sistema virtual em execução do padrão.

Antes de Iniciar

Estes pré-requisitos devem ser concluídos antes de implementar o padrão:

- Configure o DataPower para a amostra; consulte “Configurando o DataPower para as IBM SOA Policy Gateway Patterns” na página 53.
- Configure a Segurança para a amostra; consulte “Segurança para os Padrões IBM SOA Policy Gateway Pattern” na página 53.
- Configure o servidor SCP para hospedar arquivos de segurança.

- Configure o LDAP para a amostra; consulte “Configurando o LDAP para a Amostra” na página 60.

Sobre Esta Tarefa

A implementação de um padrão cria uma instância de sistema virtual que está em execução na nuvem.

Procedimento

Para implementar o padrão SOA Policy Gateway Basic Runtime Sample, conclua as etapas a seguir:

1. Clique em **Padrões** > **Sistemas Virtuais**.
2. Na lista Padrões de Sistema Virtual, selecione **SOA Policy Gateway 2.0.0.0 - Basic Runtime Sample**.
3. Clique no ícone Implementar.
4. Preencha os campos obrigatórios para implementar o padrão. Uma marca de seleção ao lado de cada item indica que ele não requer configuração adicional.
   a. Na caixa **Nome do Sistema Virtual**, insira um nome exclusivo para a instância.
   b. Configure os padrões virtuais. Clique em **Configurar Partes Virtuais**, em seguida, clique no nome da parte para abrir o editor para as partes e o script:

      Nota: Todas as senhas para este padrão, exceto o parâmetro DataPower_admin_id, foram assumidas por padrão como `password`.
      - “Parâmetros de Configuração da Parte do DB2 Enterprise para o Padrão SOA Policy Gateway Basic Runtime Sample” na página 28.
      - “Parâmetros de Configuração da Parte de Servidor Independente do WSRR para o Padrão SOA Policy Gateway Basic Runtime Sample” na página 36
      - “SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Amostra para o Padrão SOA Policy Gateway Basic Runtime Sample” na página 46
5. Clique em **OK** para implementar o padrão.

O que Fazer Depois

Para verificar a implementação, consulte “Verificando a Implementação” na página 67.

Implementando o Padrão SOA Policy Gateway Governance Master

A implementação do padrão SOA Policy Gateway Governance Master cria uma instância de sistema virtual em execução do padrão.

Sobre Esta Tarefa

A implementação de um padrão cria uma instância de sistema virtual que está em execução na nuvem.

Procedimento

Para implementar o padrão SOA Policy Gateway Governance Master, conclua as etapas a seguir:

1. Clique em **Padrões** > **Sistemas Virtuais**.
2. Na lista Padrões de Sistema Virtual, selecione **SOA Policy Gateway 2.0.0.0 - Governance Master**.
3. Clique no ícone Implementar.
4. Preencha os campos obrigatórios para implementar o padrão. Uma marca de seleção ao lado de cada item indica que ele não requer configuração adicional.
   a. Na caixa **Nome do Sistema Virtual**, insira um nome exclusivo para a instância.
   b. Configure os padrões virtuais. Clique em **Configurar Partes Virtuais**, em seguida, clique no nome da parte para abrir o editor para a parte:
      - "Parâmetros de Configuração da Parte de HADR Primário do DB2 Enterprise para o Padrão SOA Policy Gateway Governance Master pattern" na página 31
      - "Parâmetros de Configuração da Parte de Gerenciador de Implementação do WSRR para o Padrão SOA Policy Gateway Governance Master" na página 38
      - "Parâmetros de Configuração da Parte de Nós Customizados do WSRR para o Padrão SOA Policy Gateway Governance Master" na página 40
      - "Parâmetros de Configuração da Parte de HADR de Espera do DB2 Enterprise para o Padrão SOA Policy Gateway Governance Master" na página 34
5. Clique em **OK** para implementar o padrão.

O que Fazer Depois

Para verificar a implementação, consulte "Verificando a Implementação" na página 67.

Informações de Implementação do SOA Policy Gateway Governance Master

O Governance Master deve ser implementado antes dos padrões SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime serem implementados.

Sobre Esta Tarefa

As informações de implementação a partir da instância Governance Master são necessárias como entrada para valores de implementação para os padrões de tempo de execução.

Procedimento

Para localizar os valores necessários da instância do Governance Master:

1. Navegue para **Instâncias** > **Sistemas Virtuais**.
2. Selecione a instância Governance Master da implementação.
3. Expanda **Máquinas Virtuais**.
4. Expanda a máquina virtual denominada ***WSRRDMGR***.
5. Observe o seguinte:

- Na seção **Hardware e Rede**, anote o Nome do Host e o Endereço IP. O nome do host é o valor de **Interface de Rede 0**.
- Na seção **Configuração do WebSphere**, anote o nome da Célula.

Nota: O nome do host ou IP, o nome da célula e o nome de usuário administrativo e a senha do WebSphere usados durante a implementação do Governance Master são entradas necessárias para os parâmetros a seguir nos padrões SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime:

- WSRR_GOV_DMGR_hostname
- WSRR_GOV_DMGR_cellname
- WSRR_GOV_admin_user
- WSRR_GOV_admin_password

Implementando o Padrão SOA Policy Gateway Basic Runtime

A implementação do padrão SOA Policy Gateway Basic Runtime cria uma instância de sistema virtual em execução do padrão.

Antes de Iniciar

Conclua as seguintes etapas antes de implementar o padrão Basic Runtime:

- Configure o DataPower para IBM SOA Policy Gateway Pattern; consulte "Configurando o DataPower para as IBM SOA Policy Gateway Patterns" na página 53.
- Configure a Segurança para o IBM SOA Policy Gateway Pattern; consulte "Segurança para os Padrões IBM SOA Policy Gateway Pattern" na página 53.
- Configure o servidor SCP para hospedar arquivos de segurança.
- Obtenha as informações de implementação do Governance Master; consulte "Informações de Implementação do SOA Policy Gateway Governance Master" na página 64.

Sobre Esta Tarefa

A implementação de um padrão cria uma instância de sistema virtual que está em execução na nuvem.

Nota: Se você estiver usando o Perfil de Ativação de Controle (GEP), não será possível implementar simultaneamente um ambiente de produção e de temporariedade no padrão SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime. Isso ocorre porque ele pode causar conflito durante o processo de configuração de propriedades da promoção. Implemente o ambiente de temporariedade primeiro e, em seguida, o ambiente de produção.

Procedimento

Para implementar o padrão SOA Policy Gateway Basic Runtime, conclua as etapas a seguir:

1. Clique em **Padrões** > **Sistemas Virtuais**.
2. Na lista Padrões de Sistema Virtual, selecione **SOA Policy Gateway Basic Runtime 2.0.0.0**.
3. Clique no ícone Implementar.

4. Preencha os campos obrigatórios para implementar o padrão. Uma marca de seleção ao lado de cada item indica que ele não requer configuração adicional.
   a. Na caixa **Nome do Sistema Virtual**, insira um nome exclusivo para a instância.
   b. Configure os padrões virtuais. Clique em **Configurar Partes Virtuais**, em seguida, clique no nome da parte para abrir o editor para as partes e os scripts:
      - "Parâmetros de Configuração da Parte do DB2 Enterprise para o Padrão SOA Policy Gateway Basic Runtime" na página 27
      - "Parâmetros de Configuração da Parte de Servidor Independente do WSRR para o Padrão SOA Policy Gateway Basic Runtime" na página 36
      - "SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Segurança para o Padrão SOA Policy Gateway Basic Runtime" na página 48
      - "SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Promoção para o Padrão SOA Policy Gateway Basic Runtime" na página 43
      - "SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Domínio do DataPower para o Padrão SOA Policy Gateway Basic Runtime" na página 41
5. Clique em **OK** para implementar o padrão.

O que Fazer Depois

Para verificar a implementação, consulte "Verificando a Implementação" na página 67.

Implementando o Padrão SOA Policy Gateway Advanced Runtime

A implementação do padrão SOA Policy Gateway Advanced Runtime cria uma instância de sistema virtual em execução do padrão.

Antes de Iniciar

Conclua as seguintes etapas antes de implementar o padrão Advanced Runtime:

- Configure o DataPower para IBM SOA Policy Gateway Pattern; consulte "Configurando o DataPower para as IBM SOA Policy Gateway Patterns" na página 53.
- Configure a Segurança para o IBM SOA Policy Gateway Pattern; consulte "Segurança para os Padrões IBM SOA Policy Gateway Pattern" na página 53.
- Configure o servidor SCP para hospedar arquivos de segurança.
- Obtenha as informações de implementação do Governance Master; consulte "Informações de Implementação do SOA Policy Gateway Governance Master" na página 64.

Sobre Esta Tarefa

A implementação de um padrão cria uma instância de sistema virtual que está em execução na nuvem.

Nota: Se você estiver usando o Perfil de Ativação de Controle (GEP), não será possível implementar simultaneamente um ambiente de produção e de

temporariedade no padrão SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime. Isso ocorre porque ele pode causar conflito durante o processo de configuração de propriedades da promoção. Implemente o ambiente de temporariedade primeiro e, em seguida, o ambiente de produção.

Procedimento

Para implementar o padrão SOA Policy Gateway Advanced Runtime, conclua as etapas a seguir:

1. Clique em **Padrões** > **Sistemas Virtuais**.
2. Na lista Padrões de Sistema Virtual, selecione **SOA Policy Gateway 2.0.0.0 - Advanced Runtime**.
3. Clique no ícone Implementar.
4. Preencha os campos obrigatórios para implementar o padrão. Uma marca de seleção ao lado de cada item indica que ele não requer configuração adicional.
   a. Na caixa **Nome do Sistema Virtual**, insira um nome exclusivo para a instância.
   b. Opcional: Escolha o ambiente e planeje a implementação.
   c. Configure os padrões virtuais. Clique em **Configurar Partes Virtuais**, em seguida, clique no nome da parte para abrir o editor para as partes e os scripts:
      - "Parâmetros de Configuração da Parte de HADR Primário do DB2 Enterprise para o Padrão SOA Policy Gateway Advanced Runtime pattern" na página 30
      - "Parâmetros de Configuração da Parte de Gerenciador de Implementação do WSRR para o Padrão SOA Policy Gateway Advanced Runtime" na página 38
      - "SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Segurança para o Padrão SOA Policy Gateway Advanced Runtime" na página 49
      - "SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Promoção para o Padrão SOA Policy Gateway Advanced Runtime" na página 44
      - "SOA Policy Gateway 2.0.0.0 - Parâmetros de Configuração do Script de Domínio do DataPower para o Padrão SOA Policy Gateway Advanced Runtime" na página 42
      - "Parâmetros de Configuração da Parte de Nós Customizados do WSRR para o Padrão SOA Policy Gateway Advanced Runtime" na página 39
      - "Parâmetros de Configuração da Parte de HADR de Espera do DB2 Enterprise para o Padrão SOA Policy Gateway Advanced Runtime" na página 33
5. Clique em **OK** para implementar.

O que Fazer Depois

Para verificar a implementação, consulte "Verificando a Implementação".

Verificando a Implementação

Quando você tiver implementado o padrão, verifique se a implementação foi bem-sucedida.

Procedimento

1. Verifique os logs de implementação em busca de qualquer falha no histórico de implementação de sistema virtual. Para obter informações adicionais, consulte “Resolução de Problemas com a Implementação” na página 109.
2. Opcional: Se você tiver implementado o SOA Policy Gateway Basic Runtime Sample, teste a instância implementada seguindo o tutorial para enviar algumas mensagens de amostra usando os aplicativos de amostra fornecidos. Consulte o “Executando os Casos de Teste de Amostra” na página 73.

Cenário: Incluindo um Tempo de Execução Adicional ao Padrão

O Perfil de Ativação de Controle é fornecido com um sistema de classificação do ambiente predefinido que contém quatro ambientes distintos: Desenvolvimento, Teste, Temporariedade e Produção.

Sobre Esta Tarefa

Os ambientes de Temporariedade e Produção também são codificados no ciclo vida do SOA que define o ciclo de vida de Versões de Recurso, como Versões de Serviço. Isso significa que existem estados e transições que são específicos para os ambientes de Temporariedade e Produção, permitindo assim a promoção controlada para estes tempos de execução definindo os sistemas de destino no arquivo de configuração de promoção. Isso é apropriado se sua organização define ambientes da mesma forma, com Temporariedade como um ambiente de pré-produção que permite testar antes de permitir que a Versão do Recurso seja aberta para uso generalizado. Entretanto, muitas organizações requerem ambientes adicionais, portanto, as modificações são necessárias no perfil para acomodar essas diferenças. Esta seção descreve uma maneira de como um novo ambiente de tempo de execução pode ser incluso no Perfil de Ativação de Controle do WSRR.

Para obter informações adicionais sobre o planejamento de um ambiente de implementação, consulte “Planejando a Configuração do Padrão e Pré-requisitos do Padrão” na página 51.

Procedimento

1. Implemente o SOA Policy Gateway Governance Master predefinido. Para obter informações adicionais, consulte “Implementando o Padrão SOA Policy Gateway Governance Master” na página 63.
2. Opcional: Modifique o Perfil de Ativação de Controle do WSRR. Para obter informações adicionais, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Tutorial: Customizando Ambientes de Tempo de Execução.
3. Configure os padrões SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime com os detalhes do Governance Master. Para obter informações adicionais, consulte “Informações de Implementação do SOA Policy Gateway Governance Master” na página 64.

   Nota: O valor do ambiente de promoção deve ser configurado como “Não Configurado”.
4. Implemente o SOA Policy Gateway Basic Runtime ou o SOA Policy Gateway Advanced Runtime predefinido. Para obter mais informações, consulte “Implementando o Padrão SOA Policy Gateway Basic Runtime” na página 65 e “Implementando o Padrão SOA Policy Gateway Advanced Runtime” na página 66.

Clonando e Customizando o IBM SOA Policy Gateway Pattern

O IBM SOA Policy Gateway Pattern não pode ser editado. Se a topologia fornecida nos padrões de sistema virtual do IBM SOA Policy Gateway Pattern não fornecer a função necessária, o padrão poderá ser clonado e, em seguida, editado para criar novos padrões.

Sobre Esta Tarefa

É possível customizar os padrões das maneiras a seguir:

- Incluindo domínios adicionais do DataPower. Para obter informações adicionais, consulte "Implementando com Vários Domínios DataPower" na página 70.
- Aumentando o tamanho do cluster padrão. Para obter informações adicionais, consulte Centro de Informações do IBM Workload Deployer, Versão 3.1.

  Nota: Ao expandir o tamanho do cluster, aumente o tamanho da memória do WSRR Deployment Manager também.
- Permitir que você escolha a maneira de ter o arquivo de segurança compactado no servidor. Para obter informações adicionais, consulte "Gerenciamento da Segurança" na página 54.
- Permitir que você defina e bloqueie seus próprios valores padrão; por exemplo, o ID de administrador do DataPower. Para obter mais informações sobre o bloqueio de parâmetros, consulte Centro de Informações do IBM Workload Deployer, Versão 3.1.
- Permitir que você use seu próprio mecanismo para fazer o download do arquivo `DomainZipFile.zip`. Para obter informações adicionais, consulte "Fornecendo seu Próprio Mecanismo para Fazer Download do Arquivo `DomainZipFile.zip`" na página 59.

Procedimento

Para clonar os padrões para editá-los e criar novos padrões, conclua as etapas a seguir:

1. No painel esquerdo da janela Padrão, selecione o padrão a ser clonado.
2. Clique no ícone Clonar e forneça um nome para o novo padrão. Também é possível fornecer informações adicionais, como uma descrição.
3. Selecione o novo padrão e clique no ícone Editar para alterar a configuração. É possível incluir e remover partes e configurá-las, aumentar ou diminuir o número de algumas partes ou alterar a ordem em que algumas partes são implementadas.

O que Fazer Depois

Assegure-se de que você tenha todas as partes necessárias configuradas adequadamente para o tipo de padrão criado. Será possível implementar o padrão quando sua configuração estiver concluída.

Informações relacionadas:

IBM Workload Deployer: Gerenciando Padrões de Sistema Virtual

IBM PureApplication System: Gerenciando Padrões de Sistema Virtual

Implementando com Vários Domínios DataPower

Os padrões SOA Policy Gateway Basic Runtime e SOA Policy Gateway Advanced Runtime podem ser clonados e customizados para incluir vários domínios DataPower.

Procedimento

1. Clone o padrão SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime. Para obter informações adicionais, consulte "Clonando e Customizando o IBM SOA Policy Gateway Pattern" na página 69.
2. Para editar o padrão, clique em **Editar**.
3. Expanda a seção **Scripts**.
4. Para cada domínio adicional a ser incluído, arraste e solte o pacote de scripts **Domínio DataPower do SOA Policy Gateway 2.0.0.0** para a parte do gerenciador de implementação do WSRR para o padrão Advanced Runtime, ou para a parte do WSRR Independente para o padrão Basic Runtime.
5. Clique em **Concluir Edição**.
6. Implemente o padrão, inserindo as informações a seguir para cada domínio incluído:
   - DataPower_hostname
   - DataPower_XML_mgmt_port
   - DataPower_admin_id
   - DataPower_admin_password
   - Verificar senha
   - New_DataPower_domain
   - securityFileCleanUp

   Nota: Ao usar vários domínios, o último deles deve ter o valor securityFileCleanUp configurado como **`true`** e todos os outros domínios devem ter o valor configurado como **`false`**.

   Para obter mais informações sobre a implementação dos padrões, consulte "Implementando o Padrão SOA Policy Gateway Basic Runtime" na página 65 ou "Implementando o Padrão SOA Policy Gateway Advanced Runtime" na página 66.

O Aplicativo de Amostra

O aplicativo de amostra é um Domínio do DataPower configurável e um conjunto de Artefatos do WSRR que podem ser usados para demonstrar os recursos do padrão.

O cenário básico no aplicativo de amostra é um aplicativo de inventário para um armazenamento (Warehouse). Há um serviço da web Store que tem três operações:

- purchase
- findInventory
- returnProduct

A definição de nível de serviço (SLD) básica contém duas políticas de mediação:

- Validação contra Store.wsdl. Isto supõe que a Validação de DataPower esteja desativada.
- Rejeite se houver mais de 5 mensagens em 90 segundos. Este é um limite baixo para demos fáceis.

Os consumidores desse serviço têm atualmente dois Acordos de Nível de Serviço (SLAs), Ouro e Anônimo. Se o contexto de cliente no cabeçalho de HTTP for Ouro, eles serão roteados para o Terminal Alternativo imediatamente. Se eles forem anônimos, que é atualmente não ouro, eles acessarão o Terminal de Serviço de Simulação de Armazenamento que possui um valor de preço diferente para o item.

O cenário também executa a autorização para a operação findInventory, com base na associação ao grupo de usuários. Figura 5 mostra o fluxo do aplicativo com cada caixa representando um gateway do DataPower diferente.

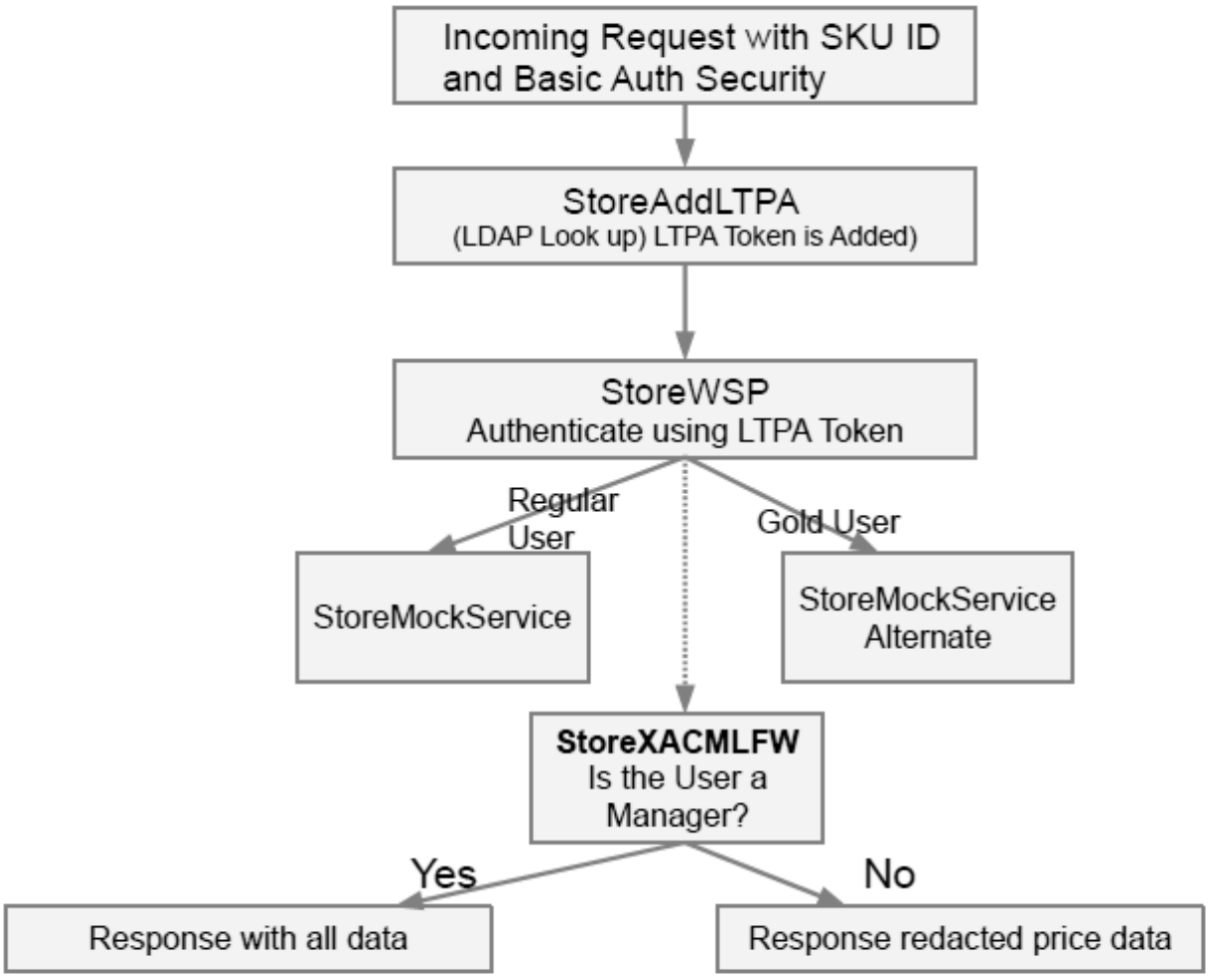


Figura 5. O Fluxograma do Aplicativo de Amostra

Tarefas relacionadas:

"Clonando e Customizando o IBM SOA Policy Gateway Pattern" na página 69
O IBM SOA Policy Gateway Pattern não pode ser editado. Se a topologia fornecida nos padrões de sistema virtual do IBM SOA Policy Gateway Pattern não fornecer a função necessária, o padrão poderá ser clonado e, em seguida, editado para criar novos padrões.

Visão Geral de Artefatos do WSRR na Amostra

Os artefatos do WSRR descrevem a operação de warehousing.

Existem quatro recursos básicos de negócios para Warehouse, que fazem parte da maior Organização Warehouse do Bob. A versão de serviço, Store V1.0, representa o serviço Store. A definição de nível de serviço (SLD) do Store tem dois acordos de nível de serviço (SLAs); uma para usuários Gold que os direciona para um serviço preferencial alternativo, e o SLA de Usuários Anônimos que se destina a todos os outros usuários e, simplesmente, efetua logon de uma notificação no DataPower em que a solicitação foi feita. O SLD de Armazenamento também tem duas outras políticas de amostra anexadas; a primeira política rejeita mensagens após 5 mensagens em 90 segundos e a segunda política executa a validação com relação ao esquema Store.wsdl.

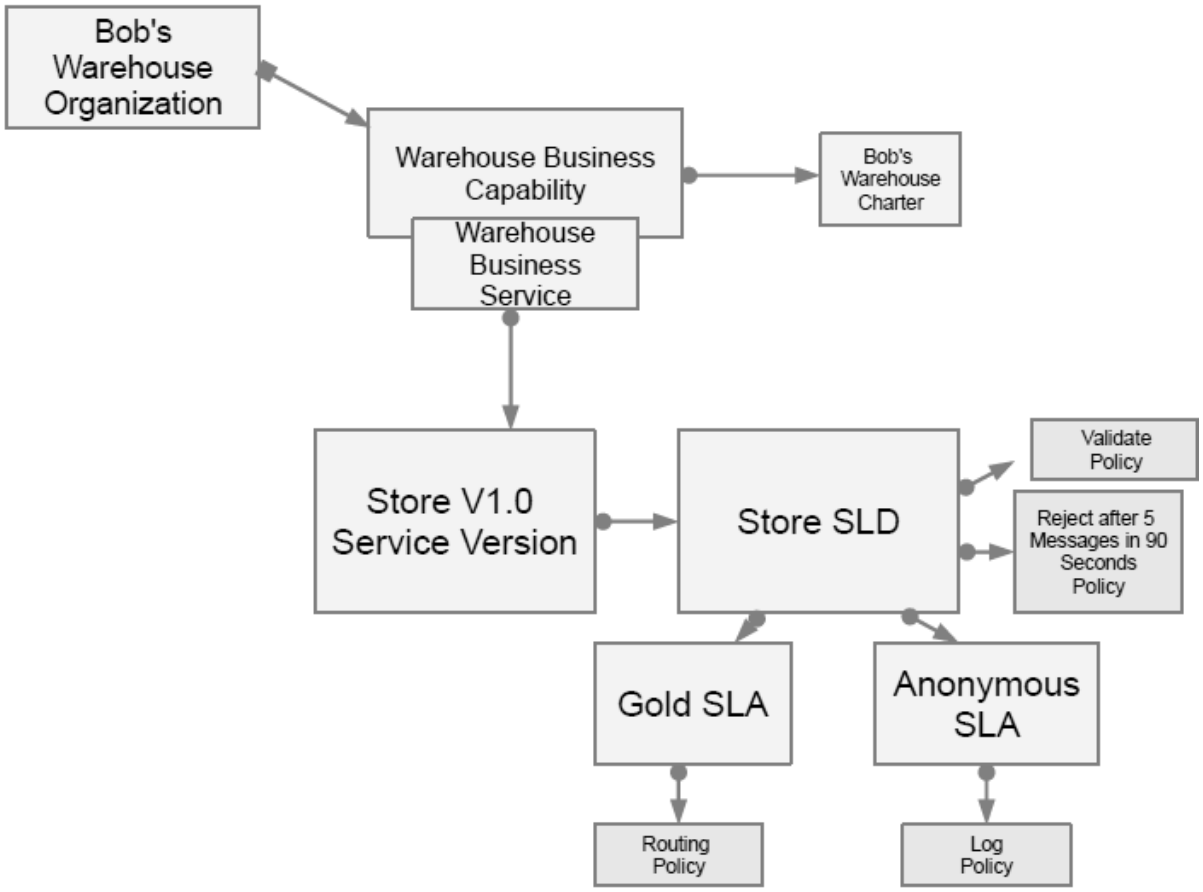


Figura 6. O Domínio de Amostra

Executando os Casos de Teste de Amostra

É possível usar o aplicativo da web de amostra ou a linha de comandos para testar o aplicativo Sample no SOA Policy Gateway Basic Runtime Sample implementado. Há seis variações de teste de linha de comandos que podem ser executadas no aplicativo de amostra.

Para implementar o Basic Sample Runtime, consulte “Implementando o Padrão SOA Policy Gateway Basic Runtime Sample” na página 62.

Nota: O valor de `SamplePolicySample_starting_port` usado nas amostras de XML a seguir é encontrado nos logs do SOA Policy Gateway Basic Runtime Sample.

Executando o caso de teste do aplicativo da web de amostra

Para executar o caso de teste do aplicativo da web:

1. Localize o nome do host do ambiente implementado no WSRR abrindo a Instância do Sistema Virtual implementado. Para fazer isso, expanda a seção **Máquinas Virtuais** e selecione a máquina virtual para que o WSRR Standalone Server veja os detalhes da máquina virtual. Na seção **Hardware e Rede**, o nome do host é o valor **Interface de Rede 0**.
2. Abra a URL em um navegador da web: `http://<wssrHostName>:9080/SoaPolicyTester`
3. A tela de teste para o aplicativo de amostra implementado no DataPower é exibida.
4. As opções são:
   - **Envio Padrão** - Envia uma solicitação findInventory para o serviço de armazenamento. O ID do contexto é um usuário “Silver”. Um resultado bem-sucedido é `Peça: SKU10 Preço: 461,73`.
   - **Envio Roteado** - Envia uma solicitação findInventory para o serviço de armazenamento. O ID de contexto é um usuário “Gold”, portanto a solicitação é roteada para uma implementação Gold do serviço. Um resultado bem-sucedido é `Peça: GOLDSKU10 Preço: 461,73`.
   - **Envio Inválido** - Envia uma solicitação com uma carga útil inválida. A política de validação requer o DataPower para validar a solicitação e um resultado de êxito será uma mensagem de resposta do DataPower `"Erro Interno (do cliente)"`.
   - **ID do Usuário = Consumidor A** - Para as chamadas com um ID do Usuário igual a Consumidor A, a política XACML é impingida para que somente os Gerentes possam ver o preço. O valor de Preço na mensagem de resposta será separado. Um resultado bem-sucedido contém `Preço: 0,0`.
   - **Muitas Solicitações Padrão** - Se mais de cinco solicitações forem executadas dentro de 90 segundos, a política de rejeição será impingida. Uma resposta bem-sucedida demonstrando a política que está sendo impingida é: `Rejeitada: "Rejeitada (do cliente)"`.
5. Abra o console do WSRR e explore o serviço e as políticas. Para obter informações adicionais, consulte .

Para executar os casos de teste do aplicativo de amostra usando a linha de comandos:

Demonstrando o XACML de Permissão/Negação com o Cenário de Edição de Dados usando a Linha de Comandos

O XML de solicitação a seguir pode ser enviado ao Serviço StoreAddLTPA do DataPower:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:stor="http://company.ibm.com/store">
  <soapenv:Header>
    <store:ConsumerIdentifier xmlns:store="http://store.com">CEO
    </store:ConsumerIdentifier>
    <store:ContextIdentifier xmlns:store="http://store.com">silver
    </store:ContextIdentifier>
  </soapenv:Header>
  <soapenv:Body>
  <stor:findInventory>
    <findInventoryReq>
      <sku>SKU10</sku>
    </findInventoryReq>
  </stor:findInventory>
  </soapenv:Body>
</soapenv:Envelope>
```

Supondo que o XML de solicitação de exemplo acima esteja contido em um arquivo denominado `silver.xml`, execute o comando curl a seguir:

```
curl -k --data-bin @./silver.xml -H "Content-Type: text/xml"
-u ConsumerX:passw0rd http://<yourDataPowerHostName>.com:<SamplePolicySample_starting_port+4>/Store/Store
```

Neste exemplo, ConsumerX é um Gerente, portanto, veremos as informações completas sobre preço como a resposta:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<KD4NS:KD4SoapHeaderV2
xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0z
YjU0LWEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxN
mRhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2>
</soapenv:Header>
<soapenv:Body>
  <b:findInventoryResponse xmlns:a="http://company.ibm.com/"
     xmlns:b="http://company.ibm.com/store">
  <findInventoryRes>
<sku>SKU10</sku>
<price>461.73</price>
<inventory>460</inventory>
<msrp>923.46</msrp>
<supplierID>IBM</supplierID>
</findInventoryRes>
</b:findInventoryResponse>
</soapenv:Body></soapenv:Envelope>
```

Executando o Cenário de Edição de Dados usando a Linha de Comandos

ConsumerA não é um gerente, portanto, veremos uma resposta diferente. Execute o comando curl:

```
curl -k --data-bin @./silver.xml -H "Content-Type: text/xml"
-u ConsumerA:passw0rd http://<yourDataPowerHostName>.com:<SamplePolicySample_starting_port+4>/Store/Store
```

Observe que a resposta tem preço com dados editados e é 0.0:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header><KD4NS:KD4SoapHeaderV2
xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0zYjU0L
WEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxNm
RhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2>
</soapenv:Header>
<soapenv:Body>
<b:findInventoryResponse xmlns:a="http://company.ibm.com/"
```

```
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
<sku>SKU10</sku>
<price>0.0</price>
<inventory>460</inventory>
<msrp>923.46</msrp>
<supplierID>IBM</supplierID>
</findInventoryRes>
</b:findInventoryResponse>
</soapenv:Body></soapenv:Envelope>
```

Testando a Política de Roteamento Usando a Linha de Comandos

O ContextId do SLA é usado para acionar a Política de Roteamento. Neste caso, o SLA para Clientes Ouro tem o valor de "Gold" no SLA. Este é o conteúdo de uma solicitação de amostra com Gold como o contextIdentifier:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:stor="http://company.ibm.com/store">
<soapenv:Header>
  <store:ConsumerIdentifier xmlns:store="http://store.com">CEO
  </store:ConsumerIdentifier>
  <store:ContextIdentifier xmlns:store="http://store.com">Gold
  </store:ContextIdentifier>
</soapenv:Header><soapenv:Body>
<stor:findInventory><findInventoryReq>
  <sku>SKU10</sku>
  </findInventoryReq>
</stor:findInventory>
</soapenv:Body></soapenv:Envelope>
```

Supondo que o XML de solicitação de exemplo acima esteja contido em um arquivo denominado `gold.xml`, execute o comando curl a seguir:

```
curl -k --data-bin @./gold.xml -H "Content-Type: text/xml"
-u ConsumerX:passw0rd http://<yourDataPowerHostName>.com:<SamplePolicySample_starting_port+4>/Store/Store
```

A resposta é a seguinte:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
  <KD4NS:KD4SoapHeaderV2
  xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0zYjU0L
  WEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxNm
  RhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2>
</soapenv:Header><soapenv:Body>
<b:findInventoryResponse xmlns:a="http://company.ibm.com/"
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
  <sku>GOLDSKU10</sku>
  <price>461.73</price>
  <inventory>460</inventory>
  <msrp>923.46</msrp>
  <supplierID>IBM</supplierID>
</findInventoryRes></b:findInventoryResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Observe que a resposta de retorno tem um `GOLDSKU` para o valor de SKU, indicando que o terminal ouro foi usado.

Testando a Validação do Esquema Usando a Linha de Comandos

A política de validação verifica o esquema da solicitação com relação ao Store.wsl e seu Company.xsd associado.

O XML a seguir, `badvalid.xml`, mostra uma solicitação que é inválida porque o corpo contém um elemento denominado `<skubad>` quando deveria ser `<sku>`:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:stor="http://company.ibm.com/store">
<soapenv:Header>
<store:ConsumerIdentifier xmlns:store="http://store.com">CEO</store:ConsumerIdentifier>
<store:ContextIdentifier xmlns:store="http://store.com">silver</store:ContextIdentifier>
</soapenv:Header>
<soapenv:Body>
<stor:findInventory>
<findInventoryReq>
<skubad>SKU10</skubad>
</findInventoryReq>
</stor:findInventory>
</soapenv:Body></soapenv:Envelope>
```

Se executarmos a solicitação curl a seguir:

```
curl -k --data-bin @./badvalid.xml -H "Content-Type: text/xml"
-u ConsumerX:passw0rd
http://<yourDataPowerHostName>.com:<SamplePolicySample_starting_port+4>/Store/Store
```

Isso produzirá o erro a seguir:

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
<env:Body>
<env:Fault><faultcode>env:Client</faultcode>
<faultstring>Erro interno (do cliente)</faultstring>
</env:Fault>
</env:Body>
</env:Envelope>
```

Testando a Rejeição na Política de Mediação Usando a Linha de Comandos

Uma das políticas de mediação incluídas na amostra testa a rejeição depois que a contagem de mensagens foi executada 5 vezes em 90 segundos. Execute o comando a seguir 6 vezes:

```
curl -k --data-bin @./silver.xml -H "Content-Type: text/xml" -u ConsumerX:passw0rd
http://<yourDataPowerHostName>.com:<SamplePolicySample_starting_port+4>/Store/Store
```

A solicitação de amostra é a seguinte:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<KD4NS:KD4SoapHeaderV2
xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0z
YjU0LWEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxN
mRhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2>
</soapenv:Header>
<soapenv:Body>
<b:findInventoryResponse xmlns:a="http://company.ibm.com/"
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
```

Neste caso, ConsumerX é um Gerente, portanto, as informações completas de preços serão exibidas abaixo para as cinco primeiras execuções:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<KD4NS:KD4SoapHeaderV2
xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0z
YjU0LWEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxN
mRhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2>
</soapenv:Header>
<soapenv:Body>
<b:findInventoryResponse xmlns:a="http://company.ibm.com/"
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
<sku>SKU10</sku>
<price>461.73</price>
```

```
<inventory>460</inventory>
<msrp>923.46</msrp>
<supplierID>IBM</supplierID>
</findInventoryRes></b:findInventoryResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Na sexta execução, você verá o erro a seguir:

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope
xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
<env:Body>
<env:Fault>
<faultcode>env:Client</faultcode>
<faultstring>Rejeitado (do cliente)</faultstring>
</env:Fault>
</env:Body>
</env:Envelope>
```

Nota: É possível ver esse erro antes se você executou outros testes dentro do intervalo de 90 segundos.

Testando a Notificação na Política de Mediação Usando a Linha de Comandos

No caso em que o contextId não é "Gold", não há nenhum SLA mapeado e o SLA Anônimo é utilizado. A política do mediação para o SLA Anônimo é registrar ou notificar. Isso requer que o Modo de Depuração seja ativado para o Domínio de Amostra. Execute o comando a seguir:

```
curl -k --data-bin @./silver.xml -H "Content-Type: text/xml" -u ConsumerX:passw0rd
http://<yourDataPowerHostName>.com:<SamplePolicySample_starting_port+4>/Store/Store
```

Neste exemplo, ConsumerX é um Gerente, portanto, veremos as informações integrais sobre preço, conforme a seguir:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<KD4NS:KD4SoapHeaderV2
xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0zYjU0L
WEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxNm
RhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2></soapenv:Header><soapenv:Body><b:fin
dInventoryResponse xmlns:a="http://company.ibm.com/"
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
<sku>SKU10</sku>
<price>461.73</price>
<inventory>460</inventory>
<msrp>923.46</msrp>
<supplierID>IBM</supplierID>
</findInventoryRes>
</b:findInventoryResponse>
</soapenv:Body>
</soapenv:Envelope>
```

A mensagem a seguir é gerada no log padrão do Domínio:

```
Notificar ação acionada ('operation_38_2_sla1-1-filter_1-notify') pela política de origem
  ('LogEveryTime_287d0790-83d9-11e1-a255-9187e20cddb0_05aec6ec-3674-4165-85de-a0f7be48a938'
```

Nota: A criação de log deve estar configurada para depuração para ver essa mensagem. Se não estiver, clique no ícone Resolução de Problemas no Console da Web do DataPower. Na seção Criação de Log, altere o valor de Nível de Log para "debug" e clique em **Configurar Nível de Log**.

Para localizar o log, selecione **Arquivos** e **Administração de Arquivos** > **Gerenciamento de Arquivos**. O log está localizado na pasta `logtemp` e nomeado `default-log`. Devido ao agrupamento do log, pode ser necessário colocar o arquivo

de log em uma janela do navegador da web antes de executar o teste e atualizar a guia no navegador depois de executar o teste.

Tarefas relacionadas:

"Implementando o Padrão SOA Policy Gateway Basic Runtime Sample" na página 62

A implementação do padrão SOA Policy Gateway Basic Runtime Sample cria uma instância de sistema virtual em execução do padrão.

Estendendo o Aplicativo de Amostra

O aplicativo de amostra pode ser modificado alterando a folha de estilo Ligações e as folhas de estilo XSL.

Modificações na Folha de Estilo de Ligações

A variável xacml-subjects foi inclusa na folha de estilo `apil-xacml-binding-new.xsl`. Ela inclui a criação da seção de assuntos da solicitação. Essa variável é acessada posteriormente no `sendToPDP.xsl`.

```
<xsl:variable name="xacml-subjects">
<xacml-context:Subject SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<!--
***********************************************
Iniciando aqui, use o resultado do MC como assunto.
***********************************************
```

sendToPDP.xsl

Essa folha de estilo chama o StoreXACMLFW usando url-open. A chamada está na caixa para outro Firewall XML, portanto, nenhum perfil Proxy SSL é usado. Se fosse desejado mover o Policy Decision Point (PDP) para outra caixa do DataPower, um perfil Proxy SSL poderia ter sido criado e usado com a chamada url-open.

```
<xsl:param name="resource" />
<!--
<xsl:variable name="incoming_resource">
<xsl:value-of select="$resource" />
</xsl:variable>
<xsl:message dp:priority="debug">
********** PRESTES A CHAMAR O PDP para RECURSO igual *************
<xsl:value-of select="$incoming_resource" />
</xsl:message>
-->
- <!--
construindo a solicitação XACML para mascaramento
-->
<xsl:variable name="customized-request">
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header />
<soapenv:Body>
<xacml-context:Request xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:ws="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
- <!--
copiar nos assuntos salvos do processamento de solicitação AAA
-->
<xsl:copy-of select="dp:variable('var://context/snip/xacml/xacmlSubjects')/*" />
<xacml-context:Resource>
<xacml-context:ResourceContent>
<xsl:copy-of select="./soap:Envelope/soap:Body" />
</xacml-context:ResourceContent>
<xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
<xacml-context:AttributeValue>PriceInfo</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Resource>
<xacml-context:Action>
<xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
<xacml-context:AttributeValue>View</xacml-context:AttributeValue>
```

```
</xacml-context:Attribute>
</xacml-context:Action>
<xacml-context:Environment>
<xacml-context:Attribute AttributeId="ContextId" DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="http://security.tivoli.ibm.com/policy/distribution">
<xacml-context:AttributeValue>StorePriceData</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Environment>
</xacml-context:Request>
</soapenv:Body>
</soapenv:Envelope>
</xsl:variable>
- <!--
Use set-variable para que fique visível na Análise, o que é conveniente
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlRequest'" value="$customized-request" />
- <!--
Relate o XACML-REQUEST no log de depuração
-->
<xsl:message dp:priority="debug">
<XACML-REQUEST>
<xsl:copy-of select="$customized-request" />
</XACML-REQUEST>
</xsl:message>
<xsl:variable name="headers">
<header name="SOAPAction">xacml:authorization</header>
</xsl:variable>
- <!--
Chame o PDP XACML para decisão
-->
<xsl:variable name="rtss-response">
<xsl:variable name="StoreGWURL">
<xsl:value-of select="concat('http://','127.0.0.1',':',$StoreGWPort,'/rtss/authz/services/AuthzService')" />
</xsl:variable>
<dp:url-open target="{$StoreGWURL}" http-headers="$headers" response="responsecode">
<xsl:copy-of select="$customized-request" />
</dp:url-open>
</xsl:variable>
- <!--
Use set-variable para que fique visível na Análise, o que é conveniente
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlResponse'" value="$rtss-response" />
- <!--
Relate o XACML-RESPONSE no log de depuração
-->
<xsl:message dp:priority="debug">
<XACML-RESPONSE>
<xsl:value-of select="$rtss-response" />
</XACML-RESPONSE>
</xsl:message>
</xsl:template>
</xsl:stylesheet>
```

Se examinarmos o arquivo `sendToPDP.xsl`, devemos observar os itens a seguir:

1. A folha de estilo obtém a porta para o XACMLFW do `soavars.xsl`.
2. A variável rtssResponse deve ser exatamente da forma que os Serviços de Segurança de Tempo de Execução usariam e, por sua vez, da forma que o PDP na caixa do DataPower pode processar.
3. A folha de estilo constrói uma solicitação SOAP:
   - As informações de assunto são construídas pela folha de estilo `apil-binding.xsl` anterior e são obtidas pela solicitação de cópia de seleção a seguir:

```
<xsl:copy-of select="dp:variable('var://context/snip/xacml/xacmlSubjects')/*" />
```

4. Esta ação é simplesmente para visualizar a ação: `<xacml-context:AttributeValue>View</xacml-context:AttributeValue>`
5. O ambiente é o StorePriceData, conhecido como um objeto do aplicativo na terminologia do IBM Tivoli Security Policy Manager ou dos Serviços de Segurança de Tempo de Execução.

Vamos examinar a folha de estilo de política para edição de dados.

StorePrivateDataXACML.xml

```
<PolicySet PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides"
PolicySetId="RPS:StorePrivateData:policy:dc703409-d408-49b3-acc1-16c89c844fce:rolec4a9f664-a0af-451b-b80b-
1cafdb9fd9f0:role:2884ab77-58d1-4b1d-8728-7d528169d608" Version="1.0">
<Target>
<Subjects>
<Subject>
<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">MANAGER</xacml:AttributeValue>
<SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
DataType="http://www.w3.org/2001/XMLSchema#string"
SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:accesssubject"
/>
</SubjectMatch>
</Subject>
</Subjects>
</Target>
<Policy PolicyId="PPS:StorePrivateData:dc703409-d408-49b3-acc1-16c89c844fce:c4a9f664-a0af-451b-b80b-1cafdb9fd9f0:c4a9f664-
a0af-451b-b80b-1cafdb9fd9f0:pps" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable"
Version="1.0">
<Target>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">PriceInfo</xacml:AttributeValue>
<ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">View</xacml:AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ActionMatch>
</Action>
</Actions>
</Target>
<Rule Effect="Permit" RuleId="PPS:StorePrivateData:dc703409-d408-49b3-acc1-16c89c844fce:c4a9f664-a0af-451b-b80b-
1cafdb9fd9f0:c4a9f664-a0af-451b-b80b-1cafdb9fd9f0:pps:rules:0">
<Target />
</Rule>
</Policy>
</PolicySet>
</PolicySet>
```

Observe o seguinte:

- A Função deve ser Gerente:

```
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">MANAGER</xacml:AttributeValue>
```

- O Recurso deve ser PriceInfo:

```
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
 xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">PriceInfo</xacml:AttributeValue>
```

- A Ação deve ser Visualizar:

```
<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
 xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">View</xacml:AttributeValue>
```

Modificando as Folhas de Estilo XSL de Amostra

Há vários pontos em que é possível modificar os scripts `.xsl` usados no aplicativo.

Procedimento

Para modificar as folhas de estilo XSL de amostra, é possível:

1. Modifique o mapeamento de credencial para AZ.

   Abra a folha de estilo `rgxacml.xsl` e conclua as instruções XSL a seguir:

```
<!-- Especifique seu Servidor LDAP -->
<xsl:variable name="server"><xsl:copy-of select="$LDAPHost"/></xsl:variable>
<xsl:variable name="bindDN"><xsl:copy-of select="$LDAPCN"/></xsl:variable>
<xsl:variable name="bindPassword"><xsl:copy-of
select="$LDAPPassword"/></xsl:variable>
<xsl:variable name="port"><xsl:copy-of select="$LDAPPort"/></xsl:variable>
```

   As variáveis a seguir são definidas na folha de estilo `soavars.xsl`:

```
<xsl:variable name="LDAPHost" select='"yourldap.something.com"' />
<xsl:variable name="LDAPPort" select='"389"' />
<xsl:variable name="LDAPCN" select='"cn=root"' />
<xsl:variable name="LDAPPassword" select='"passw0rd"' />
<xsl:variable name="StoreGWHost" select='"yourDatapowerName"' />
<xsl:variable name="StoreGWPort" select='"62151"' />
```

   A amostra contém uma senha não criptografada para o servidor LDAP, pode ser que você deseje customizar a folha de estilo fornecida para decriptografar uma senha criptografada.

```
<!-- Especifique o DN base para iniciar a procura -->
<xsl:variable name="baseDN">dc=ibm.com</xsl:variable>
```

   O `baseDN` é codificado permanentemente como `dc=ibm.com`. Se você tiver configurado seu LDAP com um sufixo diferente, baseDN, altera essa linha para customizar a amostra.

2. Modifique a folha de estilo de Edição de Dados.

   A folha de estilo `noPriceInfo.xsl` contém o código a seguir, que irá zerar quaisquer valores de preço. É possível incluir outros campos na lógica de edição de dados ou incluir transformações mais complicadas que envolvam cálculo para determinar valores para campos.

```
<!-- campos de acesso privado apenas -->
<xsl:template match="price">
<price>0.0</price>
</xsl:template>
<xsl:template match="Price">
<Price>0.0</Price>
</xsl:template>
```

   Posteriormente, a folha de estilo executa uma transformação de identidade em todos os outros elementos.

Exploração Adicional da Amostra

Para saber mais sobre a amostra, você pode configurar o XACML Policy Decision Point (PDP) no DataPower e editar documentos de política.

Alterando o PDP XACML no DataPower

É possível explorar alteração no XACML usado para o Policy Decision Point (PDP) de segurança no DataPower para saber mais sobre controle de acesso com o XACML.

Procedimento

Para alterar ou incluir um PDP:

1. No Painel de Controle do DataPower, procure `PDP XACML`.
2. Clique em um PDP existente ou clique em **Incluir**.

3. Insira uma URL; por exemplo, `local:///storePrivateDataXACML.xml`
4. Inclua quaisquer arquivos dependentes ou de diretório necessários para suportar a política.

   Nota: Se você editar um arquivo de políticas XACML diretamente no sistema de arquivos, deverá voltar para a definição de PDP e inserir novamente a URL, ou qualquer coisa que tenha sido alterada, ou reiniciar o domínio para que sua mudança entre em vigor.

Editando Documentos de Política

Use a interface com o usuário do Business Space para editar documentos de política.

Antes de Iniciar

Configure o espaço Controle SOA. Para obter informações adicionais, consulte "Configurando o Business Space para o Primeiro Uso" na página 93.

Procedimento

1. Crie uma política de mediação com as condições e ações necessárias; por exemplo, uma condição de Contagem de Mensagens > 5 mensagens em 5 minutos e uma ação de rejeição. Para obter informações adicionais sobre como criar uma política de mediação, consulte "Criando Novas Políticas" na página 106.
2. Clique em **Concluir**. A visualização Procurar é exibida
3. Controle a política de mediação. Para obter informações adicionais sobre como controlar um documento sobre políticas, consulte "Gerenciando o Ciclo de Vida da Política" na página 108.
   a. Clique no documento sobre políticas no Navegador do Registro de Serviço ou procure por ele no widget de procura. As ações são exibidas no Editor de Documento sobre Políticas.
   b. Clique em **Propor Especificação**.
   c. Clique em **Aprovar Especificação**.

   A política é aprovada. É possível redefinir, substituir ou descontinuar a política para gerenciar o ciclo de vida ou editar uma definição existente.

Tarefas relacionadas:

"Criando Novas Políticas" na página 106
Ao criar políticas de mediação na interface com o usuário do Business Space, especifique as condições e ações para a política.

"Gerenciando o Ciclo de Vida da Política" na página 108
É possível executar a transição de políticas entre os estados de controle usando a interface com o usuário do Business Space.

Informações relacionadas:

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Using the Business Space user interface

O Domínio de Amostra do DataPower

O padrão fornece um domínio de amostra do DataPower, que permite começar a usar o padrão. Como um desenvolvedor do DataPower, é possível usar os gateways existentes como um modelo para seus próprios aplicativos. O ambiente de amostra contém cinco gateways. Há um gateway primário para o serviço de Armazenamento e quatro gateways de apoio fornecem backends de exemplo para

serem chamados pelo Gateway de Armazenamento, suporte XACML para um cenário de edição de dados e um front-end para fornecer funcionalidade de segurança adicional.

Store Web Service Proxy

O Store Web Service Proxy (WSP) é o gateway primário do domínio de aplicativo. Ele recebe uma solicitação com um token LTPA anexado.

Quando solicitado, a regra de processamento da solicitação conclui as ações a seguir:

1. Valida a solicitação, conforme solicitado pela política de Validação. Para obter informações adicionais, consulte "Visão Geral de Artefatos do WSRR na Amostra" na página 72.
2. Direciona a solicitação para o terminal alternativo se o acordo de nível de serviço (ANS) é "Gold".
3. Autentica, conclui a autorização e a contabilidade (AAA) na solicitação. Isso inclui as ações a seguir:
   a. Autentica o usuário com um token LTPA.
   b. Mapeia as credenciais com relação ao servidor LDAP, que fornece informações sobre a quais grupos o cliente pertence. Esses grupos incluem Gerente, Funcionário e Cliente.
   c. Transforma as entradas fornecidas em um objeto da solicitação que o ponto de decisão de política (PDP) XACML pode entender.
   d. Conclui a autorização usando um PDP XACML na caixa DataPower com um documento sobre políticas XACML que podem ser criados no IBM Tivoli Security Policy Manager. Os critérios da política são que o usuário deve ser um Gerente, Cliente ou Funcionário. Para a operação findInventory, os retornos requerem Gerente ou Funcionário e as compras podem ser executadas pelos clientes.
4. Configura o valor de ConsumerID usando um script XSL.
5. Remove o Cabeçalho de Segurança HTTP inteiro da solicitação.
6. Chama o back end do serviço Store.

Quando a solicitação é processada, a regra de processamento de resposta conclui as ações a seguir:

1. Chama o gateway StoreXACMLFW, que age como o PDP no cenário.
2. Com base na resposta, o campo de informações de preço tem os dados editados (zerado) dependendo se o usuário tem a função de Gerente ou não.

Firewalls XML na Amostra

Os firewalls XML a seguir estão definidos na amostra.

Firewall XML StoreAddLTPA

A função do Firewall XML StoreAdd LTPA é fornecer um front-end com uma porta que os usuários podem chamar usando apenas Autenticação Básica (por exemplo, nenhum LTPA ou similar). A regra de processamento da solicitação:

1. Identifica com Autenticação Básica.
2. Autentica com uma consulta LDAP muito simples.
3. Inclui um token LTPA como parte do pós-processamento.
4. Encaminha a solicitação para a política de segurança StoreWSP com as informações de LTPA agora anexadas.

Firewall XML StoreMockService

O StoreMockService é um serviço de exemplo que usa um Firewall XML como uma implementação. As operações findInventory, comprar e retornar são todas suportadas. Os valores de respostas são estáticos. Esse serviço de exemplo é criado quando não é possível incluir um WebSphere Application Server no padrão. As três regras de solicitação da política usam uma ação correspondente para determinar a operação de solicitação e, com base em uma correspondência, responde a uma resposta SOAP estática. As respostas SOAP estáticas são fornecidas com base na operação de solicitação em vez de uma implementação de serviço integral.

Firewall XML StoreMockServiceAlternate

O StoreMockServiceAlternate é um serviço de exemplo que usa um Firewall XML como uma implementação. As operações findInventory, comprar e retornar são todas suportadas. Esse serviço é usado para demonstrar a política de roteamento que está sendo impingida.

Firewall StoreXACMLFW

Este cenário executa a edição de dados com base no resultado de um mecanismo de permissão/negação baseado em XACML. No DataPower, não há uma maneira de chamar uma ação AAA individual no fluxo de resposta. Um gateway separado é criado para conter o Policy Decision Point (PDP) XACML. Esse PDP foi encapsulado em uma ação AAA na regra de solicitação do StoreXACMLFW.

StoreXACMLFW é um gateway de firewall XML no DataPower. Essa implementação é usada porque é uma maneira simples de fornecer a funcionalidade. O firewall StoreXML usa a mesma interface WSDL que o servidor Tivoli Runtime Security Services. O gateway StoreWSP cria o objeto da solicitação e o envia, protegido usando SSL, para o gateway StoreXMLFW.

A regra de solicitação do firewall StoreXML executa o seguinte:

1. Executa AAA usando as informações de SSL para autenticação.
2. Executa autorização usando um PDP XACML na caixa. A política usada pelo PDP é criada originalmente no IBM Tivoli Security Policy Manager, mas pode ser recriada usando um editor padrão, e o esquema é definido na especificação XACML.
3. Nenhuma transformação da solicitação é necessária neste processamento de autorização.
4. Se a solicitação XACML for válida, a regra de processamento de solicitação executará uma busca de uma resposta Permit e retornará para o cliente. Caso contrário, será lançada uma exceção que é manipulada pela regra de processamento de exceção e retorna uma resposta Negar para o cliente.

Nota: Esse Permitir/Negar/Indeterminado é apenas uma resposta de nível de exemplo. Informações de erro adicionais podem ser inclusas em um fluxo específico do cliente.

Política de Segurança XACML

Este tópico descreve como os documentos XACML são criados.

Os documentos XACML usados na amostra foram criados pelo editor de políticas do IBM Tivoli Security Policy Manager, mas é possível usar qualquer editor de

texto ou XML para criar tais documentos manualmente. Para construir ou modificar políticas XACML existentes, consulte as especificações OASIS: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

A política de segurança XACML usada na amostra está contida em `storeSWPXACML.xml` e `storePrivateDataXACML.xml`. Essas políticas são usadas para avaliar a solicitação que chega ao policy decision point (PDP). A solicitação é constituída de quatro elementos principais:

1. A seção Assuntos - Contém os detalhes do Nome Distinto do responsável pela chamada da solicitação, bem como os grupos aos quais o responsável pela chamada pertence.
2. A seção de recurso - Contém os documentos aos quais o responsável pela chamada deseja ter acesso. Dois tipos de recurso são usados na amostra; o primeiro é a operação no serviço da web e o segundo é a autorização para os dados na resposta, nesse caso, o recurso priceInfo.
3. A seção Ambiente - Contém informações sobre o ambiente da solicitação.
4. A ação - O que o usuário deseja executar com o material autorizado. No cenário de edição de dados a ação é simplesmente visualizar os dados de priceInfo.

Política de Segurança StoreWSP

A política de segurança no arquivo `storeSWPXACML.xml` mapeia grupos para Operações de Serviço da Web.

Um exemplo de política de segurança é o seguinte:

```
<PolicySet PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:denyoverrides"
PolicySetId="RPS:Store:policy:aed2df4e-4159-4df0-ada2-f148d9b56cef:roled200c213-27f9-
4d17-8305-b0d3ca8fcf54:role:09b60522-76b8-4280-9c1a-31d026441164" Version="1.0">
<Target>
<Subjects>
<Subject>
<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:x500Name-equal">
<xacml:AttributeValue DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">CN=MANAGER, CN=groups,
DC=ibm.com</xacml:AttributeValue>
<SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:group-id"
DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"
SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" />
</SubjectMatch>
</Subject>
<Subject>
<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">MANAGER</xacml:AttributeValue>
<SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
DataType="http://www.w3.org/2001/XMLSchema#string"
SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" />
</SubjectMatch>
</Subject>
</Subjects>
</Target>
<Policy PolicyId="PPS:StoreSOAP:findInventory:aed2df4e-4159-4df0-ada2-f148d9b56cef:d200c213-27f9-
4d17-8305-b0d3ca8fcf54:d200c213-27f9-4d17-8305-b0d3ca8fcf54:pps"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable"
Version="1.0">
<Target>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">{http://company.ibm.com/store}findInventory</xa
cml:AttributeValue>
<ResourceAttributeDesignator AttributeId="urn:ibm:xacml:profiles:web-services:1.0:wsdl:1.1:operation"
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ResourceMatch>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
```

```
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">{http://company.ibm.com/store}StoreSOAP</xac
ml:AttributeValue>
<ResourceAttributeDesignator AttributeId="urn:ibm:xacml:profiles:web-services:1.0:wsdl:1.1:port"
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ResourceMatch>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">{http://company.ibm.com/store}Store</xacml:Attr
ibuteValue>
<ResourceAttributeDesignator AttributeId="urn:ibm:xacml:profiles:web-services:1.0:wsdl:1.1:service"
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ResourceMatch>
</Resource>
</Resources>
</Target>
```

Nota: Na seção de assuntos, ocorre uma correspondência no nome x500 ou na função do assunto do Manager. Se você examinar o arquivo `.xml` inteiro da política verá que há mapeamentos semelhantes para Cliente e Funcionário. Você verá que a operação findInventory está autorizada para usar todos os três grupos enquanto as operações returnProduce e purchase estão limitadas a apenas determinados grupos.

O Gateway de Edição de Dados

Detalhes sobre a folha de estilo storeCallPDP.xsl.

Se você examinar a folha de estilo storeCallPDP.xsl notará o seguinte:

1. A inclusão da folha de estilo storeSendToPDP.xsl. Esta é a folha de estilo com a lógica para chamar o storeXAMLFW.
2. A chamada para o modelo call_PDP dentro do storeSendToPDP.
3. A extração da decisão da resposta da chamada; por exemplo, “Permitir”.
4. A configuração do valor de var:/context/response/displayfilter para as folhas de estilo allData.xsl ou noPriceInfo.xsl.
5. Examinando o XACML quanto à Edição de Dados, storePrivateDataXACML.xml, a estrutura será quase idêntica à estrutura usada no cenário StoreWSP. A diferença é que apenas a função Gerente tem acesso.

storeCallPDP.xsl

```
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:dp="http://www.datapower.com/extensions"
extension-element-prefixes="dp" exclude-result-prefixes="dp">
  <xsl:include href="storeSendToPDP.xsl" />
    <xsl:template match="/">
      <xsl:call-template name="call_PDP">
        <xsl:with-param name="resource" select="'StorePrivateData'" />
      </xsl:call-template>
      <xsl:variable name="decision">
        <xsl:copy-of select="dp:variable('var://context/snip/xacml/BacksideXacmlResponse')/*[local-name()='url-open']/
  *[localname()='response']/*[local-name()='Envelope']/*[local-name()='Body']/*[local-name()='Response']/
  *[local-name()='Result']/*[localname()='Decision']" />
      </xsl:variable>
      <xsl:message dp:priority="debug">
        <DECISION-FROM-RTSS>
          <xsl:value-of select="$decision" />
        </DECISION-FROM-RTSS>
      </xsl:message>
      <xsl:choose>
      <xsl:when test="$decision = 'Permit'">
        <xsl:message dp:priority="debug">****** CONFIGURANDO O FILTRO PRIVADO ********</xsl:message>
        <dp:set-variable name="'var://context/response/displayFilter'" value="'local:///allData.xsl'" />
      </xsl:when>
      <xsl:otherwise>
        I<dp:set-variable name="'var://context/response/displayFilter'" value="'local:///noPriceInfo.xsl'" />
      </xsl:otherwise>
    </xsl:choose>
  </xsl:template>
</xsl:stylesheet>
```

Artefatos do WSRR Criados no Padrão SOA Policy Gateway Basic Runtime Sample

Os artefatos do WSRR criados no padrão SOA Policy Gateway Basic Runtime Sample e como a amostra os usa.

Tabela 33. Artefatos do WSRR Criados para o Padrão SOA Policy Gateway Basic Runtime Sample

Objeto	Descrição
Organização	Warehouse de Bob.
Recurso de Negócios	Warehouse, pertencente à organização Warehouse do Bob.
Versão de Serviço	O Store 1.0 usa o Serviço da Web de Armazenamento, a Service Level Definition (SLD) de Armazenamento e o Recurso de Negócios do Warehouse.
WSDL	Store.wsdl
XSD	Company.xsd
Política	• Validate.xml • RouteForGold.xml • LogEveryTime.xml • RejectAfter5MsgIn90Seconds.xml
Anexos sobre a Política	• Anonymous Users_GenericObject_Anonymous Users_LogEveryTime.xml - Anexa a política LogEveryTime ao Acordo de Nível de Serviço (SLA) de Usuários Anônimos. • Gold SLA_GenericObject_Gold SLA_RouteForGold.xml - Anexa a política RouteForGold ao SLA Ouro. • Store_GenericObject_Store_urn :RejectAfter5MsgIn90Seconds.xml - Anexa a política RejectAfter5MsgIn90Seconds à SLD de Armazenamento. • Store_GenericObject_Store_urn:Validate.xml - Anexa a política Validar à SLD de Armazenamento.
SLD	SLD de Armazenamento - Usada pela Versão de Serviço Store 1.0.
SLA	SLA Ouro - Roteia para o terminal Ouro se o ContextId for “Gold”.
SLA Anônimo	Usuários Anônimos - Usa a notificação de política LogEveryTime e é executado se o ContextId não é “Ouro”.

Uso de Aplicativo de Amostra de Artefatos do WSRR

O StoreWSP usa uma Assinatura do WSRR para recuperar artefatos de WSDL e de política. Sempre que uma solicitação é processada por meio de StoreWSP, as ações a seguir são tomadas:

1. A versão de serviço Store 1.0 é conectada à SLD de Armazenamento, que tem duas políticas diretas anexadas, Validate e RejectAfter5MsgIn90Seconds. A ordem em que as políticas são executadas é indeterminado.
   a. Se 5 solicitações tiverem ocorrido nos últimos 90 segundos, a solicitação será rejeitada.
   b. A solicitação é validada com relação a Store.wsdl com seu Company.xsd associado.
2. O serviço Store 1.0 usa a SLD de Armazenamento, que tem dois SLAs; o SLA Ouro para usar com usuários Ouro e o SLA de Usuários Anônimos para todos os outros usuários. Se o atributo ContextId for “Ouro”, a solicitação será roteada para o Firewall XML StoreMockServiceAlternate, caso contrário, se for “Prata” ou qualquer outro valor, o SLA de Usuários Anônimos assumirá o controle e a Política LogEveryTime será executada. Isso coloca uma notificação no `default.log` do domínio de Amostra. Essa notificação poderá ser vista apenas se o modo de depuração estiver ativado no domínio. A mensagem é, então, roteada para o firewall de XML StoreMockService.

Artefatos do DataPower Criados no SOA Policy Gateway Basic Runtime Sample

Os artefatos do DataPower criados no padrão SOA Policy Gateway Basic Runtime Sample.

Tabela 34. Artefatos do DataPower Criados para o Padrão SOA Policy Gateway Basic Runtime Sample

Tipo	Nome	Objetivo
WebService Proxy	StoreWSP	O serviço principal.
Firewalls de XML	StoreAddLTPA StoreMockService StoreAlternateMockService StoreXACMLFW	Autentica e inclui o Token LTPA. O provedor de serviços para clientes não Ouro O provedor de serviços para clientes não Ouro Verifica o acesso a PriceInfo.
WSRR Server	WSRRSVR	A conexão com o WSRR.
Assinatura do WSRR	StoreSub	Fornece informações de procura para o namespace, o objeto, e assim por diante.
Política AAA	StoreAddLTPA	Identificação de autenticação básica para LDAP. Consulta a autenticação. Inclui o token LTPA na solicitação.
Política AAA	StoreWSDLAAA	Identificação e autenticação LTPA. Mapeamento de grupos para a autorização. Autorização XACML.
Política AAA	StoreXACMLFWAZ	Autorização XACML para PriceInfo.
Perfil Proxy SSL	WSRRPP	Perfil proxy SSL para o WSRR Server.
Perfil de Criptografia	WSRRCP	Perfil de criptografia para o WSRR Server.
Credenciais de Validação	WSRRVC	As credenciais de validação contêm o certificado de Criptografia WSRRCERT. Todas as outras configurações são padrão.
Certificado de Criptografia	WSRRCERT	O WSRRCERT usa o certificado de assinante. Esse certificado foi extraído do NodeDefaultKeyStore, do certificado padrão para um único servidor ou do certificado padrão CMSKeyStore no caso de um ambiente ND em que um IBM HTTP Server estava presente.

As Regras de Processamento do Web Service Proxy StoreWSP

O gateway central da amostra é StoreWSP. A Política para o gateway contém uma regra de solicitação e de resposta.

Regra de solicitação

A ação de política primária do StoreWSP_default_request-rule é chamada AAA. Na ação AAA, o Token LTPA é validado, os grupos de usuários são recuperados e uma autorização é executada para ver se o usuário está no grupo LDAP de Gerente, Funcionário ou Cliente. Isso é executado quando a etapa AAA AZ chama o Policy Decision Point (PDP) StoreWSDLPDP no dispositivo DataPower. Esse PDP usa a política XACML storeWSPXACML.xml.

Regra de resposta

Na regra de resposta, StoreWSP_default_response-rule, a transformação chama o serviço de firewall XML StoreXACMLFW.

Essa transformação determina se o usuário está autorizado a acessar as informações sobre preço com base em se o usuário é um membro do grupo Gerente. Se ele for, a variável *var:///context/response/displayFilter* será configurada para `local:///allData.xsl`. Se ele não for um membro do grupo LDAP Gerente, a variável *var:///context/response/displayFilter* será configurada para `local:///noPriceInfo.xsl`.

A transformação executa, então, as ações da folha de estilo na resposta.

Regras de Processamento StoreXAMLFW

A folha de estilo customizada storeSendToPDP.xsl faz uma chamada para o FW XML StoreXACMLFW local. Há duas regras de processamento usadas nesse firewall. A solicitação StoreXACMLFW_request contém uma única ação de política AAA que usa a transformação allData.xsl. Esta ação AAA, StoreXACMLFWAZ, chama por sua vez a ação StorePDP do PDP XACML. Usando a política XACML storePrivateDataXACML.xml, uma determinação é feita sobre se o usuário está autorizado para as informações de preço.

As Folhas de Estilo XSL de Amostra

O aplicativo de amostra contém as folhas de estilo a seguir que terminam em `.xsl` e estão localizadas no diretório local do domínio instalado.

Tabela 35. Folhas de Estilo no Aplicativo de Amostra

Folha de Estilo	Objetivo
`allData.xsl`	Uma folha de estilo de Identidade que copia todos os dados da origem para o destino. Ela é usada para a função Edição de Dados e para a chamada ao Gateway XML XACML.
`apil-xacml-binding-new.xsl`	Usa as informações de mapeamento de credencial para criar uma solicitação SOAP que pode ser processada pelo Policy Decision Point (PDP) do dispositivo DataPower. Essa folha de estilo é uma modificação da folha de estilo tspm-xacml-binding-sample.xsl que é fornecida no diretório de armazenamento do dispositivo DataPower. A funcionalidade principal fornecida por este script adaptado é incluir uma variável acessível externamente que torna as informações de assunto da solicitação XACML disponíveis para a folha de estilo de edição de dados.
`noPriceInfo.xsl`	Esta folha de estilo configure o elemento de preço para um valor de 0.0.
`rgxacml.xsl`	Esta folha de estilo é uma customização da folha de estilo tspm-retrieve-groups.xsl no diretório de armazenamento do dispositivo DataPower. O propósito primário desta folha de estilo é fornecer o DN LDAP, nome do host, senha, porta e assim por diante, para que o usuário recebido possa ser consultado e suas informações sobre o grupo recuperadas.
`soavars.xsl`	Esta folha de estilo é apenas um exemplo que define as informações de LDAP em variáveis usadas pela folha de estilo rgxacml.xsl. No exemplo, a senha é decriptografada, que não é uma prática de produção.
`storeCallPDP.xsl`	Esta folha de estilo tem o código para chamar o Gateway XACML, manipula a decisão de permissão/negação e configura a variável de filtro para executar allData.xsl ou noPriceInfo.xsl.
`storeSendToPDP.xsl`	Esta folha de estilo constrói uma solicitação SOAP que é enviada ao Gateway XACML. Ela inclui as informações sobre o assunto obtidas na folha de estilo apil-xacml-binding-new.xsl, as informações sobre o recurso, a ação e o ambiente.

Objetos do DataPower que Usam as Folhas de Estilo XSL

Os objetos do DataPower usam algumas das folhas de estilo XSL que são fornecidas com o aplicativo de amostra.

Tabela 36. Objetos do DataPower que Usam as Folhas de Estilo XSL

Folha de Estilo	Objetivo
`allData.xsl`	Usada internamente na folha de estilo storeCallPDP.xsl. A folha de estilo é usada como a transformação customizada na política AAA StoreXACMLFWAZ.
`apil-xacml-binding-new.xsl`	Usada como a folha de estilo customizada na etapa AZ da política AAA StoreWSDLAAA.
`noPriceInfo.xsl`	Usada internamente na folha de estilo storeCallPDP.xsl.
`soavars.xsl`	Usada internamente na folha de estilo rgxacml.xsl.
`storeCallPDP.xsl`	Chamada como uma transformação na regra Store_default-response.
`storeSendToPDP.xsl`	Usada internamente na folha de estilo storeCallPDP.xsl.

Capítulo 6. Trabalhando com a Instância Implementada

Quando a imagem do IBM SOA Policy Gateway Pattern foi implementada, é possível registrar suas próprias definições de serviço e anexar suas próprias políticas às definições. Também é possível visualizar e gerenciar seus sistemas implementados. Para visualizar a lista de instâncias implementadas, clique em **Instâncias** > **Sistema Virtual**.

Visualizando os Detalhes da Instância

Os detalhes de uma instância implementada podem ser vistos selecionando uma instância na lista de instâncias na janela Instâncias de Sistema Virtual. Os detalhes da instância de sistema virtual são exibidos à direita. Os detalhes incluem uma lista de máquinas virtuais aprovisionadas na infraestrutura de nuvem para essa implementação, o endereço IP, o status da máquina virtual e o status da função. Função é uma unidade de função executada pelo middleware de aplicativo virtual em uma máquina virtual. Também é possível visualizar as informações de status de funcionamento da função de máquina virtual. Por exemplo, uma marca de seleção vermelha aparece na seta de status verde quando a CPU é crítica na máquina virtual.

Para ver o status de fornecimento e de implementação da instância, consulte o valor **Status Atual** na visualização de detalhes.

Para ver o status das máquinas virtuais e dos scripts durante o fornecimento, expanda a seção **Histórico** na visualização de detalhes.

Para ver os detalhes das máquinas virtuais e dos logs de script, expanda a seção **Máquinas Virtuais** na visualização de detalhes. O host e o endereço IP do sistema é o valor **Interface de Rede 0** na seção **Hardware e Rede**. Expanda uma máquina virtual em execução para ver os logs de script na seção **Pacotes de Scripts** e os links para acessar a máquina virtual usando a seção **Consoles**.

Administrando Instâncias Implementadas

Depois de implementar um padrão de sistema virtual, é possível visualizar e administrar a instância de sistema virtual que foi criada para ver seu ambiente do IBM SOA Policy Gateway Pattern.

Antes de Iniciar

Para visualizar uma instância de sistema virtual, você deve primeiro ter implementado um padrão de sistema virtual.

Sobre Esta Tarefa

A implementação de um padrão cria uma instância de sistema virtual ou um ambiente de tempo de execução do IBM SOA Policy Gateway Pattern recém-aprovisionado. Quando a implementação for concluída, a instância de sistema virtual estará em execução.

Procedimento

Para administrar as instâncias de sistema virtual do IBM SOA Policy Gateway Pattern, conclua as etapas a seguir:

1. Clique em **Instâncias** > **Sistemas Virtuais** para acessar a janela Instâncias de Sistema Virtual.
2. Na lista de instâncias na janela Instâncias de Sistema Virtual, selecione a instância que foi implementada.
3. Se a instância estiver em execução, será possível efetuar login nos componentes do sistema virtual a partir dos links do console na visualização de sistema virtual. Os componentes disponíveis dependem do padrão criado. Por exemplo, você poderia:
   - Ativar e efetuar login no console administrativo para o gerenciador de implementação e, em seguida, ver os clusters criados.
   - Ativar o centro de processos e, em seguida, fazer download do designer de processo para criar aplicativos de processo.
   - Configurar o IBM Integration Designer e conectar-se ao centro de processos para criação de processo.

Conectando ao WSRR - Business Space

Use a interface com o usuário do Business Space para administrar políticas.

Sobre Esta Tarefa

Acesse a interface com o usuário do Business Space usando o endereço do host do sistema WSRR.

Procedimento

1. Clique em **Instâncias** > **Sistemas Virtuais** para acessar a janela Instâncias de Sistema Virtual.
2. Na lista de instâncias na janela Instâncias de Sistema Virtual, selecione a instância que foi implementada. Os detalhes da instância são exibidos.
3. Acesse o sistema WSRR usando a interface com o usuário do Business Space:
   - Na seção **Consoles**, clique em **WSRR Business Space** para conectar-se ao Business Space em execução no sistema WSRR.
   - Como alternativa, em um navegador da web externo:
     a. Localize o nome do host e os números de porta para o WSRR. Expanda a seção **Máquinas Virtuais** e selecione a máquina virtual para que o Servidor Independente WSRR veja os detalhes da máquina virtual. Na seção **Hardware e Rede**, o nome do host é o valor **Interface de Rede 0**.
     b. Insira a URL do Business Space:
        – Para o servidor Independente WSRR com a segurança ativada: `https://<hostname>:9443/BusinessSpace`
        – Para o cluster: `http://<hostname>/BusinessSpace`

        em que *<hostname>* e *port* são o nome do host e o valor de porta do WSRR Server.

Resultados

O Business Space é exibido e pode ser usado para incluir, editar ou remover políticas.

O que Fazer Depois

Se estiver usando o Business Space no sistema WSRR pela primeira vez, consulte "Configurando o Business Space para o Primeiro Uso" e siga as etapas para criar o espaço Operações.

Informações relacionadas:

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0

Conectando ao WSRR - Console de Registro de Serviço

Use o Console de Registro de Serviço para classificar versões de serviço.

Sobre Esta Tarefa

Acesse a interface com o usuário do Console de Registro de Serviço usando o endereço do host do sistema WSRR.

Procedimento

1. Clique em **Instâncias** > **Sistemas Virtuais** para acessar a janela Instâncias de Sistema Virtual.
2. Na lista de instâncias na janela Instâncias de Sistema Virtual, selecione a instância que foi implementada. Os detalhes da instância são exibidos.
3. Acesse o sistema WSRR:
   - Na seção **Consoles**, clique em **WSRR_Web_UI** para conectar-se ao Business Space em execução no sistema WSRR.
   - Como alternativa, em um navegador da web externo:
     a. Localize o nome do host e os números de porta para o WSRR. Expanda a seção **Máquinas Virtuais** e selecione a máquina virtual para que o Servidor Independente WSRR veja os detalhes da máquina virtual. Na seção **Hardware e Rede**, o nome do host é o valor **Interface de Rede 0**.
     b. Insira a URL do Console de Registro de Serviço: http://*hostname*/ServiceRegistry

        em que *hostname* é o nome do host do servidor WSRR.

Informações relacionadas:

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0

Configurando o Business Space para o Primeiro Uso

Antes que a interface com o usuário do Business Space possa ser usada para criar políticas, o espaço Controle SOA deve ser criado.

Antes de Iniciar

Para obter informações sobre como acessar o Business Space, consulte "Conectando ao WSRR - Business Space" na página 92.

Sobre Esta Tarefa

Para usar os widgets do Business Space, você deve criar um Espaço. Os espaços são definidos para funções específicas. A criação de política é mais adequada para trabalhar no espaço Controle SOA. Se um espaço Controle SOA não tiver sido

criado ainda, você deverá criá-lo. Para criar um espaço com base no modelo Registro de Serviço para Controle SOA, conclua estas etapas:

Procedimento

1. Clique em **Gerenciar Espaços** na parte superior da página. O diálogo Gerenciador de Espaço é exibido.
2. Clique em **Criar Espaço**. O diálogo Criar Espaço é exibido.
3. Insira um nome no campo Nome do Espaço; por exemplo, `Controle SOA`. Opcionalmente, insira uma descrição.
4. Selecione **Registro de Serviço para Controle SOA** na lista **Criar um novo espaço usando um modelo** e, em seguida, clique em **Salvar**.
5. O novo espaço é exibido na lista **Gerenciador de Espaço**. Clique no novo espaço para abri-lo.

Resultados

O espaço de Controle SOA é criado. Para abrir o espaço Controle SOA:

1. Clique em **Acessar Espaços** na parte superior da página. O diálogo Acessar Espaços é exibido.
2. Clique no espaço para usuários do Controle SOA. O nome específico dependerá do que foi especificado quando o espaço foi criado.

O que Fazer Depois

É possível incluir ações adicionais no widget de Ações de Registro de Serviço:

1. No Business Space, clique em **Editar Página**.
2. No widget de Ações de Registro de Serviço, clique em **Editar Configurações**.
3. Selecione as ações a seguir para serem exibidas:
   - Criar uma Definição de Nível de Serviço
   - Criar uma Versão de Serviço
   - Criar um Acordo de Nível de Serviço
   - Criar um Recurso de Negócios
4. No widget de Ações de Registro de Serviço, clique em **Salvar e Fechar**.
5. Clique em **Concluir Edição**.

Configuração de Padrão de Pós-implementação

Depois de implementar os padrões, a segurança e outras configurações devem ser definidas.

Mudanças nas Configurações de LDAP do Aplicativo de Amostra

Se você estiver usando o SOA Policy Gateway Basic Runtime Sample e precisar alterar as configurações de segurança para seu servidor LDAP; por exemplo, a senha ou o nome do usuário, você precisa alterar esses valores em dois locais.

Os locais para fazer as mudanças são:

- A Seção de Autenticação de Política AAA para a política AAA StoreAddLTPA - Para localizar essa política, use o intervalo de procura da interface com o usuário da web Administração do DataPower e procure `AAA`. Selecione a política AAA correta e altere o valor na guia Autenticação.

- O arquivo `soavars.xsl` - Use a Seção de Gerenciamento de Arquivo na Interface com o Usuário Administrativo da Web do DataPower. Abra o domínio criado pelo padrão SOA Policy Gateway Basic Runtime Sample no dispositivo DataPower e pesquise o diretório local para o arquivo `soavars.xsl`. Altere as variáveis LDAPHost, LDAPPort, LDAPCN, LDAPPassword conforme necessário.

  Nota: Você poderá precisar reiniciar o domínio para que essas mudanças entrem em vigor.

Certificar Valores de DN para Certificados do DataPower

Quando SSL é usado com as IBM SOA Policy Gateway Patterns fornecidas, a verificação do host de DN é mais estrita do que a segurança padrão do WebSphere Application Server.

A verificação do host de DN não está ativada no WebSphere Application Server por padrão. No entanto, nos pacotes de script usados pelas IBM SOA Policy Gateway Patterns, a verificação do host de DN está ativada e não pode ser desativada. Um certificado muito específico que funciona entre o WebSphere Application Server padrão e o DataPower pode não funcionar para o pacote de scripts “SOA Policy Gateway 2.0.0.0 - Segurança” ou o pacote de scripts “SOA Policy Gateway 2.0.0.0 - Amostra” usados com a IBM SOA Policy Gateway Pattern; por exemplo, um DN `myserver.yourcompany.com` pode ser aceito pelos padrões do WebSphere Application Server, mas não pelos pacotes de scripts. Para incluir ou remover os certificados do DataPower usados com a implementação, consulte “Removendo ou Incluindo Certificados do DataPower no Armazenamento Confiável do WSRR” na página 96.

Alterando as Chaves LTPA

Este procedimento descreve como alterar a chave LTPA. A chave LTPA é compartilhada entre todas as células em Basic. Ele não é usado no padrão SOA Policy Gateway Basic Runtime Sample. A Chave LTPA é exportada do Governance Master e importada para os ambientes de tempo de execução, como temporariedade, produção ou Não Configurado.

Procedimento

1. Exporte a nova Chave LTPA do Governance Master WSRR Dmgr.
2. Importe a Chave LTPA para as instâncias do Runtime WSRR, que são Dmgr ou Independente.
3. Se a instância Runtime for um ambiente Advanced ND, conclua o seguinte em ordem:
   a. Sincronize todos os nós.
   b. Pare o Cluster do WSRR.
   c. Pare os agentes do nó.
   d. Pare o Dmgr.
4. Se o ambiente for Advanced, ele deverá ser reiniciado em ordem reversa:
   a. Inicie o Dmgr.
   b. Inicie os agentes do nó.
   c. Inicie o Cluster do WSRR.
5. Se o WSRR for um Standalone Server, ele deverá ser interrompido e reiniciado para que a mudança da Chave LTPA entre em vigor.

Removendo ou Incluindo Certificados do DataPower no Armazenamento Confiável do WSRR

Esta tarefa descreve como incluir ou remover certificados do DataPower. Um benefício de executar esta tarefa é que ela simplifica a configuração futura do recurso de atualização síncrona entre o WSRR e o DataPower para atualizações de política.

Sobre Esta Tarefa

Os certificados do DataPower como parte dos parâmetros usados para a ferramenta curl. As Chamadas do DataPower são transferidas por upload para o Armazenamento Confiável Padrão da Célula ou do Nó. Isso simplifica a configuração de usos futuros no recurso de atualização síncrona entre o WSRR e o DataPower para atualizações de política. Se esse recurso não for necessário, este procedimento descreve como remover os Certificados do DataPower. Este procedimento também descreve como incluir novos Certificados do DataPower se os certificados precisarem ser alterados.

Procedimento

1. Efetue login no Dmgr ou WSRR Independente em `http://hostname:9060/admin`. Insira o usuário e a senha.
2. Navegue para **Segurança, certificados SSL e gerenciamento de chaves**.
3. Clique em **Armazenamentos de Chaves e Certificados**.
4. Clique em **NodeDefaultTrustStore** se você escolheu um padrão básico ou **CellDefaultTruststore** se escolheu um padrão avançado.
5. Clique em **Certificados de Assinante**.
6. Marque as caixas de seleção de quaisquer certificados que você deseja remover.
7. Clique em **Excluir**.
8. Clique em **Salvar**.
9. Opcional: se for necessário incluir novos Certificados do DataPower, clique em **Incluir** para incluir o novo certificado.

Configurando o Policy Enforcement Point

O dispositivo DataPower é o Policy Enforcement Point (PEP) do IBM SOA Policy Gateway Pattern. Quando o Domínio de Aplicativo está implementado, é possível criar o conteúdo desse domínio.

Procedimento

Crie um Web Service Proxy (WSP):

1. No Painel de Controle do DataPower, clique em **Web Service Proxy**.
2. Clique em **Incluir** e insira um nome para o Proxy.
3. Abra a guia **Assinatura do WSRR**. Na lista de Servidores WSRR, clique em **WSRRSVR**.
4. Forneça as outras informações necessárias, como o Manipulador Frontal, o namespace, o nome do objeto e assim por diante, para criar a configuração do Web Service Proxy.

Crie políticas para o WSP:

5. Abra a guia **Política** para o Editor do WSP.
6. Clique em **Regras de Processamento** no nível apropriado. É possível criar uma nova regra ou editar a regra padrão fornecida. A ação de política

principal a ser inclusa é a **Ação AAA**. Isso manipula a Identificação, Autenticação e Autorização, que são a chave para o padrão.

As principais coisas que você deve especificar para a ação AAA incluem a Entrada e Saída, bem como a Política AAA. É possível criar a política durante o processo de criação da Ação de Política AAA, ou você pode tê-la criado antes disso usando o Editor AAA.

- Identificação é a etapa na qual o usuário é Identificado. Em nossa amostra, havia duas formas de identificação usadas. No firewall XML StoreAddLTPA, a identificação foi executada com autenticação básica. No firewall StoreWSP, a identificação foi fornecida pelo token LTPA.
- Autenticação é a etapa na qual o usuário comprova ser um usuário conhecido no sistema. Há muitas opções para escolha. Na amostra, mostramos dois exemplos; o primeiro em que o usuário foi procurado usando LDAP e o segundo que aceitou um Token LTPA válido.
- Autorização é a etapa na qual o usuário está autorizado para o recurso, neste caso, as operações de serviço da web. Os elementos principais a seguir precisam ser especificados para usar a autorização do PDP na caixa do XACML:
  - O Método: **Usar Autorização XACML**.
  - A Versão do XACMLn; por exemplo, 2.0.
  - Tipo de PDP; por exemplo, PDP baseado em negação.
  - Usar PDP na caixa: **Ativado**
  - O nome do PDP, que possui o XACML especificado.
  - Configure o PDP. Para obter informações adicionais, consulte "Alterando o PDP XACML no DataPower" na página 81.
  - A folha de estilo XSL customizada para ligar o AAA e o XACML: use `apil-xacml-bindingnew.xsl` como um ponto de início.

Para configurar o gateway para usar a Edição de Dados:

7. Modifique o arquivo `.xml` do XACML para corresponder às políticas de segurança específicas que você deseja impingir para a edição de dados.
8. Crie um Firewall XML com uma ação AAA que segue a amostra de edição de dados.
9. Modifique o PDP usado pela ação AAA acima para apontar para a folha de estilo que você está usando para impingir a edição de dados.
10. Copie e modifique a folha de estilo `storeCallPDP.xsl`, que cria a carga útil SOAP para o serviço XACML. Em particular, certifique-se de que a Ação e o Recurso correspondam a seus requisitos para o documento sobre políticas XACML criado.
11. Certifique-se de que sua folha de estilo modificada chame a porta correta para seu novo Firewall XML do XACML.

O que Fazer Depois

Além de criar um Domínio e definir uma Configuração do WSRR Server nos padrões SOA Policy Gateway Advanced Runtime e SOA Policy Gateway Basic Runtime, é possível estender o domínio executando um script de CLI customizado. O script de CLI deve estar na raiz da estrutura `DomainZipFile.zip`; por exemplo, `/cli.cli`. A CLI pode executar quaisquer comandos de CLI padrão, mas todos os artefatos aos quais a CLI se refere devem existir ou ser acessíveis pelo Domínio do DataPower criado pelo padrão. Ao implementar uma instância dos padrões SOA Policy Gateway Advanced Runtime ou SOA Policy Gateway Basic Runtime, o

nome do arquivo de CLI será solicitado nos parâmetros do pacote de Segurança.

Trabalhando com o Padrão SOA Policy Gateway Basic Runtime

O padrão SOA Policy Gateway Basic Runtime é constituído de três partes de funcionalidade principais; os arquivos necessários para a segurança entre os scripts de padrão DataPower e WSRR são recuperados, um domínio é configurado no DataPower e, finalmente, a promoção é configurada.

Quando concluído, as ações a seguir terão ocorrido:

1. O novo domínio existirá no dispositivo DataPower especificado.
2. Uma Definição de WSRR Server existirá no domínio.
3. O script de CLI customizado terá sido executado com relação ao domínio do DataPower.
4. Um WSRR Server está configurado.
5. Todos os certificados de assinante do DataPower fornecidos pelo cliente terão sido transferidos por upload para o NodeDefaultTruststore da célula WSRR.
6. A promoção entre a célula WSRR do padrão SOA Policy Gateway Basic Runtime e a célula SOA Policy Gateway Governance Master terá sido configurada.
7. Os Certificado de Assinante terão sido trocados. O Certificado de Assinante do Dmgr de Controle é colocado no NodeDefaultTrustStore da célula Básica e o Certificado de Assinante do Dmgr de Célula Avançada é colocado no CellDefaultTrustStore da Célula de Controle.
8. As Chaves LTPA terão sido trocadas. A Chave LTPA da célula Controle é importada para a célula Básica.
9. Cada host no cluster de WSRR de Governance Master está incluído nas regiões confiáveis da célula Básica. Cada host do cluster de WSRR da célula Básica está incluído nas regiões confiáveis do Governance Master.
10. O arquivo de propriedades de promoção estará configurado se a célula foi designada como um ambiente de temporariedade ou de produção nas entradas especificadas.

Embora será necessário realizar outras etapas para concluir um ambiente de produção totalmente seguro, a configuração executada neste momento permitirá que você faça o seguinte:

1. Crie serviços e políticas e controle-os por meio do ciclo de vida da Política SOA no WSRR (quando ambientes de produção e temporários foram fornecidos) usando o GEP padrão.
2. Crie Proxies de Serviço da Web que podem usar a definição do WSRR Server pré-criada para construir assinaturas.

Trabalhando com o Padrão SOA Policy Gateway Advanced Runtime

O padrão SOA Policy Gateway Advanced Runtime é constituído de três partes de funcionalidade principais; os arquivos necessários para a segurança entre os scripts de padrão DataPower e WSRR são recuperados, um domínio é configurado no DataPower e, finalmente, a promoção é configurada.

Quando concluído, as ações a seguir terão ocorrido:

1. Um novo domínio existirá no dispositivo DataPower especificado.
2. Uma Definição de WSRR Server existirá no domínio.

3. O script de CLI customizado terá sido executado com relação ao domínio do DataPower.
4. Um ambiente em cluster do WSRR com 'n' nós terá sido criado e configurado.
5. Quaisquer certificados de assinante do DataPower fornecidos pelo cliente terão sido transferidos por upload para o CellDefaultTruststore da célula WSRR.
6. A promoção entre a célula WSRR do padrão SOA Policy Gateway Advanced Runtime e a célula SOA Policy Gateway Governance Master terá sido configurada:
   a. Os Certificado de Assinante terão sido trocados. O Certificado de Assinante do Dmgr de Controle é colocado no CellDefaultTrustStore da célula Avançada e o Certificado de Assinante do Dmgr de célula Avançada é colocado no CellDefaultTrustStore da célula de Controle.
   b. As Chaves LTPA terão sido trocadas. A Chave LTPA da célula de Controle é importada para a célula Avançada.
   c. Cada host no cluster de WSRR de Governance Master está incluso nas regiões confiáveis da célula Avançada. Cada host do cluster de WSRR da célula Avançada está incluído nas regiões confiáveis do Governance Master.
   d. O arquivo de propriedades de promoção estará configurado se a célula foi designada como um ambiente de temporariedade ou de produção nas entradas especificadas.

A configuração atual permite que você faça o seguinte:

1. Crie serviços e políticas e controle-os por meio do ciclo de vida da política SOA no WSRR (quando ambientes de produção e temporários foram fornecidos) usando o GEP padrão.
2. Crie Proxies de Serviço da Web que podem usar a definição do WSRR Server pré-criada para construir assinaturas.

Em seguida, você deve executar etapas adicionais para concluir um ambiente de produção totalmente seguro. Para obter informações adicionais, consulte "Segurança para os Padrões IBM SOA Policy Gateway Pattern" na página 53.

Objetos do DataPower Criados nos Padrões Basic Runtime e Advanced Runtime

Uma visão geral dos objetos do DataPower criados nos padrões SOA Policy Gateway Basic Runtime e SOA Policy Gateway Advanced Runtime e suas funções.

Tabela 37. Objetos de Padrão do DataPower

Objeto	Descrição
Domínio	Um Domínio que pode ser usado para o aplicativo de usuários.
WSRR Server	Nomeado WSRRSVR. A URL do SOAP, o Usuário e a Senha são configurados, bem como um Perfil Proxy SSL com as Credenciais de Validação.
Perfil Proxy SSL	Nomeado WSRRPP, é um perfil de encaminhamento (cliente). Ele usa o Perfil de Criptografia WSRRCP. Todos os outros padrões são usados.
Perfil de Criptografia	O WSRRCP contém um objeto de credenciais de validação WSRRVC, que contém o Certificado de Assinante que foi transferido por upload como parte dos scritps de padrão.
Credenciais de Validação	As Credenciais de Validação do WSRR contêm o Certificado de Criptografia WSRRCERT. Todas as outras configurações são padrão.
Certificado de Criptografia	O WSRRCERT utiliza o certificado de assinante. Esse certificado foi extraído do NodeDefaultKeyStore, Cert. padrão para um único servidor, ou do certificado Padrão CMSKeyStore no caso de um ambiente ND em que um IBM HTTP Server estava presente.

Exemplo de uso da Definição do WSRR Server em um Web Service Proxy:

1. No Painel de Controle do DataPower, clique em **Web Service Proxy**.
2. Clique em **Incluir** e forneça um **Nome** para o Proxy.
3. Em seguida, selecione a guia **Assinatura do WSRR**
4. Selecione WSRR Server no menu. O objeto WSRRSVR está disponível.
5. Forneça as outras informações necessárias, como o Manipulador Frontal, o namespace, o nome do objeto e assim por diante, para criar a configuração do Web Service Proxy.

Criação e Controle de Serviço

Use a interface com o usuário do WSRR Business Space para criar e controlar serviços de negócios e seus objetos associados.

O espaço Controle SOA deve ser criado no espaço de negócios para que as políticas possam ser criadas. Se o espaço Controle SOA não tiver sido criado, consulte "Configurando o Business Space para o Primeiro Uso" na página 93 e siga as etapas para criar o espaço.

Para obter informações adicionais sobre como criar um serviço controlado, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Tutorial: Controlando um Novo Serviço.

Para obter informações adicionais sobre como controlar um serviço existente, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Tutorial: Controlando um Serviço Existente.

Tarefas relacionadas:

"Conectando ao WSRR - Business Space" na página 92
Use a interface com o usuário do Business Space para administrar políticas.

Políticas

Detalhes da implementação para usar o WSRR como o Ponto de Criação de Política e o WebSphere DataPower como o Ponto de Cumprimento de Política ao criar políticas de mediação.

Políticas no WSRR

O WSRR pode ser usado para criar todas as políticas SOA, incluindo políticas SLA (Acordo de Nível de Serviço), políticas de mediação, políticas de monitoramento, políticas customizadas e outros domínios de política que deverão ser suportados no futuro. Usando a interface com o usuário do Business Space, é possível criar, atualizar ou excluir um documento sobre políticas no WSRR. O documento sobre políticas pode conter uma expressão de política que especifica várias políticas de um domínio de política específico. Como alternativa, é possível criar um documento sobre políticas que monta políticas existentes de outros documentos. As políticas individuais são referidas usando identificadores de política, que você especifica ao incluir políticas em seu documento. Uma expressão de política representa a declaração de uma política e é equivalente a um elemento `<wsp:Policy>` em um documento WS-Policy.

Para criar uma política de mediação no Business Space, consulte "Criando Novas Políticas" na página 106.

Asserções de Política de Mediação

Os Acordos de Nível de Serviço (SLAs) devem se originar de um requisito dos negócios de que a qualidade de serviço fornecida por um serviço deve atender a um padrão especificado. Como um serviço está sendo projetado, requisitos funcionais são criados para orientar a lógica do que o serviço executa. Requisitos não funcionais devem ser especificados em paralelo como parte da análise e design desse serviço para designar a qualidade de serviço que espera-se que o serviço forneça. Por exemplo, a empresa pode ter um serviço que fornece informações em resposta a uma consulta de Internet do cliente. O destino é para retornar a resposta em 3 segundos. Como parte da engenharia da transação de ponta a ponta, é determinado que esse serviço deve retornar suas informações em 2 segundos, a fim de atender aos requisitos não funcionais dos negócios.

Podemos escrever uma política que implemente verificações de tempo de execução sobre o desempenho do serviço e tome uma ação quando o SLA não está sendo atendido de forma a garantir que o serviço atenda a seu SLA. Por exemplo, podemos ter um terminal primário de serviço que é normalmente capaz (95% do tempo) de fornecer resposta de serviço em 2 segundos. O Arquiteto de SOA criou um terminal secundário em outro servidor que é normalmente usado como uma espera a quente para indisponibilidades do terminal primário, mas também está autorizado a ser usado para o tráfego de estouro quando o terminal primário não é capaz de acompanhar o carregamento da transação. Podemos escrever uma política que verifica o tempo de resposta de serviço e roteia novamente o tráfego quando necessário para atender ao SLA.

Outro exemplo em que os SLAs são mantidos por meio da política de tempo de execução é uma situação na qual um serviço está respondendo às transações que possuem uma variedade de consumidores, cada um com um nível diferente de prioridade. Um exemplo simples pode ter clientes “ouro” e “bronze”, em que apenas garantimos uma qualidade de serviço específica para nossos clientes “ouro”. Neste exemplo, podemos verificar se o consumidor é “ouro” e rotear novamente para nosso terminal secundário, deixando nosso cliente “bronze” lidar com um tempo de resposta mais lento. A empresa tomou essa decisão uma vez que os clientes “bronze” fornecem renda incremental insuficiente para justificar a despesa do tempo de resposta de engenharia para atender ao SLA de clientes “ouro”.

Em um terceiro exemplo, podemos ter uma situação em que um serviço fará o melhor possível, mas quando determinar que está com subcarregamento, ele enfileirará ou mesmo rejeitará mensagens de serviços do consumidor de baixa prioridade. Um exemplo disso é quando uma rotina de lote inunda o sistema com as solicitações do consumidor em um momento inesperado. Para proteger a qualidade de serviço, podemos criar uma política de tempo de execução que fique em vigor apenas durante as horas de expediente e que rejeitará todas as solicitações de lote durante esse período.

Mais genericamente, a política de mediação permite a validação e transformação na mensagem recebida do cliente (consumidor) antes da apresentação ao servidor (provedor).

As políticas suportam este tipo de validação e transformação de mensagem. As políticas podem ser especificadas para um serviço de provedor apenas, para um par de consumidor/provedor específico ou para consumidores Anônimos de um serviço de provedor. As políticas para clientes Anônimos fornecem uma maneira de definir uma política padrão que se aplica apenas aos consumidores para os

quais nenhuma outra política se aplica. O uso desse recurso permite que políticas sejam especificadas para consumidores suspeitos que não se identificam. Tais serviços de consumidor podem, então, ter suas transações rejeitadas. Isso pode ser útil para evitar ataques de negação de serviço de hackers consumidores que tentam inundar o sistema com transações destinadas a derrubar um serviço de provedor.

Condições da Política de Mediação

Podem ser feitas asserções de mediação que permitem que a política de tempo de execução controle o SLA do serviço, a transformação de mensagens de consumidor para provedor ou valide o esquema de mensagem da mensagem do consumidor.

As condições da política SLA, um tipo especial de política de mediação, permitem efetivamente uma construção if-then-else clássica com uma condição e, em seguida, um conjunto de ações a serem executadas dependendo de como a condição é avaliada. A especificação de uma condição é opcional. Se nenhuma condição for especificada, ela será equivalente à condição lógica que avalia como Verdadeiro e quaisquer ações especificadas serão impingidas adequadamente.

A condição, se especificada, deve consistir em uma expressão booleana ou uma especificação de planejamento, ou podem ser ambas.

Planejamento

O planejamento, se especificado, identifica quando a política está em vigor. A data e hora especificadas são avaliadas pelo Policy Enforcement Point local e o fuso horário usado é aquele do Policy Enforcement Point. Se nenhum planejamento for especificado, a política será iniciada assim que for transferida por download do Policy Authoring Point para o Policy Enforcement Point, e confinuará indefinidamente.

O planejamento define uma data de início opcional e uma data de parada opcional, um intervalo de tempo diário opcional e uma lista opcional de dias da semana. Por exemplo, um planejamento pode ser definido como efetivo a partir de 1º de outubro de 2012 a 30 de outubro de 2012, das 8h às 17h, nas quarta-feiras e domingos.

Os parâmetros para o planejamento que podem ser especificados são os seguintes:

- **StartDate** - Este atributo opcional especifica a data em que o planejamento torna-se efetivo no formato xs:date. StartDate é inclusivo e, se este atributo não estiver presente, o planejamento se tornará efetivo imediatamente hoje.

  Nota: Clique no hiperlink xs:date para entender esse padrão de mercado.
- **StopDate** - Este atributo opcional especifica a data em que o planejamento para de ser efetivo no formato xs:date. StopDate é exclusivo e a data especificada deve ser após a data de início. Quando a data de parada é anterior ou igual à data de início, o planejamento nunca é efetivo. Se este atributo não estiver presente, o planejamento será efetivo indefinidamente.
- **Daily** - Este elemento opcional especifica o intervalo de tempo diário durante o qual o planejamento é efetivo. Se esse elemento não estiver presente, o planejamento será efetivo o dia inteiro.
  - **StartTime** – Se Daily estiver especificado, este atributo é obrigatório. Ele especifica o horário em que o planejamento inicia diariamente no formato xs:time. (Nota: clique no hiperlink xs:time para entender esse padrão de mercado).

  - **StopTime** - Se Daily estiver especificado, este atributo é obrigatório. Ele especifica o horário em que o planejamento para diariamente no formato xs:time. StopTime é exclusivo e, se o horário especificado for anterior ou igual ao horário de início diário, o planejamento parará no horário de parada especificado no dia seguinte.
- **Weekdays** - Este elemento opcional especifica os dias da semana inclusos no planejamento. Se este elemento não estiver presente, todos os dias da semana serão inclusos no planejamento. Este elemento afeta apenas o início do intervalo de tempo diário, uma vez que os planejamentos são permitidos executar após a meia-noite. Por exemplo, se um planejamento estiver configurado para iniciar às 23h e for executado por 2 horas às quarta-feiras, o planejamento terminará efetivamente na quinta-feita à 1h.
  - **Days** - Se Weekdays estiver especificado, este atributo é obrigatório. Ele lista os dias da semana inclusos no planejamento como uma lista de nomes separados com o sinal de mais ('+'), por exemplo, “Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday”.

Expressão de Condição da Política de Mediação

A expressão de condição, se especificada, é um elemento sem repetição que especifica uma expressão booleana.

A expressão inclui três parâmetros necessários, que consistem em Attribute, Operator e Value, além de Interval e Limit opcionais. Se o aplicativo do Operador no Attribute e no Value, além de Interval e Limit quando apropriado, avaliar como Verdadeiro, a expressão avaliará como Verdadeiro. O elemento Limit é usado apenas com os operadores HighLow e TokenBucket. Se não for especificado, o valor de Limit será 0. Se Interval não for especificado, o padrão será 60 segundos.

Os parâmetros para Expression que podem ser especificados são os seguintes:

- **Attribute** - A tabela a seguir resume os atributos definidos e seus tipos.

Tabela 38. Atributos Definidos

Atributo	Descrição e Tipo
ErrorCount	O número de falhas observado durante este intervalo de monitoramento.
MessageCount	O número de mensagens reais interceptadas durante o intervalo de monitoramento.
InternalLatency	A latência interna (tempo de processamento) em segundos.
BackendLatency	A latência de dispositivo-para-servidor em segundos.
TotalLatency	A soma de latência interna e de backend em segundos.

- **Operator** - A tabela a seguir resume os operadores disponíveis e seus significados:

Tabela 39. Operadores

Operador	Significado
GreaterThan	Um algoritmo numérico simples que avalia como Verdadeiro quando o Attribute é maior que o Value definido.
LessThan	Um algoritmo numérico simples que avalia como Verdadeiro quando o Attribute é menor que o Value definido.

Tabela 39. Operadores (continuação)

Operador	Significado
TokenBucket	Um algoritmo baseado em taxa que permite bursting. O algoritmo consiste em um depósito com uma capacidade máxima de tokens de Limit. O depósito é reenchido a uma taxa constante de tokens de Value por Interval, enquanto um token é removido para cada unidade de Attribute. Esse algoritmo avalia como Verdadeiro quando não há tokens no depósito e avaliado como Falso caso contrário. Aqui está um exemplo para ajudar a explicar o algoritmo: Suponha Limit=100, Value=5, Interval=1 second e o Attribute=MessageCount. 1. O depósito inicia integral com uma capacidade máxima de 100 tokens 2. Quando uma mensagem chega, o algoritmo verifica se o depósito retém quaisquer tokens: a. Se sim, o algoritmo avalia como Falso e um token é removido do depósito b. Se não, o algoritmo avalia como Verdadeiro. 3. Nesse período, a cada segundo, o algoritmo inclui 5 tokens novamente no depósito conforme o espaço permite.
HighLow	Um algoritmo que avalia como Verdadeiro quando o Attribute atinge o limite alto especificado como o Valor e, em seguida, continua a avaliar como Verdadeiro até que o Attribute atinja o limite baixo especificado como o Limit.

- **Value** – Este é um elemento de número inteiro positivo. “0” é válido.
- **Interval** - Este elemento opcional define o intervalo de tempo, usado como uma janela deslizante, para medir o wsme:Attribute ao avaliar a expressão, no formato xs:duration. Se não especificado, o intervalo usado será de 60 segundos. Se especificado, um valor razoável deverá ser especificado, levando em consideração os recursos configurados do Policy Enforcement Point. Ou seja, quanto maior esse valor, mais memória será necessária ao Policy Enforcement Point para manter o controle do atributo.

  Nota: Clique no hiperlink xs:duration para entender esse padrão de mercado.
- **Limit** - Este elemento de número inteiro define o argumento Limit adicional requerido quando wsme:Operator é TokenBucket ou HighLow. A unidade depende do wsme:Operator especificado.

  Quando wsme:Operator é HighLow, isto define o limite baixo enquanto wsme:Value define o limite alto. O limite especificado deve ser inferior àquele de wsme:Value. Quando não especificado, o Limite padrão é 0.

  Quando wsme:Operator é TokenBucket, isto define o tamanho máximo do burst, ou o número máximo de tokens no depósito, enquanto Value especifica a taxa em que o depósito é reenchido, em número de tokens por Intervalo. Quando não especificado, o limite padrão é 0 e TokenBucket é, então, equivalente a uma operação GreaterThan.

Ações da Política de Mediação

O elemento Ação de Mediação especifica as ações a serem tomadas. Embora a sintaxe permita muitas combinações, nem todas elas fazem sentido, e quando ações conflitantes forem especificadas, como pedir que uma mensagem seja tanto enfileirada quanto rejeitada, o comportamento será rejeitado pelo Policy Authoring Point. As ações da política de mediação permissões são:

- **QueueMessage** – Esta ação especifica que as transações serão enfileiradas quando a condição lógica for atendida. O processamento de mensagens não recomeçará até que a condição lógica deixe de ser atendida. A metodologia da fila e quaisquer tempos limites associados são conforme definidos pelo Policy

Enforcement Point, neste caso, o WebSphere DataPower. Quando várias ações são especificadas, dentro de um único elemento de Ação, QueueMessage deve ser a primeira ação.

- **RejectMessage** – Esta ação especifica que as transações serão rejeitadas quando a condição lógica for atendida. As transações continuarão a ser rejeitadas até que a condição lógica deixe de ser atendida. Quando as transações forem rejeitadas, uma falha de SOAP será retornada para o serviço de cliente (consumidor). Quando várias ações são especificadas, dentro de um único elemento de Ação, RejectMessage deve ser a primeira ação. QueueMessage e RejectMessage são mutuamente exclusivos.
- **Notify** - Este elemento opcional especifica que uma notificação será produzida quando a condição lógica for atendida. Para o WebSphere DataPower, uma mensagem será gravada no log do sistema do DataPower.
- **RouteMessage** - Este elemento opcional especifica que as mensagens serão roteadas para um destino de terminal especificado quando a condição lógica for atendida. As transações continuarão a ser roteadas para o terminal especificado até que a condição lógica deixe de ser atendida.
  - **EndPoint** – Este parâmetro será necessário quando uma ação de RouteMessage for especificada. O valor de terminal suportado pode ser um endereço IP, nome do host ou host virtual; como grupo de balanceadores de carga.
- **ValidateMessage** - Este elemento opcional especifica que as mensagens deverão ser validadas com relação às gramáticas especificadas. As mensagens deverão ser rejeitadas quando a validação falhar. O XSD ou WSDL deve ser especificado como um subparâmetro se ValidateMessage estiver especificado. SCOPE é opcional e, se não especificado, SOAPBody será usado para a validação.
  - **XSD** - Especifica que as mensagens serão validadas com relação ao esquema XML identificado pelo URI que ele contém.
  - **WSDL** - Especifica que as mensagens serão validadas com relação à descrição de serviços da web (WSDL) identificada pelo URI que ela contém.
  - **SCOPE** – Especifica qual parte da mensagem será validada. A tabela a seguir lista os valores possíveis e o que eles significam:

Tabela 40. Elementos de ValidateMessage

Valor	Descrição
SOAPBody	O conteúdo do elemento de Corpo SOAP, sem o processamento especial para falhas de SOAP. (Padrão)
SOAPBodyOrDetails	O conteúdo do elemento de detalhe para falhas de SOAP e, caso contrário, o conteúdo do Corpo.
SOAPEnvelope	A mensagem SOAP inteira, incluindo o envelope.
SOAPIgnoreFaults	Sem validação se a mensagem for uma falha de SOAP, caso contrário, o conteúdo do Corpo SOAP.

- **ExecuteXSL** - Especifica que uma conversão XSL será executada com a Folha de Estilo e os Parâmetros especificados. As transações serão rejeitadas quando a execução falhar. As informações de Stylesheet devem ser especificadas, enquanto as de Parameters são opcionais e devem ser especificadas conforme necessário pela folha de estilo particular especificada.
  - **Stylesheet** - Especifica que a operação de conversão usará a folha de estilo especificada pelo URI contido. A folha de estilo DEVE ser um arquivo XSLT.
  - **Parameter** - Este elemento de repetição opcional especifica um parâmetro de folha de estilo a ser usado para a operação ExecuteXSL.

- **Name** – Este atributo é necessário para cada Parameter correspondente e especifica o nome do parâmetro.
- **Value** - Este atributo é necessário para cada parâmetro Name correspondente e especifica o valor do parâmetro.

Criando Novas Políticas

Ao criar políticas de mediação na interface com o usuário do Business Space, especifique as condições e ações para a política.

Antes de Iniciar

Para obter informações sobre como acessar o Business Space, consulte “Conectando ao WSRR - Business Space” na página 92.

O espaço Controle SOA deve ser criado para que as políticas possam ser criadas. Se o espaço Controle SOA não tiver sido criado, consulte “Configurando o Business Space para o Primeiro Uso” na página 93 e siga as etapas para criar o espaço.

Sobre Esta Tarefa

Crie novas políticas usando o espaço Controle SOA.

Procedimento

1. Abra o espaço Controle SOA:
   a. Clique em **Acessar Espaços**. O diálogo Acessar Espaços é exibido.
   b. Clique no espaço para usuários do Controle SOA. O nome específico dependerá do que foi especificado quando o espaço foi criado.
2. Na guia Visão Geral, clique em **Criar uma Política de Mediação**.
3. Insira um nome significativo e uma descrição opcional.
4. Inclua as condições e ações conforme necessário. Para obter informações adicionais sobre as condições e ações, consulte “Políticas” na página 100 e Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Criando uma Política de Mediação.
5. Clique em **Concluir**.

Resultados

A política é criada e armazenada no WSRR. Para visualizar o documento sobre políticas para a política recém-criada, selecione o documento sobre políticas no Widget de Navegador do Registro de Serviço na parte inferior esquerda da tela. Como alternativa, procure o nome especificado, incluindo `.xml` no final. O documento sobre políticas é exibido no widget Detalhe de Registro de Serviço à direita.

Conceitos relacionados:

"Políticas" na página 100
Detalhes da implementação para usar o WSRR como o Ponto de Criação de Política e o WebSphere DataPower como o Ponto de Cumprimento de Política ao criar políticas de mediação.

Informações relacionadas:

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Criando uma Política de Mediação

Gerenciando Políticas

As políticas podem ser editadas ou removidas usando a interface com o usuário do Business Space.

Antes de Iniciar

Configure o espaço Controle SOA. Para obter informações adicionais, consulte "Configurando o Business Space para o Primeiro Uso" na página 93.

Procedimento

1. Para abrir o documento sobre políticas para a política, selecione o documento sobre políticas no Widget de Navegador do Registro de Serviço na parte inferior esquerda da tela. Como alternativa, procure o nome especificado, incluindo `.xml` no final. O documento sobre políticas é exibido no widget Detalhe de Registro de Serviço à direita.
2. Para alterar os detalhes da política:
   a. Clique no ícone Editar nesse widget para editar o documento sobre políticas. Uma janela é exibida com as opções para editar os detalhes da política.
   b. Se a política tiver quaisquer condições ou ações, elas serão exibidas. Crie e modifique as condições e ações, conforme necessário.
   c. Clique em **Concluir** para salvar e fechar o editor de políticas. O widget Detalhe de Registro de Serviço é atualizado para mostrar as mudanças feitas.
3. Para excluir a política:
   a. Faça a transição da política para um estado de controle que permita a edição ou exclusão do documento sobre políticas. Para obter informações adicionais sobre como executar a transição de uma política por meio do Ciclo de Vida de SOA Policy, consulte "Gerenciando o Ciclo de Vida da Política" na página 108.
   b. Clique em **Ação** > **Excluir**. A opção Excluir é listada no menu.
   c. Selecione **Excluir** para excluir a política.
   d. Clique em **Sim** para confirmar a exclusão.

Informações relacionadas:

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Policies in the governance enablement profile

Gerenciando o Ciclo de Vida da Política

É possível executar a transição de políticas entre os estados de controle usando a interface com o usuário do Business Space.

Sobre Esta Tarefa

Para obter informações adicionais sobre controle, consulte "O Ciclo de Vida de SOA Policy" na página 4.

Procedimento

Para executar a transição de uma política para um estado de ciclo de vida diferente, conclua as etapas a seguir. Repita estas etapas quantas vezes forem necessárias para atingir o estado do ciclo de vida desejado:

1. No Business Space, abra o documento sobre políticas para a política selecionando o documento sobre políticas no Widget de Navegador do Registro de Serviço na parte inferior esquerda da tela. Como alternativa, procure o nome especificado, incluindo `.xml` no final. O documento sobre políticas é exibido no widget Detalhe de Registro de Serviço à direita. A propriedade **Estado de Controle** exibe o estado de controle atual para o perfil.
2. Clique em **Ação**. Uma lista de transições de ciclo de vida possíveis é exibida juntamente com outras operações possíveis.
3. Selecione a transição de ciclo de vida necessária para mover a política para o estado requerido. A propriedade **Estado de Controle** da política é atualizada para mostrar o novo estado do ciclo de vida.

Conceitos relacionados:

"O Ciclo de Vida de SOA Policy" na página 4
As políticas de mediação são controladas usando o ciclo da Política SOA. Isso faz com que a política seja inicialmente identificada, até ser implementada na produção e, finalmente, descontinuada quando não for mais necessária.

Informações relacionadas:

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - SOA policy lifecycle

Políticas Anexadas a um Serviço

As políticas podem ser conectadas a um serviço usando o WSRR.

Para obter informações adicionais, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Tarefas de Anexo sobre a Política.

Capítulo 7. Resolução de Problemas

Obtenha assistência ao diagnosticar problemas que você possa ter antes, durante e após a implementação do padrão.

Use os links para localizar os tópicos relevantes para um problema com os padrões.

Resolução de Problemas com a Implementação

É possível solucionar problemas comuns ao implementar os padrões no IBM SOA Policy Gateway Pattern.

Falha ao Conectar-se ao DataPower Durante a Implementação

Tente as soluções a seguir:

- Verifique com o Administrador do DataPower se o usuário e a senha são válidos:
  - No DataPower, valide se o usuário existe acessando **Painel de Controle** > **Gerenciar Contas do Usuário**.
  - Verifique se a conta existe.
  - Verifique se o usuário é privilegiado para usar a Interface de Gerenciamento XML; por exemplo, o administrador do sistema.
  - O Administrador do DataPower pode precisar verificar se a conta do usuário está ativada nas configurações de agente do usuário; por exemplo, as Configurações de Autenticação Básica.
- Verifique se o Nome do Host do DataPower está correto
- Verifique se a Interface de Gerenciamento XML do DataPower está ativada.
- Revise as etapas da Falha de Conexão SSL abaixo para validar se os Certificados estão instalados corretamente no `DomainZipFile.zip` e no dispositivo DataPower.

Resolução de Problemas de Falha de Autenticação de Cliente de Autenticação Mútua

Tente as soluções a seguir:

- Verifique se os certificados corretos estavam no `DomainZipFile.zip`.
- Verifique se o Perfil de Criptografia na Porta da Interface de Gerenciamento XML possui Credenciais de Validação com todos os certificados na Cadeia.
- Verifique se as senhas para a Chave Pública de Cliente e o Certificado Público de Cliente estão corretas.

Resolução de Problemas de Falha de Autenticação de Servidor

Tente as soluções a seguir:

- Verifique se todos os certificados na cadeia estão presentes no diretório *`yourDataPowerHostName`* do arquivo `DominZipFile.zip` que você está usando.
- Verifique se o Perfil Proxy SSL possui um perfil de criptografia reversa que contém as Credenciais de Identificação com a Cadeia de Certificados.

Resolvendo problemas de um erro para o domínio já existente

Tente a solução a seguir:

- No Painel de Controle do DataPower, abra os Domínios do Aplicativo. Verifique se o Domínio já existe.

Resolvendo problemas de erro de sobreposição de porta para o aplicativo de amostra

Se um dos serviços de amostra estiver indisponível, verifique se as portas em seu domínio estão em conflito com outros domínios.

Tente as soluções a seguir:

- Efetue sign in no DataPower e alterne para o domínio de amostra. Em seguida, abra o Painel de Controle e clique no ícone Firewall XML. Verifique se os Firewalls XML estão todos no estado Ativo.
- Procure o Manipulador Frontal HTTP. Verifique se o único manipulador Frontal HTTP está no estado Ativo.

Resolvendo problemas da falha para conectar a um SCP

Tente as soluções a seguir:

- Verifique se o nome do host do SCP está correto.
- Verifique se o usuário do SCP está correto.
- Verifique se a senha do SCP está correta.
- Teste manualmente o SCP a partir de um Nó no ambiente IBM Workload Deployer ou IBM PureApplication System com as informações fornecidas.

Resolução de Problemas da Falha ao Recuperar o Arquivo `DomainZipFile.zip` do SCP ou Depurar Artefatos Ausentes

Tente as soluções a seguir:

- Verifique se o `DomainZipFile.zip` existe no URI.
- Verifique se o arquivo mencionado na falha do log existe no local correto no arquivo `DomainZipFile.zip`. Em particular, assegure-se de que os certificados necessários estejam localizados no diretório correto.

Resolução de Problemas de Falha de Promoção

Há muitos problemas que podem surgir em uma promoção, incluindo falha ao conectar-se com o Governance Master durante a implementação.

Tente as soluções a seguir:

- Verifique os parâmetros:
  - Verifique o usuário do WSRRCELL do Governance Master.
  - Verifique a senha do usuário da Célula WSRR do Governance Master.
  - Verifique o nome do host da Célula do Governance Master WSRR.
  - Verifique o nome de CÉLULA da Célula do Governance Master WSRR.
- Verifique a troca do certificado de assinante:
  - Acesse o Armazenamento Confiável Padrão da Célula da célula do Governance Master e certifique-se de que exista uma entrada de certificado

para o Dmgr ou que o servidor Independente do ambiente de tempo de execução, SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime, exista.
  - Acesse cada Ambiente de Tempo de Execução, SOA Policy Gateway Basic Runtime ou SOA Policy Gateway Advanced Runtime, e verifique o armazenamento CellDefaultTrust (para o caso do ambiente do ND) ou o NodeDefaultTrustStore (para servidores Independentes do WSRR) para certificar-se de que exista um certificado para o Dmgr do Governance Master.
  - Exporte as chaves LTPA de ambas as células usando a mesma senha e verifique se elas são as mesmas (por exemplo, os bytes).
- Certifique-se de que o arquivo de propriedades de promoção contenha seções de servidor com o host e a porta apropriados e as informações do usuário e senha. Essas informações podem ser localizadas no console ServiceRegistry para o Governance Master:
  - Acesse o GovernanceMasterDMgrHost ou ServiceRegistry e alterne para a perspectiva Configurações. Na seção Ações, localize **Promoção** e abra o arquivo de propriedades de promoção. Para cada ambiente, deve haver elementos XML para cada servidor no nó ou cluster do WSRR de temporariedade. Se existir um cluster ou nó de produção, deverá haver entradas server:port para cada um e, além disso, deverá haver informações do usuário e senha.
- Verifique se a Versão de Serviço e o Terminal SOAP possuem ambos a Classificação para temporariedade e Produção.
  - No Console de Registro de Serviço, selecione a perspectiva Controle SOA. Abra a Versão de Serviço e selecione a guia Classificações. A Temporariedade e a Produção devem estar ativadas.

Resolução de Problemas de Falhas de CLI Customizada

Tente as soluções a seguir:

- Verifique as mensagens de erro no defaultLog no Domínio do DataPower.
- Ative a depuração de CLI e marque esses logs antes de quaisquer execuções adicionais da CLI.

Resolvendo problemas de falhas de SSL devido a certificados ausentes do DataPower

Se o nome do host correto para seu diretório de Certificados do DataPower não foi fornecido no arquivo `DomainZipFile.zip`, os pacotes de scripts falharão ao conectar ao WSRR Server se a Autenticação Mútua ou de Servidor está ativada no host do DataPower.

Resolvendo problemas de conexão do WSRR/DataPower

Se você vir que o status do WSDL em um Proxy de Serviço da Web está no estado Inativo ou Sincronizando que nunca é alterado para OK, verifique o seguinte:

1. Verifique se o Certificado de Criptografia é válido para o WSRR Server (WSRRSVR).
2. Verifique se o DataPower tem o DNS correto configurado para reconhecer o Nome do Host do WSRR Server ou Dmgr.
3. Se o DNS está incorreto, uma solução alternativa temporária é alterar a URL na definição do WSRR Server para apontar diretamente para o IP, substituindo o IP para o Nome do Host na URL.

4. Acesse a Assinatura do WSRR e execute uma sincronização manual:
   a. Verifique no `default.log` se há erros relacionados à conectividade do WSRR Server.
5. Verifique se os certificados necessários correspondem àqueles nas Credenciais de identificação para o Perfil de Criptografia do Perfil Proxy SSL da Interface XMLManagement dos Dispositivos DataPower.

Resolução de Problemas na Instância Implementada

É possível solucionar problemas comuns na instância implementada.

Falha ao Conectar-se ao LDAP

Para diagnosticar Falhas de LDAP na amostra, tente as soluções a seguir:

- Na Resolução de Problemas do Painel de Controle do DataPower, assegure-se de que o rastreio esteja no modo de depuração.
- Acesse StoreAddLTPA, abra os detalhes da Análise e ative a análise.
- Execute um teste de cliente.
- Visualize os logs na análise. Procure mensagens de falha de Ligação LDAP.
- Verifique o Nome do Host LDAP.
- Verifique o DN LDAP; por exemplo, cn=root,dc=ibm.com.
- Verifique a senha LDAP; por exemplo, passw0rd.
- Verifique se a porta LDAP é 389 e não segura.
- Verifique se as senhas de entrada para ConsumerX, ConsumerA, ConsumerB são todas passw0rd. Certifique-se de que a importação do arquivo LDIF tenha transcrito as senhas corretas.

Conexões com Falha com o Servidor LDAP ou com a Porta StoreWSP do DataPower

Você pode ter um problema com as configurações de Domínio se os logs do DataPower mostrarem um erro de conexão com o LDAP ou o gateway StoreWSP e se você estiver usando o nome do alias do host; por exemplo, `xyz`, em vez do nome completo do host `xyz.company.com` para um dos parâmetros a seguir no pacote de scripts:

- O Nome do Host do DataPower
- O Nome do Host do LDAP

Tente a solução a seguir:

1. No Console de Administração do DataPower, alterne para o domínio padrão.
2. Procure `Configurar Definições de DNS`.
3. Clique na guia Procurar Domínios.
4. Certifique-se de que seu domínio, por exemplo, `company.com`, esteja na lista. Se não estiver, clique em `Incluir` e inclua-o na lista.

Coletando Informações sobre Diagnóstico

É possível usar os logs para ajudar a localizar e resolver problemas. Os logs são armazenados no dispositivo e podem ser visualizados a partir da interface com o usuário ou podem ser transferidos por download para seu sistema de arquivos local.

Procedimento

Para coletar informações de diagnóstico, conclua as etapas a seguir:

1. Visualize as instâncias virtuais:
   a. Clique em **Instâncias** > **Sistema Virtual**.
   b. Selecione a instância na lista de instâncias na janela Instâncias de Sistema Virtual.
2. Para a máquina virtual do WSRR:
   a. Na seção **Máquinas Virtuais**, expanda a máquina virtual do WSRR e verifique se existem erros na seção **Pacotes de Scripts**. Se qualquer um dos pacotes de scripts tiver erros, clique nos links de log para **remote_std_out.log** e **remote_std_err.log** ao lado dos nomes de pacote de scripts.
   b. Efetue login na instância do WSRR e verifique os erros do servidor.
   c. Consulte os guias de resolução de problemas do WSRR: http://pic.dhe.ibm.com/infocenter/sr/v8r0/topic/com.ibm.sr.doc/cwsr_troubleshootingandsupport.html
3. Para o DataPower:
   a. Recupere o arquivo **default.log** para o domínio criado pelo padrão.
   b. Recupere o arquivo **default.log** para o domínio padrão.

Capítulo 8. Manutenção e Suporte

É possível executar funções de manutenção, como aplicar correções temporárias.

Incluindo uma Correção Emergencial no Catálogo

As correções temporárias e os fix packs são aplicados a instâncias de sistema virtual como correções emergenciais. É possível incluir correções emergenciais em seu catálogo para serem aplicadas às suas imagens virtuais.

Antes de Iniciar

Você deve ser designado à permissão *Criar novo conteúdo de catálogo* ou à função *Administrador* do Dispositivo IBM Workload Deployer com permissões integrais para executar estas etapas.

Sobre Esta Tarefa

As correções são fornecidas pela IBM ou um provedor de imagem e devem ser transferidas por download. As correções novas são transferidas por download a partir do IBM Fix Central. As correções são então transferidas por upload para o catálogo e podem ser aplicadas a todas as instâncias de sistema virtual aplicáveis.

Procedimento

Conclua as etapas a seguir para incluir uma correção emergencial em seu catálogo.

1. Localize e faça download da correção emergencial (ou correções) a partir do Fix Central.
2. Opcional: É possível incluir diversas correções temporárias de uma vez. Para incluir várias correções de uma vez, faça download dos arquivos compactados a partir do Fix Central e empacote-os em um único arquivo compactado.
3. No menu, selecione **Catálogo** > **Correções de Emergência**.
4. Clique no ícone de inclusão no painel esquerdo.
5. Insira um nome para a correção a ser inclusa. Opcionalmente, também é possível incluir uma descrição da correção que você está incluindo. A correção é mostrada no painel esquerdo da janela Correções Emergenciais e as informações da correção são mostradas no painel direito.
6. Navegue até o local no qual você armazenou a correção e clique em **Fazer Upload**. Por segurança, apenas os arquivos .zip, tgz e pak podem ser transferidos por upload. O Red Hat RPM também é suportado.
7. Preencha as informações sobre a correção. É possível conceder acesso aos usuários e fornecer uma classificação de severidade. Use o campo **Aplicável a** para especificar a imagem virtual ou imagens virtuais às quais essa correção se aplica.

Resultados

A correção emergencial está no catálogo e disponível para ser aplicada às imagens de sistema virtual.

Aplicando uma Correção Emergencial

As correções temporárias e os fix packs são aplicados a instâncias de sistema virtual como correções emergenciais. É possível aplicar correções emergenciais às suas imagens de sistema virtual.

Antes de Iniciar

Você deve ser designado ao acesso Todos para a instância de sistema virtual ou ser designado à função de administração de Dispositivo com permissões integrais para concluir estas etapas. A instância de sistema virtual deve ser iniciada para que o serviço seja planejado ou aplicado. A correção emergencial deve ser inclusa no catálogo para que possa ser aplicada a um sistema virtual.

Sobre Esta Tarefa

Ao incluir uma nova correção emergencial, você define as imagens virtuais às quais a correção é aplicável. A lista de correções disponíveis quando você planeja uma solicitação de serviço é construída usando todas as correções aplicáveis à imagem virtual usada para criar a instância de sistema virtual. Se uma correção já tiver sido aplicada ao sistema virtual, será possível vê-la na listagem **Histórico** e ela não será inclusa na lista de correções disponíveis.

Procedimento

Conclua as etapas a seguir para aplicar uma correção temporária.

1. Selecione uma instância de sistema virtual à qual aplicará a correção na janela Instâncias de Sistema Virtual.
2. Clique no ícone “Aplicar Serviço”.
3. Opcional: Planeje uma solicitação de serviço. Por padrão, a correção é aplicada imediatamente. Para planejá-la para ser aplicada posteriormente, clique em **Planejar Serviço** e forneça as informações necessárias.
4. Clique em **Selecionar nível de serviço ou correções**.
5. Clique em **Aplicar Correções Emergenciais** para ver e selecionar a correção a ser aplicada. A correção emergencial é aplicada a todas as máquinas virtuais na instância de sistema virtual. O status da instância de sistema virtual mostra que o serviço foi aplicado no sistema virtual.
6. Verifique os erros. Verifique os arquivos a seguir para assegurar que nenhum erro tenha ocorrido durante o processo de aplicação das correções emergenciais:
   - Remote_std_out.log
   - Remote_std_err.log

   É possível acessar os arquivos de log a partir da janela Instâncias de Sistema Virtual.

Capítulo 9. Appendices

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. 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. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não lhe garante direito algum 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

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

IBM World Trade Asia Corporation
Licensing 2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a Web sites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses Web sites. Os materiais contidos nesses Web sites não fazem parte dos materiais desse produto IBM e a utilização desses Web sites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Licenciados deste programa que desejam obter 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

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio e representam apenas metas e objetivos.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos podem incluir nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e endereços utilizados por uma empresa real é mera coincidência.

LICENÇA DE COPYRIGHT:

Estas informações contêm programas de aplicativos de amostra na linguagem fonte, ilustrando as técnicas de programação em diversas plataformas operacionais. O Cliente pode copiar, modificar e distribuir estes programas de amostra sem a necessidade de pagar à IBM, com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para a qual os programas de amostra são criados. Esses exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou implicar a confiabilidade, manutenção ou função destes programas.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

Informações sobre a Interface de Programação

As informações sobre interface de programação destinam-se a facilitar a criação de software aplicativo utilizando este programa.

No entanto, estas informações também podem conter informações sobre diagnósticos, modificações e ajustes. As informações sobre diagnósticos, modificações e ajustes são fornecidas para ajudá-lo a depurar seu software aplicativo.

Importante: Não utilize estas informações sobre diagnósticos, modificações e ajustes como uma interface de programação, pois elas estão sujeitas a alterações.

Marcas Registradas

IBM, o logotipo IBM e ibm.com são marcas registradas da IBM Corporation, registradas em vários países no mundo todo. Uma lista atual de marcas registradas da IBM está disponível na Web em “Copyright and trademark information” www.ibm.com/legal/copytrade.shtml. Outros nomes de produtos e serviços podem ser marcas registradas da IBM ou de outras empresas.

Este produto inclui o software desenvolvido pelo Projeto Eclipse (http://www.eclipse.org/).

Java e todas as marcas registradas e logotipos baseados em Java são marcas ou marcas registradas da Oracle e/ou suas afiliadas.

Enviando Seus Comentários para IBM

Se você gostar ou não gostar de algo deste manual, use um dos métodos listados abaixo para enviar seus comentários para IBM.

Sinta-se a vontade para fazer comentários sobre o que você considerar erros específicos ou omissões e sobre a precisão, s organização, o assunto ou a totalidade deste manual.

Limite seus comentários às informações deste manual e ao meio em que as informações estão apresentadas.

Para fazer comentários sobre as funções dos produtos ou sistemas IBM, converse com seu representante IBM ou seu revendedor autorizado IBM.

Quando o cliente envia seus comentários à IBM, concede à IBM direitos não exclusivos para usá-los ou distribuí-los das maneira que achar conveniente, sem que isso implique em qualquer obrigação com o Cliente.

O Cliente pode enviar seus comentários à IBM por um dos seguintes métodos:

- Por correio, para este endereço:

  IBM Brasil - Centro de Traduções
  Rodovia SP 101 Km 09
  CEP 13185-900
  Hortolândia, SP

- Por fax:
  - Fora do Reino Unido, depois do seu código de acesso internacional, disque 44-1962-816151
  - No Reino Unido, disque 01962-816151
- Eletronicamente, use a de rede adequada:
  - IBM Mail Exchange: GBIBM2Q9 em IBMMAIL
  - IBMLink: HURSLEY(IDRCF)
  - Internet: idrcf@hursley.ibm.com

Qualquer que seja o método utilizado,assegure-se de incluir:

- O título da publicação e o número de ordem
- O tópico ao qual seu comentário se aplica
- Seu nome e endereço/número de telefone/número de fax/ID de rede.