IBM Spectrum Protect para AIX 8.1.12

Guia de instalação

Observação:

Antes de utilizar essas informações e o produto que elas suportam, leia as informações em “Aviso” na página 207.

Observe Edition

Esta edição se aplica à versão 8, liberação 1, modificação 12 do IBM Spectrum Protect (números do produto 5725-W98, 5725-W99, 5725-X15) e a todas as liberações e modificações subsequentes, até que seja indicado de outra forma em novas edições.

Índice

Sobre esta publicação

Esta publicação contém instruções de instalação e configuração para o servidor IBM Spectrum Protect, idiomas do servidor, licença e driver de dispositivo.

As instruções para instalação do Operations Center também estão incluídas nesta publicação.

Quem Deve Ler Este Guia

Esta publicação destina-se a administradores de sistema que instalam, configuram ou fazem upgrade do servidor do IBM Spectrum Protect ou do Operations Center.

Componentes Instaláveis

O servidor IBM Spectrum Protect e as licenças são componentes necessários.

Esses componentes estão diversos pacotes de instalação diferentes.

Tabela 1. Componentes Instaláveis do IBM Spectrum Protect

Componente do IBM Spectrum Protect	**Descrição**	**Informações adicionais**
Servidor (obrigatório)	Inclui o banco de dados, o Global Security Kit (GSKit), IBM® Java™ Runtime Environment (JRE) e ferramentas para ajudar a configurar e gerenciar o servidor.	"Instalando o IBM Spectrum Protect Usando o Assistente de Instalação" na página 76
Pacote de idioma (opcional)	Cada pacote de idiomas (um para cada idioma) contém informações específicas do idioma para o servidor.	Consulte "Instalando os Pacotes de Idioma do Servidor" na página 79.
Licenças (obrigatório)	Inclui suporte para todos os recursos licenciados. Depois de instalar esse pacote, é necessário registrar as licenças adquiridas.	Use o comando **REGISTER LICENSE**.
Dispositivos (opcional)	Estende a capacidade de gerenciamento de mídia.	Uma lista de dispositivos que são suportados por este driver está disponível a partir do IBM Support Portal.

Tabela 1. Componentes Instaláveis do IBM Spectrum Protect (continuação)		
Componente do IBM Spectrum Protect	**Descrição**	**Informações adicionais**
Agente de armazenamento (opcional)	Instala o componente que permite que os sistemas do cliente gravem dados diretamente nos dispositivos de armazenamento, ou leiam dados a partir dele, que estão conectados em uma rede de área de armazenamento (SAN). **Lembre-se:** O IBM Spectrum Protect for Storage Area Networks é um produto licenciado separadamente.	Para obter informações adicionais sobre agentes de armazenamento, consulte Tivoli Storage Manager for Storage Area Networks (V7.1.1).
Operations Center (opcional)	Instala o Operations Center, que é uma interface baseada na web para gerenciar seu ambiente de armazenamento.	Consulte Parte 2, “Instalando e Fazendo Upgrade do Operations Center”, na página 127.

Publicações

A família de produtos do IBM Spectrum Protect inclui o IBM Spectrum Protect Plus, o IBM Spectrum Protect for Virtual Environments, o IBM Spectrum Protect for Databases e vários outros produtos de gerenciamento de armazenamento da IBM.

Para visualizar a documentação do produto IBM, consulte IBM Knowledge Center.

O que Há de Novo Nessa Liberação

Esta liberação do IBM Spectrum Protect introduz novos recursos e atualizações.

Para obter uma lista de novos recursos e atualizações, consulte O que há de novo.

Se houver mudanças na documentação, elas serão indicadas por uma barra vertical (|) na margem.

Parte 1. Instalando e Atualizando o Servidor

Instale e atualize o servidor IBM Spectrum Protect.

Capítulo 1. Planejando para Instalar o Servidor

Instale o software do servidor no computador que gerencia dispositivos de armazenamento e instale o software cliente em cada estação de trabalho que transfere dados para o armazenamento gerenciado pelo servidor do IBM Spectrum Protect.

O Que Você Deveria Saber Primeiro

Antes de instalar o IBM Spectrum Protect, esteja familiarizado com os sistemas operacionais, dispositivos de armazenamento, protocolos de comunicação e configurações do sistema.

Liberações de manutenção de servidor, software cliente e publicações estão disponíveis no IBM Support Portal.

Restrição: É possível instalar e executar o servidor do IBM Spectrum Protect em um sistema que já tenha o IBM Db2 instalado nele, se o Db2 tiver sido instalado independentemente ou como parte de algum outro aplicativo, com algumas restrições.

Para obter detalhes, consulte “Compatibilidade do servidor IBM Spectrum Protect com outros produtos IBM Db2 no sistema” na página 50.

Administradores experientes do Db2 podem escolher executar consultas SQL avançadas e usar ferramentas do Db2 para monitorar o banco de dados. Entretanto, não use ferramentas do Db2 para mudar as definições de configuração do Db2 daquelas que estão pré-configuradas pelo IBM Spectrum Protect ou altere o ambiente Db2 para IBM Spectrum Protect de outras maneiras, como com outros produtos. O diretório do servidor foi construído e testado extensivamente usando a linguagem de definição de dados (DDL) e a configuração do banco de dados que o servidor implementa.

Atenção: Não altere o software Db2 que é instalado com os pacotes de instalação e fix packs do IBM Spectrum Protect. Não instale ou atualize para uma versão, liberação ou fix pack diferente do software Db2, pois isso pode danificar o banco de dados.

O que é necessário saber sobre segurança antes de instalar ou fazer upgrade do servidor

Revise as informações sobre os recursos de segurança aprimorados no servidor IBM Spectrum Protect e os requisitos para atualizar seu ambiente.

Antes de iniciar

A partir da Versão 8.1.2, foram incluídos aprimoramentos no IBM Spectrum Protect que utilizam configurações de segurança mais rígidas. Antes de instalar ou fazer upgrade do IBM Spectrum Protect, conclua as etapas a seguir:

- Em IBM Knowledge Center, no tópico *O que há de novo*, revise as informações nas seções de Segurança para conhecer as atualizações de segurança de cada versão.
- Se houver versões anteriores do servidor em seu ambiente, revise as restrições e os problemas conhecidos na nota técnica 562939. Para evitar essas restrições e aproveitar os aprimoramentos de segurança mais recentes, planeje atualizar todos os servidores e clientes de backup-archive do IBM Spectrum Protect em seu ambiente para a versão mais recente.

Aperfeiçoamentos de Segurança

Os aprimoramentos de segurança a seguir foram incluídos a partir da V8.1.2:

Protocolo de segurança que usa Segurança da Camada de Transporte (TLS)

O software IBM Spectrum Protect V8.1.2 e mais recente tem um protocolo de segurança melhorado que usa o TLS Versão 1.2 ou mais recente para autenticação entre o servidor, o agente de armazenamento e os clientes de backup e archive.

Iniciando no IBM Spectrum Protect V8.1.11, é possível ativar o protocolo TLS 1.3 para proteger as comunicações entre os servidores, os clientes e os agentes de armazenamento. Para usar o TLS 1.3, ambas as partes na sessão de comunicação devem usar o TLS 1.3. Se uma das partes usar o TLS 1.2, ambas usarão o TLS 1.2 por padrão.

Configuração e distribuição automáticas de certificados do Secure Sockets Layer (SSL)

Os servidores, agentes de armazenamento e clientes que usam o software V8.1.2 ou mais recente são configurados automaticamente para autenticação entre si usando TLS.

Usando o novo protocolo, cada servidor, agente de armazenamento e cliente tem um certificado autoassinado que é usado para autenticar e permitir conexões TLS. Os certificados autoassinados do IBM Spectrum Protect permitem a autenticação segura entre entidades, permitem a criptografia avançada para transmissão de dados e distribuem chaves públicas automaticamente para nós clientes. Os certificados são trocados automaticamente entre todos os clientes, agentes de armazenamento e servidores que usam o software V8.1.2 ou mais recente. Não é necessário configurar manualmente o TLS nem instalar manualmente os certificados para cada cliente. Os novos aprimoramentos de TLS não requerem mudanças de opções e os certificados são transferidos para os clientes automaticamente na primeira conexão, a menos que você esteja usando um único ID de administrador para acessar múltiplos sistemas.

Por padrão, os certificados autoassinados são distribuídos, mas é possível opcionalmente usar configurações, como certificados que são assinados por uma autoridade de certificação. Para obter mais informações sobre como usar certificados, veja *Comunicação SSL e TLS* no IBM Knowledge Center.

Combinação de protocolos TCP/IP e TLS para comunicação segura e impacto mínimo no excluir

Em versões anteriores do software IBM Spectrum Protect, você tinha que escolher TLS ou TCP/IP para criptografar toda a comunicação. O novo protocolo de segurança usa uma combinação de TCP/IP e TLS para proteger a comunicação entre servidores, clientes e agentes de armazenamento. Por padrão, o TLS é usado somente para criptografar autenticação e metadados, enquanto o TCP/IP é usado para transmissão de dados. Como a criptografia TLS é usada principalmente somente para autenticação, o desempenho para operações de backup e restauração não é afetado.

Opcionalmente, é possível usar o TLS para criptografar a transmissão de dados usando a opção do cliente **SSL** para comunicação cliente-para-servidor e o parâmetro **SSL** no comando **UPDATE SERVER** para comunicação servidor-para-servidor.

A compatibilidade com versões anteriores facilita o planejamento de upgrades em lotes

As versões submetidas a upgrade de servidores e clientes do IBM Spectrum Protect poderão continuar se conectando a versões mais antigas quando o parâmetro **SESSIONSECURITY** estiver configurado como TRANSITIONAL.

Não é necessário atualizar clientes de backup e archive para a V8.1.2 ou mais recente antes de fazer upgrade de servidores. Depois que você fizer upgrade de um servidor para a V8.1.2 ou mais recente, os nós e os administradores que estiverem usando versões anteriores do software continuarão se comunicando com o servidor usando o valor TRANSITIONAL até que a entidade atenda aos requisitos para o valor STRICT. Da mesma forma, é possível fazer upgrade de clientes de backup e archive para a V8.1.2 ou mais recente antes de fazer upgrade dos seus servidores IBM Spectrum Protect, mas não é necessário fazer upgrade dos servidores primeiro. A comunicação entre servidores e clientes que estão usando versões diferentes não é interrompida. No entanto, você não terá os benefícios dos aprimoramentos de segurança até que tanto os clientes quanto os servidores sejam submetidos a upgrade.

Cumprir a segurança estrita com o parâmetro SESSIONSECURITY

Para usar o novo protocolo de segurança, as entidades de servidor, nó do cliente ou administrador devem estar usando o software IBM Spectrum Protect que suporta o parâmetro **SESSIONSECURITY**. A segurança de sessão é o nível de segurança usado para a comunicação entre os nós clientes,

clientes administradores e servidores do IBM Spectrum Protect. É possível especificar os valores a seguir para esse parâmetro:

STRICT
Cumpre o nível mais alto de segurança para comunicação entre servidores, nós e administradores do IBM Spectrum Protect, que é atualmente o TLS 1.2.

TRANSITIONAL
Especifica que o protocolo de comunicação existente (por exemplo, TCP/IP) é usado até que você atualize seu software IBM Spectrum Protect para a V8.1.2 ou mais recente. Isto é o padrão. Quando **SESSIONSECURITY=TRANSITIONAL**, configurações de segurança mais estritas são aplicadas automaticamente quando versões mais altas do protocolo TLS são usadas e quando o software é atualizado para a V8.1.2 ou mais recente. Depois que um nó, um administrador ou um servidor atender aos requisitos do valor STRICT, a segurança de sessão será atualizada automaticamente para o valor STRICT e a entidade não poderá mais ser autenticada usando uma versão anterior do cliente ou protocolos anteriores do TLS.

Se **SESSIONSECURITY=TRANSITIONAL** e o servidor, o nó ou o administrador nunca tiverem atendido aos requisitos do valor STRICT, o servidor, o nó ou o administrador continuarão sendo autenticados usando o valor TRANSITIONAL. No entanto, depois que o servidor, o nó ou o administrador atenderem aos requisitos do valor STRICT, o valor do parâmetro **SESSIONSECURITY** será atualizado automaticamente de TRANSITIONAL para STRICT. Em seguida, o servidor, o nó ou o administrador não poderão mais ser autenticados usando uma versão do cliente ou um protocolo SSL/TLS que não atenda aos requisitos de STRICT.

Restrição: Após um administrador ser autenticado com sucesso com um servidor usando o software IBM Spectrum Protect V8.1.2 ou mais recente ou o software Tivoli Storage Manager V7.1.8 ou mais recente, o administrador não poderá mais se autenticar com o mesmo servidor usando versões de cliente ou servidor anteriores à V8.1.2 ou V7.1.8. Essa restrição também se aplica ao servidor de destino ao usar funções como roteamento de comando, exportação de servidor para servidor que é autenticada com o servidor de destino IBM Spectrum Protect como um administrador de outro servidor, conexões do administrador usando o Operations Center e conexões do cliente da linha de comando administrativo.

Para sessões administrativas e do cliente, as sessões de roteamento do comando administrativo poderão falhar, a menos que o ID do administrador já tenha adquirido certificados para todos os servidores aos quais o ID do administrador se conectará. Administradores autenticados usando o comando **dsmadmc**, o comando **dsmc** ou o programa dsm não poderão ser autenticados usando uma versão anterior depois de serem autenticados usando a V8.1.2 ou mais recente. Para resolver problemas de autenticação para administradores, consulte as seguintes dicas:

- Assegure-se de fazer upgrade de todos os softwares IBM Spectrum Protect que a conta do administrador usa para efetuar logon para a V8.1.2 ou mais recente. Se uma conta de administrador efetuar logon em vários sistemas, assegure-se de que o certificado do servidor esteja instalado em cada sistema.
- Se necessário, crie uma conta do administrador separada para usar somente com clientes e servidores que estão usando o software V8.1.1 ou anterior.

Antes de fazer upgrade

Antes de fazer upgrade de um servidor, revise as diretrizes na lista de verificação a seguir.

Tabela 2. Planejando a lista de verificação

Diretriz	**Descrição**
Faça backup dos seguintes arquivos do servidor: • Bancos de dados de chaves (cert.kdb e dsmkeydb.kdb) • Arquivos stash (cert.sth e dsmkeydb.sth)	A partir do IBM Spectrum Protect Versão 8.1.2, uma chave mestra de criptografia é gerada automaticamente quando o servidor é iniciado, caso a chave mestra de criptografia ainda não existisse. A chave mestra de criptografia é armazenada em um banco de dados de chaves, dsmkeydb.kdb. Os certificados do servidor ainda são armazenados no banco de dados de chaves cert.kdb e acessados pelo arquivo stash cert.sth. Deve-se proteger os bancos de dados de chaves (cert.kdb e dsmkeydb.kdb) e os arquivos stash (cert.sth e dsmkeydb.sth) que fornecem acesso a cada um dos bancos de dados de chaves. Por padrão, o comando **BACKUP DB** protege a chave mestra de criptografia da mesma maneira em que o histórico do volume e os arquivos devconfig são protegidos. É necessário lembrar-se da senha de backup de banco de dados para restaurar o banco de dados. O arquivo `dsmserv.pwd` do servidor IBM Spectrum Protect, que foi usado para armazenar a chave mestra de criptografia em liberações anteriores, não é mais usado.
Planejar upgrades com cuidado para IDs de administrador	Identifique todos os sistemas que as contas do administrador usam para efetuar login para propósitos de administração. Após uma autenticação bem-sucedida para o software V8.1.2 ou mais recente, os administradores não podem se autenticar em versões anteriores do software IBM Spectrum Protect no mesmo servidor. Se um único ID de administrador é usado para efetuar login em múltiplos sistemas, planeje fazer upgrade de todos esses sistemas com o software V8.1.2 ou mais recente para assegurar que o certificado seja instalado em todos os sistemas nos quais o administrador efetua login. **Dica:** Você não será bloqueado de um servidor se o parâmetro **SESSIONSECURITY** de todos os seus IDs de administrador for atualizado para o valor STRICT. É possível importar manualmente o certificado público do servidor para um cliente do qual você emite o comando **dsmadmc**.

Tabela 2. Planejando a lista de verificação (continuação)

Diretriz	Descrição
Se você estiver usando o TLS com versões anteriores do cliente que usam o certificado "TSM Server SelfSigned Key" (cert.arm), atualize seus clientes para a V8.1.4 ou mais recente.	Em liberações anteriores à V7.1.8, o certificado padrão era rotulado como "TSM Server SelfSigned Key" e possuía uma assinatura MD5, que não suporta o protocolo TLS 1.2 ou mais recente que é exigido por padrão para os clientes V8.1.2 ou mais recentes e pelo Operations Center. Para resolver esse problema, conclua uma das etapas a seguir: • Faça upgrade do servidor para a V8.1.4 ou mais recente. Começando com o V8.1.4, os servidores que usam o certificado assinado por MD5 como o padrão são atualizados automaticamente para usarem um certificado padrão com uma assinatura SHA, que é rotulada como "TSM Server SelfSigned SHA Key". Uma cópia do novo certificado padrão é armazenada no arquivo `cert256.arm`, que está localizado no diretório de instância do servidor. **Dica:** Antes de atualizar o servidor para usar o novo certificado padrão com uma assinatura SHA, distribua o arquivo `cert256.arm` para os clientes para evitar falhas de backup de cliente. Cada cliente deve obter e importar o novo certificado antes de poder se conectar a um servidor que estiver usando o novo certificado SHA padrão. Não é necessário remover certificados prévios. • Para atualizar manualmente seu certificado padrão, siga as instruções na nota técnica 562939.

O Que Fazer a Seguir

- Siga o procedimento em “Aplicando atualizações de segurança” na página 7 para instalar ou fazer upgrade de um servidor IBM Spectrum Protect.
- Para obter informações sobre a resolução de problemas de comunicação relacionados a atualizações de segurança, veja “Resolução de problemas de atualizações de segurança” na página 13.
- Para obter informações de FAQ, consulte FAQ - Atualizações de segurança no IBM Spectrum Protect.
- Para obter informações sobre como usar o Web client de backup e archive do IBM Spectrum Protect no novo ambiente de segurança, consulte a nota técnica 728037.

Aplicando atualizações de segurança

Aplique atualizações de segurança que são entregues com novas liberações do IBM Spectrum Protect.

Antes de Iniciar

Revise as informações a seguir:

- Para obter detalhes sobre as atualizações de segurança entregues com uma liberação, consulte o tópico *O que há de novo* em IBM Knowledge Center.

- Para obter informações sobre as atualizações e quaisquer restrições que possam ser aplicadas, consulte “O que é necessário saber sobre segurança antes de instalar ou fazer upgrade do servidor” na página 3.
- Para determinar a ordem de upgrade dos servidores e clientes em seu ambiente, responda às seguintes questões:

Tabela 3. Perguntas a serem consideradas antes de fazer upgrade

Questões	**Contraprestação**
Qual é a função do servidor na configuração?	Em geral, é possível fazer upgrade dos servidores IBM Spectrum Protect em seu ambiente primeiro e, em seguida, fazer upgrade de clientes de backup e archive. No entanto, em determinadas circunstâncias, por exemplo, se você usar as funções de roteamento de comando, o servidor poderá agir como o cliente em sua configuração. Nesse caso, para evitar problemas de comunicação, a abordagem sugerida é fazer upgrade de clientes primeiro. Para obter informações sobre os diferentes cenários, consulte Cenários de upgrade.

Tabela 3. Perguntas a serem consideradas antes de fazer upgrade (continuação)

Questões	**Contraprestação**
Quais sistemas são usados para autenticação do administrador?	Para contas do administrador, a sequência de upgrade é importante para evitar problemas de autenticação. – Clientes em vários sistemas que efetuam logon usando o mesmo ID (ID do nó ou ID administrativo) devem ser submetidos a upgrade ao mesmo tempo. Os certificados do servidor são transferidos para os clientes automaticamente na primeira conexão. – Antes de fazer upgrade de seu servidor, considere todos os terminais que o administrador usa para se conectar para propósitos de administração. Se um único ID administrativo for usado para acessar múltiplos sistemas, assegure-se de que o certificado do servidor esteja instalado em cada sistema. – Depois que um ID de administrador autenticar com êxito no servidor usando o software IBM Spectrum ProtectV8.1.2 ou mais recente ou o software Tivoli Storage Manager V7.1.8 ou mais recente, o administrador não poderá mais autenticar nesse servidor usando as versões de cliente ou servidor anteriores à V8.1.2 ou V7.1.8. Isso também será verdadeiro para um servidor de destino quando você autenticar nesse servidor IBM Spectrum Protect de destino como um administrador de outro servidor. Por exemplo, isso será verdadeiro ao usar as seguintes funções: - Roteamento de - Exportação de servidor para servidor - Conexão de um cliente administrativo no Operations Center

Tabela 3. Perguntas a serem consideradas antes de fazer upgrade (continuação)

Questões	Contraprestação
Em qual sequência devo fazer upgrade de meus sistemas?	– **Se você fizer upgrade de servidores antes de fazer upgrade de nós clientes:** - Faça upgrade do servidor do hub primeiro e, em seguida, de quaisquer servidores spoke. - Quando fizer upgrade de um servidor para a V8.1.2 ou mais recente, os nós e administradores que usarem versões anteriores do software poderão continuar se comunicando com o novo servidor usando o protocolo de comunicação existente. O **SESSIONSECURITY** está configurado para TRANSITIONAL e se o servidor, nó ou administrador nunca atendeu aos requisitos para o valor STRICT, o servidor, nó ou administrador continuará a autenticar usando o valor TRANSITIONAL. No entanto, assim que o servidor, nó ou administrador atender aos requisitos para o valor STRICT, o valor de parâmetro **SESSIONSECURITY** será atualizado automaticamente de TRANSITIONAL para STRICT. – **Se você fizer upgrade de nós clientes antes de fazer upgrade de servidores:** - Faça upgrade de clientes administrativos primeiro e, em seguida, o upgrade de clientes não administrativos. Os clientes em níveis da liberação mais recentes continuarão se comunicando com servidores em níveis anteriores. **Importante:** Se você fizer upgrade de qualquer um dos clientes administrativos em seu ambiente, todos os outros clientes que usarem o mesmo ID que o cliente submetido a upgrade deverão ser submetidos a upgrade ao mesmo tempo. - Não será necessário fazer upgrade de todos os seus clientes não administrativos ao mesmo tempo, a menos que múltiplos clientes estejam usando o mesmo ID para efetuar logon. Então, todos os outros clientes que usarem o mesmo ID que o cliente com upgrade deverão ser submetidos a upgrade ao mesmo tempo e o certificado do servidor deverá ser instalado em cada sistema.

Sobre Esta Tarefa

Quando o seu ambiente inclui clientes de backup-archive do IBM Spectrum Protect ou servidores IBM Spectrum Protect anteriores à V7.1.8 ou à V8.1.2, talvez seja necessário customizar sua configuração para assegurar que a comunicação entre servidores e clientes não seja interrompida. Siga o procedimento padrão neste tópico para instalar ou atualizar seu ambiente.

Revise Cenários de upgrade para obter outros cenários de exemplo que possam se aplicar a seu ambiente.

Dica: Para aproveitar os aprimoramentos de segurança mais recentes, planeje atualizar todos os servidores e clientes de backup-archive do IBM Spectrum Protect em seu ambiente para o nível de liberação mais recente.

Procedimento

1. Instale ou faça upgrade de servidores IBM Spectrum Protect em seu ambiente. Para obter mais informações, consulte o tópico *Instalando e fazendo upgrade do servidor* no IBM Knowledge Center.
   a) Faça upgrade do Operations Center e do servidor do hub. Para obter informações adicionais, consulte Parte 2, “Instalando e Fazendo Upgrade do Operations Center”, na página 127.
   b) Faça upgrade dos servidores spoke.
   c) Configure ou verifique as comunicações servidor-para-servidor. Para obter mais informações, consulte os seguintes tópicos:
      - O comando *UPDATE SERVER* no IBM Knowledge Center.
      - O tópico *Configurando comunicações SSL entre o servidor do hub e um servidor spoke* no IBM Knowledge Center.
      - O tópico *Configurando o servidor para se conectar a outro servidor usando SSL* no IBM Knowledge Center.

      Dica:

      - A partir do IBM Spectrum Protect V8.1.2 e do Tivoli Storage Manager V7.1.8, o parâmetro **SSL** usará SSL para criptografar a comunicação com o servidor especificado, mesmo se o parâmetro **SSL** estiver configurado como NO.
      - A partir da V8.1.4, os certificados são configurados automaticamente entre agentes de armazenamento, clientes de biblioteca e servidores do gerenciador de bibliotecas. Os certificados são trocados na primeira vez que uma conexão servidor-para-servidor é estabelecida para um servidor com segurança aprimorada.
2. Instale ou faça upgrade de clientes administradores. Para obter mais informações, consulte o tópico *Instalando e configurando clientes* no IBM Knowledge Center.
3. Ative as comunicações seguras entre todos os sistemas que os administradores usam para efetuar login para propósitos de administração.
   - Assegure-se de que o software IBM Spectrum Protect que a conta do administrador usa para efetuar login seja submetido a upgrade para a V8.1.2 ou mais recente.
   - Se um ID administrativo efetuar logon por meio de múltiplos sistemas, assegure-se de que o certificado do servidor esteja instalado em cada sistema.
4. Instale ou faça upgrade de clientes não administrativos. Para obter mais informações, consulte o tópico *Instalando e configurando clientes* no IBM Knowledge Center.

   Lembre-se: É possível fazer upgrade dos clientes não administrativos em fases. É possível continuar se conectando a servidores em níveis de liberação mais recentes por meio de clientes em níveis de liberação anteriores emitindo o comando **UPDATE NODE** e configurando o parâmetro **SESSIONSECURITY** como TRANSITIONAL para cada nó.

   ```
   update node nodename sessionsecurity=transitório
   ```

O que Fazer Depois

Outros cenários de upgrade podem se aplicar a seu ambiente. Revise os cenários de upgrade de exemplo na tabela a seguir.

Tabela 4. Cenários de Atualização

Cenário	Contraprestações	Abordagem de upgrade sugerida
Eu uso funções de roteamento de comando administrativo para rotear comandos para um ou mais servidores. Quero conectar-me a um servidor IBM Spectrum Protect que seja anterior à V8.1.2.	• Com o roteamento de comando, o servidor pode agir como o cliente administrador. • O roteamento de comando usa o ID e a senha do administrador que está emitindo o comando. • Se você usar um único ID administrativo para acessar múltiplos sistemas, assegure-se de que o certificado do servidor esteja instalado em cada sistema.	• Faça upgrade do cliente administrador primeiro. **Importante:** Clientes em vários sistemas que efetuam logon usando o mesmo ID de nó ou ID administrativo devem ser submetidos a upgrade ao mesmo tempo. • Em cada servidor para o qual os comandos estão sendo roteados, verifique se as informações a seguir estão configuradas: – O mesmo ID de administrador e senha – A autoridade administrativa necessária em cada servidor – Os certificados necessários estão instalados • Faça upgrade dos servidores que a conta do administrador usa para efetuar logon na V8.1.2 ou mais recente.
Meu cliente administrativo está na versão de liberação mais recente e eu uso o mesmo ID de administrador para autenticação em sistemas diferentes usando o comando **dsmadmc**. Eu fui autenticado com êxito em um servidor do IBM Spectrum Protect em meu ambiente que está sendo executado na versão mais recente. Agora, desejo autenticar em um servidor em uma versão anterior à V8.1.2.	• Depois que um administrador se autenticar em um servidor IBM Spectrum Protect V8.1.2 ou mais recente usando uma versão do cliente na V8.1.2 ou mais recente, o ID administrativo poderá ser autenticado somente com esse servidor em clientes ou servidores que estiverem usando a V8.1.2 ou mais recente. • Se você usar um único ID administrativo para acessar múltiplos sistemas, planeje fazer upgrade de todos esses sistemas com o software V8.1.2 ou mais recente para assegurar que o certificado do servidor seja instalado em todos os sistemas nos quais o administrador efetua login.	• Assegure-se de que todos os softwares IBM Spectrum Protect que os administradores usam para efetuar logon sejam submetidos a upgrade para a V8.1.2 ou mais recente. A ação preferencial é fazer upgrade de todos os servidores em seu ambiente para a versão mais recente. • Se necessário, crie uma conta do administrador separada para usar somente com clientes e servidores que estão usando o software V8.1.1 ou anterior.

Tabela 4. Cenários de Atualização (continuação)

Cenário	Contraprestações	Abordagem de upgrade sugerida
O servidor IBM Spectrum Protect já foi submetido a upgrade para o nível da liberação mais recente. Eu tenho um cliente administrador no nível da liberação V8.1.0 e desejo conectar-me ao servidor por meio do Operations Center.	• Se você fizer upgrade de qualquer um dos clientes administrativos em seu ambiente, todos os outros clientes que usarem o mesmo ID que o cliente submetido a upgrade deverão ser submetidos a upgrade ao mesmo tempo. • Para usar um ID de administrador em uma configuração de múltiplos servidores, o ID deve ser registrado nos servidores de hub e spoke com a mesma senha, nível de autoridade e certificados necessários.	• Em cada servidor, verifique se as informações a seguir estão configuradas: – O mesmo ID de administrador e senha – A autoridade administrativa necessária em cada servidor – Os certificados necessários • Faça upgrade de clientes não administrativos por fase.
Eu uso a replicação de nó para proteger meus dados.	• A pulsação de replicação inicia uma troca de certificado quando a primeira conexão de servidor para servidor é estabelecida após o upgrade do servidor.	• Faça upgrade de seus servidores antes de fazer upgrade dos clientes; siga o procedimento padrão.
Quero fazer upgrade de meus clientes de backup-archive antes de fazer upgrade dos servidores.	• Depois que você fizer upgrade de um servidor para a V8.1.2 ou mais recente, os nós e os administradores que estiverem usando versões anteriores do software continuarão se comunicando com o servidor usando o valor TRANSITIONAL até que a entidade atenda aos requisitos para o valor STRICT. • A comunicação entre os servidores e clientes não será interrompida.	• Se você fizer upgrade de seus clientes antes do upgrade dos servidores, faça upgrade dos clientes administrativos primeiro e, em seguida, faça upgrade dos clientes não administrativos. Os clientes em níveis da liberação mais recentes continuarão se comunicando com servidores em níveis anteriores.

Resolução de problemas de atualizações de segurança

Solucione problemas que possam ocorrer após o upgrade do IBM Spectrum Protect.

Sintoma	Resolução
A conta do administrador não pode efetuar login em um sistema que está usando software anterior à V8.1.2.	Depois que um administrador for autenticar com sucesso no servidor usando o software IBM Spectrum Protect V8.1.2 ou mais recente, o administrador não poderá mais ser autenticado nesse servidor usando versões de cliente ou servidor anteriores à V8.1.2. Essa restrição também se aplica ao servidor de destino ao usar funções como roteamento de comando, exportação de servidor para servidor que é autenticada com o servidor de destino IBM Spectrum Protect como um administrador de outro servidor, conexões do administrador que usam o Operations Center e conexões do cliente da linha de comandos administrativos. Para resolver problemas de autenticação para administradores, conclua as etapas a seguir:

Sintoma	Resolução
	1. Identifique todos os sistemas por meio dos quais os administradores efetuam login e que usam o ID administrativo para efetuar login. Faça upgrade do software do sistema para o IBM Spectrum Protect V8.1.2 ou mais recente e assegure-se de que o certificado do servidor esteja instalado em cada sistema. 2. Configure o valor do parâmetro **SESSIONSECURITY** do administrador como TRANSITIONAL, emitindo o comando `update admin` *admin_name* `sessionsecurity=transitional` 3. Tente novamente a conexão do administrador. **Dica:** Se necessário, crie uma conta do administrador separada para usar somente com clientes e servidores que estão usando o software V8.1.1 ou anterior.

A distribuição do certificado falhou para um nó, administrador ou servidor.	Um nó, um administrador ou um servidor que está usando o software V8.1.2 ou mais recente tem um valor **SESSIONSECURITY** de STRICT, mas é necessário reconfigurar o valor para TRANSITIONAL para tentar novamente a distribuição do certificado.
	Ao usar o novo protocolo, a transferência automática do certificado público de um servidor é executada somente na primeira conexão com um servidor com segurança aprimorada. Após a primeira conexão, o valor do parâmetro **SESSIONSECURITY** de um nó muda de TRANSITIONAL para STRICT. É possível atualizar temporariamente um nó, um administrador ou um servidor como TRANSITIONAL para permitir outra transferência automática do certificado. Enquanto em TRANSITIONAL, a próxima conexão transferirá automaticamente o certificado, se necessário, e reconfigurará o parâmetro **SESSIONSECURITY** para STRICT.
	Atualize o valor do parâmetro **SESSIONSECURITY** para TRANSITIONAL, emitindo um dos comandos a seguir:
	• Para nós clientes, emita:
	`update node` *node_name* `sessionsecurity=transitional`
	• Para administradores, emita:
	`update admin` *admin_name* `sessionsecurity=transitional`
	• Para servidores, emita:
	`update server` *server_name* `sessionsecurity=transitional`
	Como alternativa, é possível transferir e importar manualmente o certificado público usando o utilitário dsmcert para emitir os comandos a seguir:
	`openssl s_client -connect tapsrv04:1500 -showcerts > tapsrv04.arm`
	`dsmcert -add -server tapsrv04 -file tapsrv04.arm`
	Se você está usando certificados assinados por CA, deve-se instalar os certificados raiz de CA e intermediário de CA em cada banco de dados de chaves para o cliente, servidor e agente de armazenamento que inicia a comunicação de SSL.

A troca de certificado entre os servidores IBM Spectrum Protect não foi bem-sucedida.	Ao usar o novo protocolo, a transferência automática do certificado público de um servidor é executada somente na primeira conexão com um servidor com segurança aprimorada. Após a primeira conexão, o valor do parâmetro **SESSIONSECURITY** de um servidor muda de TRANSITIONAL para STRICT. Tente novamente a troca de certificado entre dois servidores IBM Spectrum

Sintoma	Resolução
	Protect. Para obter informações, consulte *Tentando novamente a troca de certificado entre servidores*.

A troca de certificado entre um servidor IBM Spectrum Protect e um nó cliente não foi bem-sucedida.	Ao usar o novo protocolo, a transferência automática do certificado público de um servidor é executada somente na primeira conexão com um servidor com segurança aprimorada. Após a primeira conexão, o valor do parâmetro **SESSIONSECURITY** de um nó muda de TRANSITIONAL para STRICT. Para tentar novamente a troca de certificado entre clientes e servidores em versões anteriores à V8.1.2, conclua estas etapas:
	1. Para clientes existentes configurados para usar SSL com o certificado cert.arm, reconfigure-os para usar o certificado `cert256.arm`. Para obter instruções, consulte *Configurando agentes de armazenamento, servidores, clientes e o Centro de operações para se conectar ao servidor usando SSL* no IBM Knowledge Center.
	2. Atualize o certificado padrão emitindo o comando a seguir por meio do diretório de instância do servidor:
	`gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed -label "TSM Server SelfSigned SHA Key"`
	3. Reinicie o servidor.
	Para clientes e servidores na V8.1.2 e mais recente, os certificados são distribuídos automaticamente. Se a comunicação entre clientes ou servidores falhar, conclua estas etapas para tentar novamente a aquisição do certificado:
	1. Para nós e administradores, configure o parâmetro **SESSIONSECURITY** como TRANSITIONAL emitindo os comandos a seguir para cada nó ou administrador que você desejar tentar novamente:
	`update node *nodename* sessionsecurity=Transição`
	`update admin *adminname* sessionsecurity=transitório`
	Dica: Administradores autenticados usando o comando **dsmadmc**, o comando **dsmc** ou o programa dsm não poderão ser autenticados usando uma versão anterior depois de serem autenticados usando a V8.1.2 ou mais recente. Para resolver problemas de autenticação para administradores, consulte as seguintes dicas:
	• Assegure-se de que todos os softwares IBM Spectrum Protect que a conta do administrador usa para efetuar login sejam submetidos a upgrade para a V8.1.2 ou mais recente. Se uma conta do administrador efetua logon por meio de múltiplos sistemas, assegure-se de que o certificado do servidor esteja instalado em cada sistema antes de a conta do administrador ser usada para roteamento de comando.
	• Após um administrador autenticar-se em um servidor V8.1.2 ou mais recente usando um cliente V8.1.2 ou mais recente, o administrador pode autenticar-se somente em clientes ou servidores que estão usando a V8.1.2 ou mais recente. Um comando do administrador pode ser emitido a partir de qualquer sistema. Se necessário, crie uma conta do administrador separada para usar somente com clientes e servidores que estão usando o software V8.1.1 ou anterior.
	2. Para agentes de armazenamento, atualize a opção **STASESSIONSECURITY** no arquivo de opções do agente de armazenamento `dsmsta.opt` mudando o valor STRICT para TRANSITIONAL.
	3. Reinicie os servidores. As mudanças de certificado não entram em vigor até que você reinicie os servidores ou agentes de armazenamento.

Sintoma	Resolução
	4. Se ainda não for possível trocar certificados depois de concluir as etapas 1-4, inclua manualmente os certificados nos servidores e agentes de armazenamento e reinicie-os. Para obter instruções, consulte *Configurando agentes de armazenamento, servidores, clientes e o Centro de operações para se conectar ao servidor usando SSL* no IBM Knowledge Center.
Você deseja distribuir certificados manualmente para sistemas do cliente.	O administrador do servidor IBM Spectrum Protect pode implementar automaticamente um cliente de backup e archive para atualizar as estações de trabalho nas quais o cliente de backup e archive já está instalado. Para obter informações, consulte *Implementação automática do cliente de backup e archive* no IBM Knowledge Center. Para incluir certificados manualmente em clientes, consulte *Configurando a comunicação cliente/servidor do IBM Spectrum Protect com o Secure Sockets Layer* no IBM Knowledge Center.
Você deseja reconfigurar certificados para sessões cliente para cliente.	O utilitário dsmcert que é instalado com o cliente de backup e archive IBM Spectrum Protect é usado para criar um armazenamento de certificados para certificados do servidor. Use o utilitário dsmcert para excluir os arquivos e reimportar os certificados.
Como usuário raiz, você deseja permitir que usuários não raiz gerenciem seus arquivos.	O agente de comunicações confiável (TCA), anteriormente usado por usuários não raiz em clientes do IBM Spectrum Protect V8.1.0 e V7.1.6 e mais recentes, não está mais disponível. Os usuários raiz podem usar os métodos a seguir para permitir que usuários não raiz gerenciem seus arquivos: **Método de Help Desk** Com o método de help desk, o usuário raiz executa todas as operações de backup e restauração. O usuário não raiz deve entrar em contato com o usuário raiz para solicitar que o backup ou a restauração de determinados arquivos seja feita. **Método de usuário autorizado** Com o método de usuário autorizado, um usuário não raiz obtém o acesso de leitura/gravação ao armazém de senhas usando a opção `passworddir` para apontar para um local da senha que seja legível e gravável pelo usuário não raiz. Esse método permite que os usuários não raiz façam backup e restaurem seus próprios arquivos, usem criptografia e gerenciem suas senhas com a opção `passwordaccess generate`. Para obter mais informações, consulte *Permitir que usuários não raiz gerenciem seus próprios dados* no IBM Knowledge Center. Se nenhum desses métodos for satisfatório, deve-se usar os clientes anteriores que incluíram o TCA.
Você deseja resolver os problemas de compatibilidade do Global Security Kit (GSKit).	Quando vários aplicativos que usam o GSKit são instalados no mesmo sistema, podem ocorrer problemas de incompatibilidade. Para resolver esses problemas, consulte as informações a seguir: • Para clientes do IBM Spectrum Protect, consulte a Nota técnica 2011742. • Para o Db2, consulte a Nota técnica 7050721. • Para o servidor IBM Spectrum Protect, consulte a Nota técnica 2007298. • Para o servidor e o cliente do IBM Spectrum Protect no mesmo sistema Windows, consulte a Nota técnica 7050721.

Para obter mais informações sobre a resolução de problemas de atualizações de segurança, consulte a nota técnica 2004844.

Tentando novamente a troca de certificado entre servidores

Se a troca de certificado entre servidores falha, é possível tentar outra troca.

Procedimento

1. Remova o certificado do banco de dados do servidor parceiro emitindo o comando a seguir em ambos os servidores:

   ```
   update server  servername  forcesync=yes
   ```

   Dica: O servidor pode estar usando o certificado errado se você ainda estiver obtendo mensagens de erro para cada sessão de servidor para servidor depois de ter concluído as etapas nesta tarefa e reiniciado os servidores. Se você determinar que o servidor está tentando usar o certificado errado, exclua o certificado do banco de dados de chaves emitindo o comando a seguir:

   ```
   gsk8capicmd_64 -cert -delete -db cert.kdb -stashed -label certificate_labelname
   ```

2. Exclua a definição do servidor emitindo o comando **DELETE SERVER** para o servidor e o servidor parceiro. Quando não é possível excluir a definição de servidor, deve-se configurar os certificados manualmente. Para obter instruções sobre como configurar manualmente os certificados, consulte *Configurando agentes de armazenamento, servidores, clientes e o Operations Center para se conectar ao servidor usando SSL* no IBM Knowledge Center.
3. Para readquirir o certificado, defina de forma cruzada os servidores entre si e permita que eles troquem certificados emitindo os comandos a seguir em ambos os servidores:

   ```
   configurar crossdefine on
   set serverhladdress hladdress
   set serverlladdress lladdress
   set serverpassword  password
   ```

4. Emita o comando a seguir em um dos servidores que você está definindo de forma cruzada:

   ```
   define server  servername  crossdefine=yes ssl=yes
   ```

5. Repita a etapa 3 para todos os outros pares de servidores Versão 8.1.2 ou mais recentes.
6. Inicie os servidores novamente.
7. Para verificar se os certificados foram trocados, emita o comando a seguir por meio do diretório de instância do servidor de cada servidor que você deseja verificar:

   ```
   gsk8capicmd_64 -cert -list -db cert.kdb -stashed
   ```

   Saída de exemplo:

   ```
   example.website.com:1542:0
   ```

   Dica: Se você usar a replicação, a pulsação de replicação será executada aproximadamente a cada 5 minutos e iniciará uma troca de certificado durante a primeira conexão após o upgrade do servidor. Essa conexão faz com que as mensagens ANR8583E e ANR8599W apareçam no log uma vez, antes que uma troca de certificado ocorra. Se você não usa replicação, os certificados são trocados na primeira vez que uma sessão de servidor para servidor é iniciada, exceto para configurações do servidor sem um servidor definido em ambos os computadores.
8. Para servidores que estão definidos como um volume virtual, conclua as etapas a seguir:
   a) Remova o certificado do parceiro do banco de dados do servidor, emitindo o comando a seguir em ambos os servidores:

      ```
      update server  servername  forcesync=yes
      ```

b) Assegure-se de que a mesma seja usada para o valor de senha do servidor no comando **DEFINE SERVER** no servidor de origem, o valor de senha no comando **REGISTER NODE** no servidor de volume virtual e o valor **SET SERVERPASSWORD** no servidor de volume virtual. Se necessário, atualize uma senha usando os comandos **UPDATE SERVER**, **UPDATE NODE** ou **SET SERVERPASSWORD**, respectivamente. Os certificados são trocados após a primeira operação de backup de cliente do servidor de volume virtual para o servidor de origem.

9. Se ainda não for possível trocar certificados entre servidores, conclua as etapas a seguir:
   a) Na definição do servidor para cada um dos servidores de comunicação, verifique se você especificou um nome do servidor que corresponda ao nome que foi configurado, emitindo o comando **SET SERVERNAME** no servidor parceiro.
   b) Verifique se as definições do servidor têm senhas que são especificadas com o comando **SET SERVERPASSWORD**. As senhas devem corresponder ao valor especificado com o comando **SET SERVERNAME** para o servidor parceiro.
   c) Depois de concluir as etapas a e b, emita novamente o comando a seguir:

```
update server  servername  forcesync=yes
```

   d) Tente novamente as etapas 1 a 3.

Planejamento para o desempenho ideal

Antes de instalar o servidor IBM Spectrum Protect, avalie as características e a configuração do sistema para assegurar que o servidor esteja configurado para obter o desempenho ideal.

Sobre Esta Tarefa

O ambiente ideal do IBM Spectrum Protect é configurado usando o IBM Spectrum Protect Blueprints.

Procedimento

1. Revise o “O Que Você Deveria Saber Primeiro” na página 3.
2. Revise cada uma das subseções a seguir.

Planejando o hardware do servidor e o sistema operacional

Use a lista de verificação para verificar se o sistema no qual o servidor está instalado atende aos requisitos de configuração de hardware e software.

Questão	Tarefas, características, opções ou configurações	Mais Informações
O sistema operacional e o hardware atendem aos, ou excedem os, requisitos? • Número e velocidade de processadores • Memória do sistema • Nível do sistema operacional suportado	Se você estiver usando a quantia mínima necessária de memória, será possível suportar uma carga de trabalho mínima. É possível tentar incluir mais memória do sistema, para determinar se há melhoria no desempenho. Em seguida, decida se deseja manter a memória do sistema dedicada ao servidor. Teste as variações de memória usando o ciclo diário inteiro da carga de trabalho do servidor. Se você executar diversos servidores no sistema, inclua os requisitos para cada servidor para obter os requisitos do sistema. **Restrição:** Não use o Active Memory Expansion (AME). Quando você usa o AME, o software IBM Db2 usa páginas de 4 KB em vez de páginas de 64 KB. Cada página de 4 KB deve ser descompactada quando acessada e compactada quando não for necessária. Quando a compactação ou descompactação ocorre, o Db2 e o servidor esperam para acessar a página, o que compromete o desempenho do servidor.	Revise os requisitos do sistema operacional na nota técnica 84861. Além disso, revise a orientação em Ajustando Tarefas para Sistemas Operacionais e Outro Aplicativos. Para obter informações adicionais sobre os requisitos quando esses recursos estiverem em uso, consulte os tópicos a seguir: • Lista de verificação para deduplicação de dados • Lista de Verificação para Replicação de Nó Para obter mais informações sobre os requisitos de dimensionamento para o servidor e o armazenamento, consulte o IBM Spectrum Protect Blueprint.

Questão	Tarefas, características, opções ou configurações	Mais Informações
Os discos estão configurados para um desempenho ideal?	A quantia de ajuste que pode ser feita varia para diferentes sistemas de disco. Certifique-se de que as profundidades de fila adequadas e outras opções do sistema de disco estejam configuradas.	Para obter mais informações, consulte os seguintes tópicos: • "Planejando os discos de banco de dados do servidor" • "Planejando os discos de log de recuperação do servidor" • "Planejamento para conjuntos de armazenamentos em classes de dispositivo DISK ou FILE"
O servidor tem memória suficiente?	Cargas de trabalho mais pesadas e recursos avançados, como a deduplicação de dados e a replicação de nó requerem mais do que a memória mínima do sistema especificada no documento de requisitos do sistema. Para bancos de dados que não estão ativados para deduplicação de dados, use as diretrizes a seguir para especificar os requisitos de memória: • Para bancos de dados menores que 500 GB, são necessários 16 GB de memória. • Para bancos de dados com tamanhos de 500 GB a 1 TB, são necessários 24 GB de memória. • Para bancos de dados com tamanhos de 1 TB a 1,5 TB, são necessários 32 GB de memória. • Para bancos de dados maiores que 1,5 TB, são necessários 40 GB de memória. Certifique-se de alocar espaço adicional para o log ativo e o log de archive para o processamento de replicação.	Para obter informações adicionais sobre os requisitos quando esses recursos estiverem em uso, consulte os tópicos a seguir: • Lista de verificação para deduplicação de dados • Lista de Verificação para Replicação de Nó • Requisitos de memória

Questão	Tarefas, características, opções ou configurações	Mais Informações
O sistema possui adaptadores de barramento de host (HBAs) suficientes para manipular operações de dados que o servidor IBM Spectrum Protect deve executar simultaneamente?	Entenda quais operações requerem uso de HBAs ao mesmo tempo. Por exemplo, um servidor deve armazenar 1 GB/s de dados de backup enquanto também realiza a migração do conjunto de armazenamentos que requer 0,5 GB/s de capacidade para concluir. Os HBAs devem poder manipular todos os dados na velocidade requerida.	Consulte Ajustando a Capacidade do HBA.
A largura da banda da rede é maior do que o rendimento máximo planejado para os backups?	A largura da banda da rede deve permitir que o sistema conclua operações, como backups, no tempo permitido ou que atenda aos compromissos de nível de serviço. Para replicação de nó, a largura da banda da rede deve ser maior do que o rendimento máximo planejado.	Para obter mais informações, consulte os seguintes tópicos: • Ajustando o Desempenho de Rede • Lista de Verificação para Replicação de Nó

Questão	Tarefas, características, opções ou configurações	Mais Informações
Você está usando um sistema de arquivos preferencial para os arquivo do servidor IBM Spectrum Protect?	Use um sistema de arquivos que assegure o desempenho e a disponibilidade de dados ideais. O servidor usa E/S direta com sistemas de arquivos que suportam o recurso. Usar a E/S direta pode melhorar o rendimento e reduzir o uso do processador. Para obter mais informações sobre o sistema de arquivos preferencial para seu sistema operacional, consulte Sistemas de arquivos suportados pelo servidor do IBM Spectrum Protect.	Para obter mais informações, consulte Configurando o Sistema Operacional para Desempenho de Disco.

Questão	Tarefas, características, opções ou configurações	Mais Informações
Você está planejando configurar espaço de paginação suficiente?	O espaço de paginação ou o espaço de troca estende a memória disponível para processamento. Quando a quantidade de RAM livre no sistema é baixa, os programas ou dados que não estão em uso são movidos da memória para o espaço de paginação. Essa ação libera memória para outras atividades, como operações do banco de dados. **Restrição:** Não use espaço de paginação para incluir memória em seu sistema. O espaço de paginação destina-se a fornecer somente uma extensão limitada e temporária do espaço. Se o sistema usa espaço de paginação, a memória do sistema está cheia e deve ser estendida. Use um mínimo de 32 GB de espaço de paginação ou 50% e sua RAM, escolha o de maior valor.	

Planejamento para discos do banco de dados do servidor

Use a lista de verificação para verificar se o sistema no qual o servidor está instalado atende aos requisitos de configuração de hardware e software.

Questões	Tarefas, características, opções ou configurações	Informações adicionais
O banco de dados está em discos rápidos de baixa latência?	Não use as unidades a seguir para o banco de dados IBM Spectrum Protect: • Nearline SAS (NL-SAS) • SATA (Serial Advanced Technology Attachment) • Parallel Advanced Technology Attachment (PATA) Não use discos internos que são incluídos, por padrão, na maioria dos hardwares de servidor. Os discos de estado sólido (SSD) de grau corporativo, com interface Fibre Channel ou SAS, oferecem o melhor desempenho. Se você planejar usar as funções de deduplicação de dados do IBM Spectrum Protect, foque no desempenho do disco em termos de operações de E/S por segundo (IOPS).	Para obter mais informações, consulte Lista de verificação para deduplicação de dados.
O banco de dados está armazenado em discos ou LUNs separados dos discos ou LUNs que são usados para o log ativo, log de archive e volumes do conjunto de armazenamentos?	A separação do banco de dados do servidor de outros componentes ajuda a reduzir a contenção dos mesmos recursos por diferentes operações que devem ser executadas ao mesmo tempo. **Dica:** O banco de dados e o log de archive podem compartilhar uma matriz ao utilizar a tecnologia de unidade de estado sólido (SSD).	
Caso esteja utilizando RAID, você sabe como selecionar o nível de RAID ideal para seu sistema? Você está definindo todos os LUNs com o mesmo tamanho e tipo de RAID?	Quando um sistema precisa executar um grande número de gravações, o RAID 10 supera o RAID 5. No entanto, o RAID 10 requer mais discos do que o RAID 5 para a mesma quantia de armazenamento útil. Se o seu sistema de disco for RAID, defina todas as LUNs com o mesmo tamanho e tipo de RAID. Por exemplo, não misture 4+1 RAID 5 com 4+2 RAID 6.	

Questões	Tarefas, características, opções ou configurações	Informações adicionais
Caso uma opção para configurar o tamanho de faixa ou o tamanho de segmento esteja disponível, você está planejando otimizar o tamanho ao configurar o sistema de disco?	Caso seja possível configurar o tamanho de faixa ou segmento, use tamanhos de faixa de 64 KB ou 128 KB nos sistemas de disco para o banco de dados.	O tamanho de bloco que é usado para o banco de dados varia, dependendo do espaço de tabela. A maioria dos espaços de tabela usa blocos de 8 KB, enquanto outros usam blocos de 32 KB.
Você está planejando criar pelo menos quatro diretórios, também chamados de caminhos de armazenamento, em quatro LUNs separadas para o banco de dados? Crie um diretório por matriz distinta no subsistema. Se você tiver menos de três matrizes, crie um volume de LUN separado dentro da matriz.	Cargas de trabalho e o uso mais pesado de alguns recursos requerem mais caminhos de armazenamento do banco de dados do que os requisitos mínimos. As operações do servidor, como deduplicação de dados, causam um número alto de operações de entrada/saída por segundo (IOPS) para o banco de dados. Essas operações executam melhor quando o banco de dados tem mais diretórios. Para bancos de dados do servidor maiores que 2 TB, ou que se espera que cresçam até esse tamanho, use oito diretórios. Considere o crescimento planejado do sistema ao determinar quantos caminhos de armazenamento criar. O servidor usa maior número de caminhos de armazenamento mais efetivamente se os caminhos de armazenamento estiverem presentes quando o servidor é criado pela primeira vez. Use a variável *DB2_PARALLEL_IO* para forçar a ocorrência da E/S paralela nos espaços de tabela que têm um contêiner ou em espaços de tabela que têm contêineres em mais de um disco físico. Caso a variável *DB2_PARALLEL_IO* não seja configurada, o paralelismo de E/S será igual ao número de contêineres utilizados pelo espaço de tabela. Por exemplo, se um espaço de tabela abrange quatro contêineres, o nível de paralelismo de E/S utilizado é 4.	Para obter informações adicionais, consulte os seguintes tópicos: • Lista de verificação para deduplicação de dados • Lista de Verificação para Replicação de Nó Para obter ajuda com a previsão de crescimento quando o servidor duplicar dados, consulte a nota técnica 1596944. Para obter as informações mais recentes sobre o tamanho do banco de dados, reorganização do banco de dados e considerações de desempenho para servidores IBM Spectrum Protect, consulte a nota técnica 1683633. Para obter informações sobre como configurar a variável *DB2_PARALLEL_IO*, consulte Configurações recomendadas para as variáveis de registro do IBM Db2.

Questões	Tarefas, características, opções ou configurações	Informações adicionais
Todos os diretórios do banco de dados têm o mesmo tamanho?	Todos os diretórios que tiverem o mesmo tamanho asseguram um grau consistente de paralelismo para as operações do banco de dados. Se um ou mais diretórios do banco de dados forem menores que os outros, eles reduzem o potencial de pré-busca paralela otimizada. Esta diretriz também se aplicará se você precisar incluir caminhos de armazenamento após a configuração inicial do servidor.	
Você está planejando aumentar a profundidade da fila dos LUNs de banco de dados em sistemas AIX?	A profundidade da fila padrão geralmente é muito baixa.	Consulte a seção Configurando sistemas AIX para desempenho de disco.

Planejamento para os discos do log de recuperação do servidor

Use a lista de verificação para verificar se o sistema no qual o servidor está instalado atende aos requisitos de configuração de hardware e software.

Questões	Tarefas, características, opções ou configurações	Informações adicionais
O log ativo e o log de archive estão armazenados em discos ou em LUNs que são separados do que é usado para os volumes do conjunto de armazenamentos e de banco de dados?	Assegure-se de que os discos nos quais você coloca o log ativo não sejam usados para outros propósitos do servidor ou do sistema. Não coloque o log ativo em discos que contiverem o banco de dados do servidor, o log de archive ou os arquivos de sistema como página ou espaço de troca.	A separação do banco de dados do servidor, do log ativo e do log de archive ajuda a reduzir a contenção dos mesmos recursos para diferentes operações que devem ser executadas ao mesmo tempo.
Os logs estão em discos que possuem cache de gravação não volátil?	O cache de gravação não volátil permite que os dados sejam gravados nos logs o mais rápido possível. Operações de gravação mais rápidas para os logs pode melhorar o desempenho para operações do servidor.	

Questões	Tarefas, características, opções ou configurações	Informações adicionais
Você está configurando os logs com um tamanho que suporte adequadamente a carga de trabalho?	Se você não tiver certeza sobre a carga de trabalho, use o maior tamanho possível. **Log ativo** O tamanho máximo é 512 GB, configure a opção do servidor **ACTIVELOGSIZE**. Certifique-se de que haja pelo menos 8 GB de espaço livre no sistema de arquivos de log ativos após os logs ativos de tamanho fixo serem criados. **Log de archive** O tamanho do log de archive é limitado pelo tamanho do sistema de arquivos no qual ele está localizado, e não por uma opção do servidor. Faça com que o log de archive seja pelo menos maior do que o log ativo.	• Para obter detalhes do dimensionamento do log, consulte as informações do log de recuperação na nota técnica 400357. • Para obter informações sobre o dimensionamento ao usar a deduplicação de dados, consulte Lista de verificação para deduplicação de dados.
Você está definindo um log de failover de archive? Esse log será colocado em um disco separado do log de archive?	O log de failover de archive é para uso de emergência pelo servidor quando o log de archive ficar cheio. Discos mais lentos podem ser usados para o log de failover do archive.	Use a opção do servidor **ARCHFAILOVERLOGDIRECTORY** para especificar o local do log de failover do archive. Monitore o uso do diretório para o log de failover do archive. Se o log de failover do archive tiver que ser usado pelo servidor, o espaço para o log de archive poderá não ser grande o suficiente.
Ao espelhar o log ativo, você está usando apenas um único tipo de espelhamento?	É possível espelhar o log usando um dos seguintes métodos. Use apenas um tipo de espelhamento para o log. • Use a opção **MIRRORLOGDIRECTORY** que está disponível para o servidor IBM Spectrum Protect especificar um local de espelho. • Use o espelhamento de software, como o Gerenciador de Volume Lógico (LVM) no AIX. • Use o espelhamento no hardware do sistema de disco.	Se você espelhar o log ativo, assegure-se de que os discos para o log ativo e a cópia espelhada tenham velocidade e confiabilidade iguais. Para obter mais informações, consulte Configurando e ajustando o log de recuperação.

Planejamento para conjuntos de armazenamentos de contêiner em diretório e contêiner em nuvem

Revise como os conjuntos de armazenamentos de contêiner em diretório e de contêiner em nuvem são configurados para assegurar o desempenho ideal.

Questões	Tarefas, características, opções ou configurações	Mais Informações
Medido em termos de operações de entrada/saída por segundo (IOPS), você está usando um armazenamento em disco rápido para o banco de dados do IBM Spectrum Protect?	Use um disco de alto desempenho para o banco de dados. Use a tecnologia de unidade de estado sólido para o processamento de deduplicação de dados. Certifique-se de que o banco de dados tenha uma capacidade mínima de 3.000 IOPS. Para cada TB de dados que são submetidos a backup diariamente (antes da deduplicação de dados), inclua 1.000 IOPS nesse mínimo. Por exemplo, um servidor IBM Spectrum Protect que alimenta 3 TB de dados por dia precisaria de 6000 IOPS para os discos do banco de dados: `3000 IOPS minimum + 3000 (3 TB x 1000 IOPS) = 6000 IOPS`	Para obter recomendações sobre a seleção de disco, consulte "Planejando os discos de banco de dados do servidor." Para obter mais informações sobre IOPS, consulte os IBM Spectrum Protect Blueprints.

Questões	Tarefas, características, opções ou configurações	Mais Informações
Você possui memória suficiente para o tamanho de seu banco de dados?	Use no mínimo 40 GB de memória do sistema para servidores IBM Spectrum Protect, com um tamanho de banco de dados de 100 GB e que deduplicam dados. Se a capacidade retida de dados de backup aumentar, o requisito de memória pode precisar ser maior. Monitore o uso de memória regularmente para determinar se mais memória é necessária. Use mais memória do sistema para melhorar o armazenamento em cache das páginas do banco de dados. As diretrizes de tamanho de memória a seguir são baseadas na quantidade diária de novos dados que são feitos backup: • 128 GB de memória do sistema para backups diários de dados, em que o tamanho do banco de dados é de 1 - 2 TB • 192 GB de memória do sistema para backups diários de dados, em que o tamanho do banco de dados é de 2 - 4 TB	Requisitos de memória

Questões	Tarefas, características, opções ou configurações	Mais Informações
Você dimensionou adequadamente a capacidade de armazenamento para o log ativo do banco de dados e o log de archive?	Configure o servidor para que o log ativo tenha um tamanho mínimo de 128 GB, configurando a opção do servidor **ACTIVELOGSIZE** com um valor de 131072. O tamanho inicial sugerido para o log de archive é de 1 TB. O tamanho do log de archive é limitado pelo tamanho do sistema de arquivos no qual ele está localizado, e não por uma opção do servidor. Certifique-se de que haja pelo menos 10% de espaço em disco adicional para o sistema de arquivos além do tamanho do log de archive. Use um diretório para os logs de archive do banco de dados com uma capacidade livre inicial de pelo menos 1 TB. Especifique o diretório usando a opção do servidor **ARCHLOGDIRECTORY**. Defina espaço para o log de failover de archive usando a opção do servidor **ARCHFAILOVERLOGDIRECTORY**.	Para obter mais informações sobre como dimensionar o sistema, consulte os IBM Spectrum Protect Blueprints.
A compactação está ativada para o log de archive e os backups do banco de dados?	Ative a opção do servidor ARCHLOGCOMPRESS para economizar espaço de armazenamento. Essa opção de compactação é diferente da compactação sequencial. A compactação sequencial é ativada por padrão com o IBM Spectrum Protect V7.1.5 e posteriores. **Restrição:** Não use essa opção se a quantidade de dados de backup exceder 6 TB por dia.	Para obter mais informações sobre compactação para o sistema, consulte os IBM Spectrum Protect Blueprints.
O banco de dados e os logs do IBM Spectrum Protect estão em volumes de discos separados (LUNs)? O disco que é usado para o banco de dados está configurado de acordo com as melhores práticas para um banco de dados transacional?	O banco de dados não deve compartilhar volumes de disco com log do banco de dados ou conjuntos de armazenamentos do IBM Spectrum Protect ou com qualquer outro aplicativo ou sistema de arquivos.	Para obter mais informações sobre a configuração do banco de dados do servidor e do log de recuperação, consulte Configuração e ajuste de log do banco de dados do servidor e de recuperação.

Questões	Tarefas, características, opções ou configurações	Mais Informações
Você está usando no mínimo 8 processadores (2.2 GHz ou equivalente) para cada servidor IBM Spectrum Protect que será utilizado com a deduplicação de dados?	Se você estiver planejando usar a deduplicação de dados do lado do cliente, verifique se os sistemas do cliente possuem recursos adequados disponíveis durante uma operação de backup para concluir o processamento da deduplicação de dados. Use um processador que seja equivalente a pelo menos um núcleo de processador de 2.2 GHz por processo de backup com a deduplicação de dados do lado do cliente.	• Perguntas mais frequentes sobre deduplicação de dados • IBM Spectrum Protect Blueprints
Foi alocado espaço de armazenamento suficiente para o banco de dados?	Para obter uma estimativa aproximada, planeje-se para 100 GB de armazenamento de banco de dados para cada 25 TB de dados que devem ser protegidos em conjuntos de armazenamentos deduplicado. *Dados protegidos* representa a quantidade de dados antes da deduplicação de dados, incluindo todas as versões de objetos armazenados. Para operações de backup de banco de dados com um grande número de arquivos pequenos, em que o tamanho médio do arquivo é menor que 512 KB, é necessário mais espaço de banco de dados. Para tamanhos de objetos menores, planeje-se para 100 GB de espaço de banco de dados para cada 10 TB armazenado. Como uma boa prática, defina um novo conjunto de armazenamentos de contêiner exclusivamente para a deduplicação de dados. A deduplicação de dados ocorre no nível do conjunto de armazenamento, e todos os dados contidos no conjunto de armazenamento, exceto dados criptografados, são deduplicados.	O ambiente ideal do IBM Spectrum Protect é configurado usando o IBM Spectrum Protect Blueprints.

Questões	Tarefas, características, opções ou configurações	Mais Informações
Você estimou a capacidade do conjunto de armazenamentos para configurar espaço suficiente para o tamanho do seu ambiente?	É possível estimar os requisitos de capacidade para um conjunto de armazenamentos deduplicado utilizando a seguinte técnica: 1. Estime o tamanho base dos dados de origem. 2. Estime o tamanho de backup diário usando uma taxa de mudança e crescimento estimada. 3. Determine os requisitos de retenção. 4. Estime a quantia total de dados de origem fatorando o tamanho base, o tamanho de backup diário e os requisitos de retenção. 5. Aplique o fator de proporção de deduplicação. 6. Aplique o fator de proporção de compactação. 7. Arredonde a estimativa para considerar o uso do conjunto de armazenamentos temporário.	Para obter um exemplo de uso dessa técnica, consulte Perguntas mais frequentes sobre deduplicação de dados.

Questões	Tarefas, características, opções ou configurações	Mais Informações
Você distribuiu a E/S de disco entre muitos dispositivos e controladores de disco?	Use matrizes consistentes com o máximo de discos possíveis, o que, às vezes, é mencionado como wide striping. Certifique-se de utilizar um diretório do banco de dados por matriz distinta no subsistema. Configure a variável de registro *DB2_PARALLEL_IO* para ativar a E/S paralela para cada espaço de tabela utilizado se os contêineres no espaço de tabela abrangerem vários discos físicos. Quando a largura da banda estiver disponível e os arquivos forem grandes, por exemplo, 1 MB, o processo de localização de duplicatas pode ocupar os recursos de um processador inteiro. Quando os arquivos são menores, outros gargalos podem ocorrer. Especifique oito ou mais sistemas de arquivos para a classe de dispositivo do conjunto de armazenamentos deduplicado, para que a E/S seja distribuída entre o maior número possível de LUNs e dispositivos físicos.	Para obter diretrizes sobre a configuração de conjuntos de armazenamentos, consulte "Planejando conjuntos de armazenamento em classes de dispositivo DISK ou FILE." Para obter informações sobre como configurar a variável *DB2_PARALLEL_IO*, consulte Configurações recomendadas para as variáveis de registro do IBM Db2.
Você planejou operações diárias com base em sua estratégia de backup?	A sequência de boa prática das operações é a seguinte ordem: 1. Backup de cliente 2. Proteção do conjunto de armazenamentos 3. Replicação de nó 4. Backup de banco de dados 5. Inventário de Expiração	• Planejando Processos de Deduplicação de Dados e Replicação de Nó • Operações diárias para conjuntos de armazenamentos de contêiner de diretório
Você planejou operações de auditoria para identificar arquivos corrompidos em conjuntos de armazenamentos?	Para planejar operações de auditoria, use o comando **DEFINE STGRULE** e especifique o parâmetro **ACTIONTYPE=AUDIT**. Como uma boa prática, para assegurar que as operações de auditoria sejam executadas continuamente, não especifique o parâmetro **DELAY**.	

Questões	Tarefas, características, opções ou configurações	Mais Informações
Você tem armazenamento suficiente para gerenciar a lista de bloqueios do IBM Db2?	Ao deduplicar dados que incluem arquivos grandes ou grandes quantidades de arquivos simultaneamente, o processo pode resultar em espaço de armazenamento insuficiente. Quando o armazenamento da lista de bloqueios é insuficiente, podem ocorrer falhas de backup, falhas no processo de gerenciamento de dados ou indisponibilidades do servidor. Os arquivos de tamanhos superiores a 500 GB que são processados pela deduplicação de dados são os que mais provavelmente esgotarão o espaço de armazenamento. No entanto, caso várias operações de backup usem a deduplicação de dados do lado do cliente, esse problema também pode ocorrer com arquivos de tamanhos menores.	Para obter informações sobre o ajuste do parâmetro Db2 **LOCKLIST**, consulte Ajustando a deduplicação de dados do lado do servidor .
A largura da banda disponível é suficiente para transferir dados para um servidor IBM Spectrum Protectw	Para transferir dados para um servidor IBM Spectrum Protect, use a deduplicação e a compactação de dados do lado do cliente ou do lado do servidor para reduzir a largura de banda que é necessária. Use um servidor V7.1.5 ou superior para usar a compactação sequencial e use um cliente V7.1.6 ou posterior para ativar o processo de compactação aprimorado.	Para obter mais informações, consulte a opção do cliente **enablededup**.
Você determinou quantos diretórios do conjunto de armazenamentos devem ser designados para cada conjunto de armazenamentos?	Designe diretórios para um conjunto de armazenamentos utilizando o comando **DEFINE STGPOOLDIRECTORY**. Crie vários diretórios de conjuntos de armazenamentos e certifique-se de que o backup de cada diretório seja feito em um volume de disco (LUN) separado.	

Questões	Tarefas, características, opções ou configurações	Mais Informações
Foi alocado espaço em disco suficiente no conjunto de armazenamentos de contêiner em nuvem?	Para evitar falhas de backup, assegure-se de que o diretório local tenha espaço suficiente. Use a lista a seguir como um guia para espaço em disco otimizado: • Para o Serial-attached SCSI (SAS) e o disco giratório, calcule a quantia de novos dados esperados após a redução de dados diários (compactação e deduplicação de dados). Aloque até 100 por cento dessa quantia, em terabytes, para o espaço de disco. • Forneça 3 TB para os sistemas de armazenamento baseados em flash com conexões rápidas de rede nos sistemas em nuvem do local e de alto desempenho. • Forneça 5 TB para sistemas de unidade de estado sólido (SSD) com conexões rápidas de rede para sistemas em nuvem de alto desempenho.	

Questões	Tarefas, características, opções ou configurações	Mais Informações
Foi selecionado o tipo apropriado de armazenamento local?	Assegure-se de que as transferências de dados do armazenamento local para a nuvem terminem antes que o próximo ciclo de backup comece. **Dica:** Os dados são removidos do armazenamento local logo após serem movidos para a nuvem. Use as diretrizes a seguir: • Use o flash ou a SSD para sistemas grandes que possuem sistemas em nuvem de alto desempenho. Assegure-se de ter um link rede de longa distância (WAN) de 10 GB dedicada com uma conexão de alta velocidade para o armazenamento de objeto. Por exemplo, use flash ou SSD se você tiver um link WAN 10 GB dedicado mais uma conexão de alta velocidade para um local do IBM Cloud Object Storage ou para um datacenter do Amazon Simple Storage Service (Amazon S3). • Use uma capacidade maior de 15.000 rpm de discos SAS para estes cenários: – Sistemas de tamanho médio – Conexões em nuvem mais lentas, por exemplo, 1 GB – Quando você usa o IBM Cloud Object Storage como seu provedor de serviços em várias regiões • Para o SAS ou disco giratório, calcule a quantia de novos dados esperados após a redução de dados diários (compactação e deduplicação de dados). Aloque até 100 por cento dessa quantia, em terabytes, para o espaço de disco.	

Questões	Tarefas, características, opções ou configurações	Mais Informações
Para conjuntos de armazenamentos de contêiner em nuvem, você especificou o número máximo total de processos paralelos para a regra de armazenamento e cada uma de suas sub-regras?	Para especificar o número máximo de processos paralelos, emita o comando **DEFINE STGRULE** e especifique o parâmetro **MAXPROCESS**. O valor padrão é 8. Por exemplo, se o valor padrão 8 for especificado e a regra de armazenamento tiver quatro sub-regras, a regra de armazenamento poderá executar oito processos paralelos e cada uma de suas sub-regras poderá executar oito processos paralelos. Para obter o rendimento ideal, use o número máximo de processos paralelos a seguir para sistemas Blueprint pequenos, médios e grandes: • Sistema pequeno: 10 processos • Sistema médio: 25 processos • Sistema grande: 35-50 processos	
Para conjuntos de armazenamento de contêineres em nuvem, você definiu diversos terminais do Accesser caso esteja usando um sistema IBM Cloud Object Storage no local com o IBM Spectrum Protect?	Para otimizar o desempenho, defina o acesso exclusivo para o seguinte número de Accessers para sistemas de blueprint pequeno, médio e grande, dependendo dos requisitos de ingestão de dados: • Sistema pequeno: 1 Accesser • Sistema médio: 2 Accessers • Sistema grande: 3 a 4 Accessers	Para obter informações adicionais, consulte o IBM Spectrum Protect Cloud Blueprints.

Questões	Tarefas, características, opções ou configurações	Mais Informações
Para conjuntos de armazenamentos de contêiner em nuvem, você definiu diversos terminais Accesser, caso esteja usando um sistema IBM Cloud Object Storage no local com o IBM Spectrum Protect?	Geralmente, o recurso Ethernet a seguir é necessário para se conectar a terminais privados do IBM Cloud Object Storage para sistemas Blueprint pequenos, médios e grandes: • Sistema pequeno: 1 Gbit • Sistema médio: 5 Gbit • Sistema grande: 10 Gbit **Dica:** Dependendo da ingestão de dados do cliente e da transferência de dados simultânea para o armazenamento de objeto, você pode requerer mais de uma rede Ethernet de 10 Gbit. Ao configurar a conexão Ethernet, trabalhe com um administrador de rede e considere os fatores a seguir: • A capacidade do servidor Ethernet • A natureza da rede entre o servidor e o terminal do IBM Cloud Object Storage • O ponto de ingestão final no armazenamento de objeto por meio de um conjunto de armazenamentos de contêiner em nuvem	

Planejamento para conjuntos de armazenamentos em classes de dispositivo DISK ou FILE

Use a lista de verificação para revisar a configuração dos conjuntos de armazenamentos em disco. Essa lista de verificação inclui dicas para conjuntos de armazenamentos que usam classes de dispositivos `DISK` ou `FILE`.

Questão	Tarefas, características, opções ou configurações	Mais Informações
As LUNs do conjunto de armazenamentos podem sustentar taxas de rendimento para leituras e gravações sequenciais de 356KB que manipulem adequadamente a carga de trabalho dentro das restrições de tempo?	Quando estiver planejando picos de carregamentos, considere todos os dados que deseja que o servidor leia e grave nos conjuntos de armazenamentos em disco simultaneamente. Por exemplo, considere o pico de fluxo de dados das operações de backup do cliente e das operações de movimentação de dados do servidor, como migração, que são executadas ao mesmo tempo. O servidor IBM Spectrum Protect lê e grava nos conjuntos de armazenamentos predominantemente em blocos de 256 KB. Se o sistema de disco inclui o recurso, configure o sistema de disco para um desempenho ideal com operações de leitura/gravação sequenciais ao invés de operações de leitura/gravação aleatórias.	Para obter mais informações, consulte Analisando o Desempenho Básico de Sistemas de Disco.

Questão	Tarefas, características, opções ou configurações	Mais Informações
Foi alocado espaço de armazenamento suficiente para o banco de dados?	Para uma estimativa aproximada, as diretrizes de tamanho do banco de dados a seguir se baseiam nos sistemas blueprint pequenos, médios e grandes para permitir o crescimento do banco de dados: • Sistema pequeno: Pelo menos 1 TB • Sistema médio: Pelo menos 2 TB • Sistema grande: Pelo menos 4 TB **Dica:** Talvez você precise de mais memória com base na quantia de dados que deve ser protegida, no número de arquivos armazenados e se você usa deduplicação de dados. Com a deduplicação de dados, o carregamento no banco de dados se torna maior porque haverá consultas frequentes para o banco de dados para determinar quais extensões deduplicadas estão no servidor. Para se ter uma estimativa aproximada, planeje 100 GB de armazenamento do banco de dados para cada 50 TB de dados que devem ser protegidos em conjuntos de armazenamentos deduplicados. Dados protegidos são a quantia de dados antes da deduplicação de dados, incluindo todas as versões de objetos armazenados. Se você tiver várias centenas de TB de dados protegidos ou se estiver fazendo backup de vários TBs de dados diariamente, o tamanho inicial do banco de dados deverá ser de pelo menos 1 TB. Use o IBM Spectrum Protect para dimensionar o banco de dados para seu sistema.	O ambiente ideal do IBM Spectrum Protect é configurado usando o IBM Spectrum Protect Blueprints. Para obter informações sobre a quantia mínima de memória que deve ser alocada no servidor para concluir as operações, com base no tamanho do banco de dados, consulte Requisitos de memória.
O disco está configurado para usar cache de leitura e gravação?	Use mais cache para obter um desempenho melhor.	

Questão	Tarefas, características, opções ou configurações	Mais Informações
Você precisa fazer backup do banco de dados IBM Spectrum Protect para o armazenamento de objeto de nuvem?	É possível fazer backup de um banco de dados para o armazenamento de objetos de nuvem e restaurar um banco de dados a partir dele para propósitos de recuperação de desastres. É possível ajustar terminais de armazenamento de objeto, IBM Cloud Object Storage Accessers, largura da banda da rede e fluxos de dados para assegurar que as operações de backup de banco de dados sejam executadas de forma eficiente.	Ajustando backups de banco de dados para armazenamento de objeto de nuvem.
Para conjuntos de armazenamentos que usam classes de dispositivo FILE, você determinou um bom tamanho a ser usado pelos volumes do conjunto de armazenamentos?	Revise as informações em Número e Tamanho Ideais para Volumes para Conjuntos de Armazenamentos que Usam Disco. Se você não tiver as informações para estimar um tamanho para os volumes de classe de dispositivo FILE, inicie com volumes de 50 GB.	Normalmente, problemas surgem mais frequentemente quando os volumes são muito pequenos. Alguns problemas são relatados quando os volumes são maiores do que o necessário. Ao determinar o tamanho de volume a ser utilizado, como precaução, escolha um tamanho que talvez seja maior do que o necessário.
Para conjuntos de armazenamentos que usam classes de dispositivo FILE, você está usando volumes pré-alocados?	Volumes utilizáveis podem causar fragmentação de arquivo. Para assegurar que um conjunto de armazenamentos não execute sem volumes, configure o parâmetro **MAXSCRATCH** para um valor maior que zero.	Use o comando do servidor **DEFINE VOLUME** para pré-alocar volumes no conjunto de armazenamentos. Use o comando do servidor **DEFINE STGPOOL** ou **UPDATE STGPOOL** para configurar o parâmetro **MAXSCRATCH**.
Para conjuntos de armazenamentos que usam classes de dispositivos FILE, você comparou o número máximo de sessões de cliente com o número de volumes que estão definidos?	Sempre mantenha volumes utilizáveis suficientes nos conjuntos de armazenamentos para permitir que o número de pico esperado de sessões do cliente seja executado de uma vez. Os volumes podem ser volumes utilizáveis, volumes vazios ou volumes parcialmente preenchidos.	Para conjuntos de armazenamentos que usam classes de dispositivos FILE, apenas uma sessão ou processo pode gravar em um volume ao mesmo tempo.

Questão	Tarefas, características, opções ou configurações	Mais Informações
Para conjuntos de armazenamentos que usam classes de dispositivo FILE, você configurou o parâmetro **MOUNTLIMIT** da classe de dispositivo para um valor alto o suficiente para contabilizar o número de volumes que podem ser montados em paralelo?	Para conjuntos de armazenamentos que usam deduplicação de dados, o parâmetro **MOUNTLIMIT** geralmente está no intervalo de 500 a 1000. Configure o valor de **MOUNTLIMIT** com o número máximo de pontos de montagem necessários para todas as sessões ativas. Considere os parâmetros que afetam o número máximo de pontos de montagem necessários: • A opção do servidor **MAXSESSIONS**, que é o número máximo de sessões do IBM Spectrum Protect que podem ocorrer simultaneamente. • O parâmetro **MAXNUMMP**, que configura o número máximo de pontos de montagem que cada nó cliente pode usar. Por exemplo, se o número máximo de sessões de backup do nó cliente geralmente for 100 e cada um dos nós tiver MAXNUMMP=2, multiplique 100 nós pelos 2 pontos de montagem para cada nó para obter o valor de 200 para o parâmetro **MOUNTLIMIT**.	Use o comando do servidor **REGISTER NODE** ou **UPDATE NODE** para configurar o parâmetro **MAXNUMMP** para os nós clientes.

Questão	Tarefas, características, opções ou configurações	Mais Informações
Para conjuntos de armazenamentos que usam classes de dispositivo DISK, você determinou quantos volumes do conjunto de armazenamentos são colocados em cada sistema de arquivos?	O modo com que você configura o armazenamento para um conjunto de armazenamentos que usa uma classe de dispositivo DISK depende se você estiver usando RAID para o sistema de disco. Se você não estiver usando RAID, configure um sistema de arquivos por disco físico e defina um volume do conjunto de armazenamentos para cada sistema de arquivos. Se você estiver usando RAID 5 com *n*+1 volumes, configure o armazenamento de uma das seguintes formas: • Configure *n* sistemas de arquivos na LUN e defina um volume do conjunto de armazenamentos por sistema de arquivos. • Configure um sistema de arquivos e *n* volumes do conjunto de armazenamentos para a LUN.	Para obter um layout de exemplo que siga essas recomendações, consulte Layout de amostra de conjuntos de armazenamentos do servidor.
Você criou seus conjuntos de armazenamentos para distribuir a E/S entre diversos sistemas de arquivos?	Assegure-se de que cada sistema de arquivos esteja em uma LUN diferente no sistema de disco. Geralmente, o ideal é ter de 10 a 30 sistemas de arquivo, mas certifique-se de que os sistemas de arquivos não sejam menores que cerca de 250 GB.	Para obter detalhes, consulte os seguintes tópicos: • Ajustando o Armazenamento em Disco para o Servidor • Ajustando e Configurando Conjuntos e Volumes de Armazenamento
Você planejou operações de auditoria para identificar arquivos corrompidos em conjuntos de armazenamentos?	Para planejar operações de auditoria, use o comando **DEFINE STGRULE** e especifique o parâmetro **ACTIONTYPE=AUDIT**. Para ajudar a otimizar as operações de auditoria e assegurar que elas sejam executadas continuamente, não especifique o parâmetro **DELAY**.	

Planejamento do tipo correto de tecnologia de armazenamento

Os dispositivos de armazenamento possuem diferentes características de capacidade e desempenho. Essas características determinam quais dispositivos são melhores para serem usados com o IBM Spectrum Protect.

Procedimento

- Revise a tabela a seguir para ajudá-lo a escolher o tipo correto de tecnologia de armazenamento para os recursos de armazenamento necessários para o servidor.

Tabela 5. Tipos de Tecnologia de Armazenamento para os Requisitos de Armazenamento do IBM Spectrum Protect

Tipo de tecnologia de armazenamento	Banco de Dados	Log ativo	Log de archive e log de failover de archive	Conjuntos de armazenamentos
Disco de estado sólido (SSD)	Coloque o banco de dados no SSD nas seguintes circunstâncias: – Você está usando a deduplicação de dados do IBM Spectrum Protect. – Você está fazendo backup de mais de 8 TB de novos dados diariamente.	Ao colocar o banco de dados IBM Spectrum Protect em um SSD, como boa prática, coloque o log ativo em um SSD. Se não houver espaço disponível, use o disco de alto desempenho em substituição.	Reserve SSDs para serem usados com o banco de dados e o log ativo. O log de archive e os logs de failover de archive podem ser colocados em tipos de tecnologia de armazenamento mais lenta.	Reserve SSDs para serem usados com o banco de dados e o log ativo. Os conjuntos de armazenamentos podem ser colocados em tipos de tecnologia de armazenamento mais lenta.
Disco de alto desempenho com as seguintes características: **– Disco de 15k rpm** **– Interface Fibre Channel ou Serial-attached SCSI (SAS)**	Use discos de alto desempenho nas seguintes circunstâncias: – O servidor não faz deduplicação de dados. – O servidor não faz replicação de nó. Isole o banco de dados do servidor de seus logs e conjuntos de armazenamento e dos dados de outros aplicativos.	Use discos de alto desempenho nas seguintes circunstâncias: – O servidor não faz deduplicação de dados. – O servidor não faz replicação de nó. Para obter desempenho e disponibilidade, isole o log ativo do banco de dados do servidor, dos logs de archive e dos conjuntos de armazenamento.	É possível usar discos de alto desempenho para o log de archive e os log de failover de archive. Para obter disponibilidade, isole esses logs do banco de dados e do log ativo.	Use discos de alto desempenho para conjuntos de armazenamento nas seguintes circunstâncias: – Os dados são lidos com frequência. – Os dados são gravados com frequência. Para obter desempenho e disponibilidade, isole os dados do conjunto de armazenamentos do banco de dados e logs do servidor e dos dados de outros aplicativos.

Tabela 5. Tipos de Tecnologia de Armazenamento para os Requisitos de Armazenamento do IBM Spectrum Protect (continuação)

Tipo de tecnologia de armazenamento	Banco de Dados	Log ativo	Log de archive e log de failover de archive	Conjuntos de armazenamentos
Disco de médio desempenho ou de alto desempenho com as seguintes características: **– Disco de 10k rpm** **– Interface Fibre Channel ou SAS**	Se o sistema de disco tiver uma combinação de tecnologias de disco, use os discos mais rápidos para o banco de dados e os logs ativos. Isole o banco de dados do servidor de seus logs e conjuntos de armazenamento e dos dados de outros aplicativos.	Se o sistema de disco tiver uma combinação de tecnologias de disco, use os discos mais rápidos para o banco de dados e os logs ativos. Para obter desempenho e disponibilidade, isole o log ativo do banco de dados do servidor, dos logs de archive e dos conjuntos de armazenamento.	É possível usar um disco de médio desempenho ou de alto desempenho para o log de archive e os logs de failover de archive. Para obter disponibilidade, isole esses logs do banco de dados e do log ativo.	Use um disco de médio desempenho ou de alto desempenho para conjuntos de armazenamentos nas seguintes circunstâncias: – Os dados são lidos com frequência. – Os dados são gravados com frequência. Para obter desempenho e disponibilidade, isole os dados do conjunto de armazenamentos do banco de dados e logs do servidor e dos dados de outros aplicativos.
SATA, armazenamento conectado à rede	Não use esse armazenamento para o banco de dados. Não coloque o banco de dados nos XIV Storage Systems.	Não use esse armazenamento para o log ativo.	O uso dessa tecnologia de armazenamento mais lenta é aceitável porque esses logs são gravados uma única vez e lidos com pouca frequência.	Use essa tecnologia de armazenamento mais lenta nas seguintes circunstâncias: – Os dados são gravados raramente, por exemplo, são gravados uma vez. – Os dados são lidos raramente. .
Fita e fita virtual				Use para retenção de longo prazo ou se os dados forem usados com pouca frequência.

Aplicando boas práticas para a instalação do servidor

Geralmente, a configuração e a seleção de hardware têm o efeito mais significativo no desempenho de uma solução do IBM Spectrum Protect. Outros fatores que afetam o desempenho são a seleção e a configuração do sistema operacional e a configuração do IBM Spectrum Protect.

Procedimento

- As melhores práticas a seguir são as mais importantes para o desempenho ideal e a prevenção de problemas.
- Revise a tabela para determinar as melhores práticas que se aplicam ao seu ambiente.

Melhor Prática	Mais Informações
Use discos rápidos para o banco de dados do servidor. Os discos de estado sólido (SSD) de grau corporativo, com interface Fibre Channel ou SAS, oferecem o melhor desempenho.	Use discos rápidos de baixa latência para o banco de dados. O uso de SSD será essencial se você estiver usando deduplicação de dados e replicação de nó. Evite discos Serial ATA e Parallel Advanced Technology Attachment (PATA). Para obter detalhes e mais dicas, consulte os tópicos a seguir: – "Planejando os discos de banco de dados do servidor" – "Planejamento do tipo correto de tecnologia de armazenamento"
Assegure-se de que o sistema do servidor tenha memória suficiente.	Revise os requisitos do sistema operacional na nota técnica 84861. Cargas de trabalho mais pesadas requerem mais de os requisitos mínimos. Recursos avançados, como deduplicação de dados e replicação de nó, podem requerer mais do que a memória mínima especificada no documento de requisitos do sistema. Se você planeja executar diversas instâncias, cada instância requer a memória que é listada para um servidor. Multiplique a memória para um servidor pelo número de instâncias planejadas para o sistema.
Separe o banco de dados do servidor, o log ativo, o log de archive e os conjuntos de armazenamentos em disco uns dos outros.	Mantenha todos os recursos de armazenamento do IBM Spectrum Protect em discos separados. Mantenha os discos do conjunto de armazenamentos separados dos discos para o banco de dados e os logs do servidor. As operações do conjunto de armazenamentos podem interferir com as operações de banco de dados quando ambos estiverem nos mesmos discos. Idealmente, o banco de dados e os logs do servidor também são separados um do outro. Para obter detalhes e mais dicas, consulte os tópicos a seguir: – "Planejando os discos de banco de dados do servidor" – "Planejando os discos de log de recuperação do servidor" – "Planejamento para conjuntos de armazenamentos em classes de dispositivo DISK ou FILE"
Use pelo menos quatro diretórios para o banco de dados do servidor. Para servidores maiores ou servidores que usem recursos avançados, use oito diretórios.	Coloque cada diretório em uma LUN que esteja isolada das outras LUNs e de outros aplicativos. Um servidor é considerado grande quando seu banco de dados é maior do que o 2 TB ou é esperado que ele aumente até esse tamanho. Use oito diretórios para esses servidores. Consulte "Planejando os discos de banco de dados do servidor."

Melhor Prática	Mais Informações
Se você estiver usando deduplicação de dados, replicação de nó ou ambos, siga as diretrizes para a configuração do banco de dados e outros itens.	Configure o banco de dados do servidor de acordo com as diretrizes, porque o banco de dados tem extrema importância no bom funcionamento do servidor quando esses recursos estão sendo usados. Para obter detalhes e mais dicas, consulte os tópicos a seguir: – Lista de verificação para deduplicação de dados – Lista de Verificação para Replicação de Nó
Para os conjuntos de armazenamentos que usam classes de dispositivos de tipo FILE, siga as diretrizes para o tamanho dos volumes do conjunto de armazenamentos. Geralmente, os volumes do 50 GB são melhores.	Revise as informações em Número e Tamanho Ideais para Volumes para Conjuntos de Armazenamentos que Usam Disco para ajudá-lo a determinar o tamanho do volume. Configure os dispositivos de conjunto de armazenamentos e sistemas de arquivos com base nos requisitos de rendimento, não apenas nos requisitos de capacidade. Isole os dispositivos de armazenamento usados pelo IBM Spectrum Protect de outros aplicativos que possuem E/S alta e assegure-se de que haja rendimento suficiente para esse armazenamento. Para obter mais detalhes, consulte Lista de verificação para conjuntos de armazenamentos em DISK ou FILE.
Planeje as operações do cliente IBM Spectrum Protect e as atividades de manutenção do servidor para evitar ou minimizar a sobreposição das operações.	Para obter mais detalhes, consulte os seguintes tópicos: – Ajustando o planejamento para operações diárias – Lista de Verificação da Configuração do Servidor
Monitore as operações constantemente.	Ao monitorar, é possível localizar problemas antecipadamente e identificar as causas com mais facilidade. Mantenha os registros dos relatórios de monitoramento por até um ano para ajudar a identificar tendências e planejar o crescimento. Consulte Monitorando e Mantendo o Ambiente para Desempenho.

Requisitos mínimos do sistema para o servidor IBM Spectrum Protect

Antes de instalar um servidor IBM Spectrum Protect em um sistema operacional AIX, revise os requisitos de hardware e de software.

Requisitos de Hardware e Software para a Instalação de Servidor IBM Spectrum Protect

O ambiente ideal do IBM Spectrum Protect é configurado com a deduplicação de dados usando os Blueprints do IBM Spectrum Protect.

Para obter as informações mais atuais sobre os requisitos do sistema do IBM Spectrum Protect, veja nota técnica 1243309.

Requisitos de Hardware

A Tabela 1 descreve os requisitos mínimos de hardware que são necessários para um servidor em um sistema AIX. Se o servidor não atender aos requisitos mínimos, a instalação falhará. Para obter mais detalhes sobre como planejar o espaço em disco, consulte “Planejamento de Capacidade” na página 53.

Tabela 6. Requisitos de Hardware	
Tipo de hardware	**Requisitos de Hardware**
Geral	Para ambientes somente de disco, use qualquer hardware fornecido e configurado apropriadamente no qual é possível executar um sistema operacional que seja suportado para este produto e liberação. Para ambientes que usam outros tipos de armazenamento, como fita, entre em contato com o seu fornecedor de dispositivo para requisitos de suporte.
Process.	IBM Spectrum Protect requer um processador POWER7 ou mais recente.
Espaço em disco	Os valores mínimos a seguir para o espaço em disco: • 7.5 GB para o diretório de instalação • 4 GB para o diretório `/tmp` • 2,5 GB para o diretório `/var` • 128 MB no diretório inicial para o usuário raiz • 2 GB para a área de recurso compartilhado No caso de um problema surgir e ser necessário qualquer diagnóstico, o ideal será ter um espaço temporário ou outro disponível no sistema para um log de primeira captura de dados com falha (FFDC) ou para outros usos temporários, como para coletar logs de rastreio. Espaço em disco adicional significativo é necessário para o banco de dados e os arquivos de log. O tamanho do banco de dados depende do número dos arquivos de cliente a serem armazenados e do método pelo qual o servidor gerencia os mesmos. O espaço no log ativo padrão é 16 GB, o mínimo necessário para a maioria das cargas de trabalho e das configurações. Ao criar o log ativo, são necessários pelo menos 64 GB para executar a replicação. Se a replicação e a deduplicação de dados estiverem sendo usadas, crie um log ativo de 128 GB de tamanho. Aloque pelo menos três vezes o espaço de log ativo padrão para o log de archive (48 GB). Assegure-se de que tenha recursos suficientes se estiver usando deduplicação de dados ou espera uma carga de trabalho pesada do cliente. Para conseguir o desempenho ideal e facilitar a E/S, especifique pelo menos dois contêineres de tamanho igual ou Números da Unidade Lógica (LUNs) para o banco de dados. Além disso, cada log ativo e log de archive precisa de seu próprio contêiner ou LUN. Assegure-se de consultar “Planejamento de Capacidade” na página 53 para obter mais detalhes sobre espaço em disco.
Memória	A seguir estão os requisitos mínimos de memória do sistema para servidores com bancos de dados de até 500 GB, com a ingestão diária de até 200 GB por dia: • 16 GB para operações do servidor padrão sem deduplicação de dados e replicação de nó • 24 GB para deduplicação de dados ou replicação de nó • 32 GB para replicação de nó com deduplicação de dados Para obter requisitos de memória mais específicos para bancos de dados maiores e capacidades de ingestão mais altas, consulte a tabela de ajuste de memória do servidor IBM Spectrum Protect. Para requisitos mais específicos de memória quando você estiver usando a deduplicação de dados, consulte o IBM Spectrum Protect Blueprint para seu sistema operacional.

Requisitos de Software

Tabela 7 na página 49 descreve os requisitos mínimos de software necessários para um servidor em um sistema AIX.

Tabela 7. Requisitos de Software

Tipo de Software	**Requisitos Mínimos de Software**
Sistema operacional	AIX 7.1 • AIX 7.1 TL5 e SP5 ou mais recente. • Nível mínimo de tempo de execução de C++ com os conjuntos de arquivos xlC.rte 13.1 ou mais recente. O conjunto de arquivos será submetido a upgrade automaticamente se o nível for anterior a 13.1. O conjunto de arquivos está incluído no pacote de fix pack de março de 2016 do IBM C++ Runtime Environment Components for AIX. AIX 7.2 • AIX 7.2 TL3 e SP3 ou mais recente. • Nível mínimo de tempo de execução C++ com conjuntos de arquivos xlC.rte 13.1.3.1 ou mais recentes. O conjunto de arquivos será automaticamente atualizado se o nível for anterior a 13.1.3.1. • Consulte a nota técnica 6430303 Para obter as recomendações mais recentes sobre os níveis de manutenção do AIX, consulte a nota técnica 21165448
Protocolo de comunicação	Um método de comunicação configurado.
Processamento	E/S assíncronas devem estar ativadas.
Drivers de Dispositivo	O driver de dispositivo do IBM Spectrum Protect é requerido para unidades não IBM e bibliotecas de fitas. O pacote do driver de dispositivo IBM Spectrum Protect contém as ferramentas do driver de dispositivo e daemons ACSLS. Para a biblioteca de fitas ou unidades IBM 3590, 3592 ou Ultrium, os drivers de dispositivo IBM são necessários. Instale os drivers de dispositivo mais atuais. É possível localizar pacotes de drivers IBM no Fix Central. Configure os drivers de dispositivo antes de usar o servidor IBM Spectrum Protect com os dispositivos de fita.
Utilitário Gunzip	O utilitário gunzip deve estar disponível em seu sistema antes que você instale ou faça upgrade do servidor. Certifique-se de que o utilitário gunzip esteja instalado e o caminho para ele esteja configurado na variável de ambiente PATH.
Outro software	• Shell Korn (ksh) • Para autenticar os usuários do IBM Spectrum Protect com um servidor Lightweight Directory Access Protocol (LDAP), deve-se usar um dos servidores de diretório a seguir: – Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2, Windows Server 2016) – IBM Security Directory Server V6.3 – IBM Security Directory Server V6.4

Compatibilidade do servidor IBM Spectrum Protect com outros produtos IBM Db2 no sistema

É possível instalar outros produtos que implementam e usam os produtos do Db2 no mesmo sistema que o servidor do IBM Spectrum Protect, com algumas limitações.

Para instalar e usar outros produtos que usam um produto Db2 no mesmo sistema que o servidor IBM Spectrum Protect, assegure-se de que os critérios a seguir sejam atendidos:

Tabela 8. Compatibilidade do servidor IBM Spectrum Protect com outros produtos Db2 no sistema

Critério	**Instruções**
Nível da versão	Os outros produtos que usam um produto Db2 devem usar o Db2 Versão 9 ou mais recente. Os produtos Db2 incluem suporte de encapsulação e segregação do produto iniciando com a Versão 9. A partir dessa versão, é possível executar múltiplas cópias de produtos Db2, em diferentes níveis de código, no mesmo sistema. Para obter detalhes, veja as informações sobre múltiplas cópias no Informações do produto DB2.
IDs do usuário e diretórios	Assegure-se de que os IDs de usuário, IDs de usuário protegido, local de instalação, outros diretórios e informações relacionadas não sejam compartilhados nas instalações do Db2. Suas especificações devem ser diferentes dos IDs e locais que você usou para a instalação e configuração do servidor IBM Spectrum Protect. Se você usou o assistente **dsmicfgx** para configurar o servidor, esses são os valores que você inseriu ao executar o assistente. Se você usou o método de configuração manual, revise os procedimentos usados, se necessário, para rechamar os valores que foram usados para o servidor.

Tabela 8. Compatibilidade do servidor IBM Spectrum Protect com outros produtos Db2 no sistema (continuação)

Critério	Instruções
Alocação de recurso	Considere os recursos e a capacidade do sistema comparados com os requisitos para o servidor IBM Spectrum Protect e os outros aplicativos que usam o produto Db2. Para fornecer recursos suficientes para os outros aplicativos do Db2, talvez você tenha que mudar as configurações do servidor IBM Spectrum Protect para que o servidor use menos memória e recursos do sistema. Da mesma forma, se as cargas de trabalho para os outros aplicativos do Db2 competirem com o servidor IBM Spectrum Protect pelos recursos do processador ou da memória, o desempenho do servidor ao manipular a carga de trabalho do cliente esperada ou outras operações do servidor poderão ser afetados de forma adversa. Para segregar recursos e fornecer mais recursos para o ajuste e alocação do processador, memória e outros recursos do sistema para diversos aplicativos, considere usar a partição lógica (LPAR), partição de carga de trabalho (WPAR) ou outro suporte de estação de trabalho virtual. Por exemplo, execute um aplicativo do Db2 em seu próprio sistema virtualizado.

IBM Installation Manager

O IBM Spectrum Protect usa o IBM Installation Manager, que é um programa de instalação que pode usar repositórios de software remotos ou locais para instalar ou atualizar muitos produtos IBM.

Se a versão necessária do IBM Installation Manager ainda não estiver instalada, ela será instalada ou atualizada automaticamente durante a instalação do IBM Spectrum Protect. Ela deve permanecer instalada no sistema para que o IBM Spectrum Protect possa ser atualizado ou desinstalado posteriormente conforme necessário.

A lista a seguir contém explicações de alguns termos que são usados no IBM Installation Manager:

Oferta
Uma unidade instalável de um produto do software.

A oferta IBM Spectrum Protect contém toda a mídia que o IBM Installation Manager requer para instalar o IBM Spectrum Protect.

Pacote
O grupo de componentes de software que são necessários para instalar uma oferta.

O pacote IBM Spectrum Protect contém os componentes a seguir:

- Programa de instalação do IBM Installation Manager
- Oferta IBM Spectrum Protect

Grupo de pacotes
Um conjunto de pacotes que compartilham um diretório-pai comum.

O grupo de pacotes padrão para o pacote do IBM Spectrum Protect é `IBM Installation Manager`.

Repositório
Uma área de armazenamento remota ou local para dados e outros recursos do aplicativo.

O pacote do IBM Spectrum Protect está armazenado em um repositório no IBM Fix Central.

Diretório de recursos compartilhados
Um diretório que contém arquivos de software ou plug-ins que são compartilhados por pacotes.

O IBM Installation Manager armazena arquivos relacionados à instalação no diretório de recursos compartilhados, incluindo arquivos que são usados para retroceder para uma versão anterior do IBM Spectrum Protect.

Planilhas para planejar detalhes para o servidor

É possível usar as planilhas para ajudá-lo a planejar a quantidade e o local do armazenamento necessário para o servidor IBM Spectrum Protect. Também é possível usá-las para controlar os nomes e IDs do usuário.

Item	Espaço necessário	Número de diretórios	Local de diretórios
O banco de dados			
Log ativo			
Log de archive			
Opcional: Espelho de log para o log ativo			
Opcional: Log de archive secundário (local de failover para o log de archive)			

Item	Nomes e IDs do usuário	Local
O *ID do usuário da instância* para o servidor, que é o ID utilizado para iniciar e executar o servidor IBM Spectrum Protect		
O *diretório inicial* para o servidor, que é o diretório que contém o ID do usuário da instância		

Item	Nomes e IDs do usuário	Local
O nome da instância de banco de dados		
O *diretório de instâncias* para o servidor, que é um diretório que contém arquivos especificamente para essa instância do servidor (o arquivo de opções do servidor e outros arquivos específicos do servidor)		
O nome do servidor, use um nome exclusivo para cada servidor		

Planejamento de Capacidade

O planejamento da capacidade para IBM Spectrum Protect inclui o gerenciamento de recursos como o banco de dados, o log de recuperação e a área do recurso compartilhado.

Antes de Iniciar

Para maximizar os recursos como parte do planejamento de capacidade, você deverá estimar os requisitos de espaço para o banco de dados e o log de recuperação. A área de recurso compartilhado deve ter espaço suficiente disponível para cada instalação ou upgrade.

Estimando os Requisitos de Espaço para o Banco de Dados

Para estimar os requisitos de espaço para o banco de dados, é possível usar o número máximo de arquivos que podem estar no armazenamento do servidor ao mesmo tempo, ou é possível usar a capacidade do conjunto de armazenamentos.

Sobre Esta Tarefa

Considere utilizar pelo menos 25 GB para o espaço inicial do banco de dados. Forneça espaço no sistema de arquivos adequadamente. Um tamanho de banco de dados de 25 GB é adequado para um ambiente de teste ou um ambiente de gerenciador de bibliotecas somente. Para um servidor de produção suportando cargas de trabalho do cliente, espera-se que o tamanho do banco de dados seja maior. Se você usar os conjuntos de armazenamentos do disco de acesso aleatório (DISK), mais banco de dados e espaço de armazenamento é necessário para conjuntos de armazenamento de acesso sequencial.

O tamanho máximo do banco de dados do IBM Spectrum Protect é 8 TB.

Para obter informações sobre dimensionamento do banco de dados em um ambiente de produção com base no número de arquivos e no tamanho do conjunto de armazenamento, consulte os seguintes tópicos.

Estimando os requisitos de espaço do banco de dados com base no número de arquivos

Se você puder estimar o número máximo de arquivos que podem estar em armazenamento no servidor em dado momento, será possível usar esse número para estimar os requisitos de espaço para o banco de dados.

Sobre Esta Tarefa

Para estimar os requisitos de espaço com base no número máximo de arquivos no armazenamento do servidor, use as seguintes diretrizes:

- 600 - 1000 bytes para cada versão armazenada de um arquivo, incluindo backups de imagem.

  Restrição: A diretriz não inclui espaço que é usado durante a deduplicação de dados.
- 100 - 200 bytes para cada arquivo em cache, arquivo do conjunto de armazenamentos de cópias, arquivo de conjunto de dados ativos e arquivo deduplicado.
- O espaço adicional é necessário para a otimização do banco de dados para suportar padrões de acesso a dados variáveis e para suportar o processamento de backend do servidor dos dados. A quantia de espaço extra é igual a 50% da estimativa para o número total de bytes para os objetos de arquivo.

No exemplo a seguir para um único cliente, os cálculos são baseados nos valores máximos das diretrizes anteriores. Os exemplos não levam em consideração que você pode usar a agregação de arquivo. Em geral, ao agregar pequenos arquivos, isso reduz a quantia de espaço de banco de dados necessária. A agregação de arquivos não afeta os arquivos gerenciados por espaço.

Procedimento

1. Calcule o número de versões do arquivo. Inclua cada um dos valores a seguir para obter o número de versões do arquivo:
   a) Calcule o número de arquivos de backup.
   Por exemplo, até 500.000 arquivos de cliente podem ter o backup feito por vez. Neste exemplo, as políticas de armazenamento são configuradas para manter até três cópias de arquivos com backup feito:

   ```
   500.000 arquivos * 3 cópias = 1.500.000 arquivos
   ```

   b) Calcule o número de arquivos no archive.
   Por exemplo, até 100.000 arquivos de cliente podem ser cópias de archive.

   c) Calcule o número de arquivos gerenciados por espaço.
   Por exemplo, até 200.000 arquivos de cliente podem ser migrados de estações de trabalho do cliente.

   Usando 1000 bytes por arquivo, a quantia total de espaço de banco de dados que é necessária para os arquivos que pertencem ao cliente é 1,8 GB:

   ```
   (1.500.000 + 100.000 + 200.000) * 1000 = 1,8 GB
   ```

2. Calcule o número de arquivos de cache, arquivos de conjunto de armazenamentos de cópia, arquivos de datapool ativo e arquivos deduplicados:
   a) Calcule o número de cópias em cache.
   Por exemplo, o armazenamento em cache está ativado em um conjunto de armazenamentos em disco de 5 GB. O alto limite de migração do conjunto é 90% e o limite baixo de migração do conjunto é 70%. Assim, 20% do conjunto de discos, ou 1 GB, é ocupado por arquivos em cache.

   Se o tamanho médio do arquivo é de aproximadamente 10 KB, aproximadamente 100.000 arquivos estão em cache em um dado momento:

   ```
   100.000 arquivos * 200 bytes = 19 MB
   ```

   b) Calcule o número de arquivos do conjunto de armazenamentos de cópias.
   Todos os conjuntos de armazenamentos primários têm seu backup feito para o conjunto de armazenamentos de cópia:

   ```
   (1.500.000 + 100.000 + 200.000) * 200 bytes = 343 MB
   ```

   c) Calcule o número de arquivos do conjunto de armazenamentos ativos.

Todos os dados ativos de backup do cliente nos conjuntos de armazenamentos primários são copiados para o conjunto de armazenamentos de dados ativos. Suponha que 500.000 versões dos 1.500.000 arquivos de backup do conjunto de armazenamento primário estejam ativas:

```
500.000 * 200 bytes = 95 MB
```

d) Calcule o número de arquivos deduplicados.
Suponha que um conjunto de armazenamentos deduplicados contenha 50.000 arquivos:

```
50.000 * 200 bytes = 10 MB
```

Com base nos cálculos anteriores, aproximadamente 0,5 GB de espaço de banco de dados extra será necessário para os arquivos em cache, arquivos do conjunto de armazenamentos de cópia, arquivos do datapool ativo e arquivos deduplicados do cliente.

3. Calcule a quantia de espaço extra necessária para a otimização do banco de dados.
Para fornecer acesso ideal a dados e gerenciamento pelo servidor, é necessário espaço de banco de dados extra. A quantia de espaço de banco de dados extra é igual a 50% dos requisitos de espaço total para objetos de arquivo.

```
(1,8 + 0,5) * 50% = 1,2 GB
```

4. Calcule a quantidade total de espaço do banco de dados que é requerido para o cliente. O total é aproximadamente 3,5 GB:

```
1,8 + 0,5 + 1,2 = 3,5 GB
```

5. Calcule a quantidade total de espaço do banco de dados que é requerido para todos os clientes.
Se o cliente que foi usado nos cálculos anteriores for típico e tiver 500 clientes, por exemplo, será possível usar o cálculo a seguir para estimar a quantia total de espaço de banco de dados que é necessária para todos os clientes:

```
500 * 3,5 = 1,7 TB
```

Resultados

Dica: Nos exemplos anteriores, os resultados são estimativas. O tamanho real do banco de dados pode diferir da estimativa devido a fatores, como o número de diretórios e o comprimento dos nomes do caminho e do arquivo. Periodicamente monitore seu banco de dados e ajuste seu tamanho conforme necessário.

O que Fazer Depois

Durante operações normais, o servidor IBM Spectrum Protect pode requerer espaço temporário do banco de dados. Esse espaço é necessário pelas seguintes razões:

- Para armazenar os resultados de classificação e ordenação que ainda não estão sendo guardados e otimizados no banco de dados diretamente. Os resultados são armazenados temporariamente no banco de dados para processamento.
- Par dar acesso administrativo ao banco de dados por um dos seguintes métodos:
  - Um cliente Open Database Connectivity (ODBC) do Db2
  - Um cliente Oracle Java Database Connectivity (JDBC)
  - Linguagem de Consulta Estruturada (SQL) para o servidor de uma linha de comandos do cliente administrativo

Considere usar 50 GB extra de espaço temporário para cada 500 GB de espaço para objetos de arquivo e otimização. Consulte as diretrizes na tabela a seguir. No exemplo que é usado na etapa anterior, um total de 1,7 TB de espaço de banco de dados é necessário para objetos de arquivo e otimização para 500 clientes. Com base nesse cálculo, 200 GB são requeridos para espaço temporário. A quantidade total de espaço requerido do banco de dados é de 1.9 TB.

Tamanho do banco de dados	Requisito de espaço temporário mínimo
< 500 GB	50 GB
≥ 500 GB e < 1 TB	100 GB
≥ 1 TB e < 1.5 TB	150 GB
≥ 1.5 e < 2 TB	200 GB
≥ 2 e < 3 TB	250 - 300 GB
≥ 3 e < 4 TB	350 - 400 GB

Estimando requisitos de espaço do banco de dados com base na capacidade do conjunto de armazenamentos

Para estimar os requisitos de espaço no banco de dados com base na capacidade do conjunto de armazenamentos, use uma proporção de 1 a 5%. Por exemplo, se você precisar de 200 TB de capacidade do conjunto de armazenamentos, espera-se que o tamanho de seu banco de dados seja de 2 a 10 TB. Como uma regra geral, torne seu banco de dados o maior possível para evitar falta de espaço. Se faltar espaço no banco de dados, as operações do servidor e as operações de armazenamento do cliente poderão falhar.

O Gerenciador de Banco de Dados e Espaço Temporário

O gerenciador de banco de dados do servidor IBM Spectrum Protect gerencia e aloca memória do sistema e espaço em disco para o banco de dados. A quantia de espaço de banco de dados que o sistema necessita depende da quantia de memória do sistema que está disponível e da carga de trabalho do servidor.

O gerenciador do banco de dados classifica dados em uma sequência específica, de acordo com a instrução SQL emitida para solicitar os dados. Dependendo da carga de trabalho no servidor, e se houver mais dados do que o gerenciador de banco de dados pode gerenciar, os dados (que são ordenadas em sequência) serão alocados para espaço em disco temporário. Os dados são alocados para espaço em disco temporário quando há um conjunto de resultados grande. O gerenciador do banco de dados gerencia dinamicamente a memória que é usada quando os dados são alocados para espaço em disco temporário.

Por exemplo, o processamento de expiração pode produzir um conjunto de resultados grande. Se não houver memória do sistema suficiente no banco de dados para armazenar o conjunto de resultados, alguns dos dados serão alocados para espaço em disco temporário. Durante o processamento de expiração, se um nó ou espaço no arquivo selecionado for muito grande para ser processado, o gerenciador de banco de dados não poderá classificar os dados na memória. O gerenciador de banco de dados deve usar o espaço temporário para classificar dados.

Para executar operações do banco de dados, considere incluir mais espaço de banco de dados para os seguintes cenários:

- O banco de dados tem uma pequena quantia de espaço e a operação do servidor que requer espaço temporário usa o espaço livre restante.
- Os espaços no arquivo são grandes ou os espaços no arquivo têm uma política designada que cria diversas versões de arquivo.
- O servidor IBM Spectrum Protect deve executar com memória limitada. O banco de dados utiliza a memória principal do servidor IBM Spectrum Protect para executar operações do banco de dados. No entanto, se houver memória insuficiente disponível, o servidor IBM Spectrum Protect aloca espaço temporário em disco para o banco de dados. Por exemplo, se 10 GB de memória estiver disponível e as operações do banco de dados requererem 12 GB de memória, o banco de dados utilizará espaço temporário.

- Um erro `sem espaço de banco de dados` é exibido quando você implementa um servidor IBM Spectrum Protect. Monitore o log de atividades do servidor para mensagens que são relacionadas ao espaço de banco de dados.

Importante: Não mude o software Db2 que é instalado com os pacotes de instalação e fix packs do IBM Spectrum Protect. Não instale ou faça upgrade para uma versão, liberação ou fix pack diferente do software Db2 para evitar danos ao banco de dados.

Requisitos de Espaço de Log de Recuperação

No IBM Spectrum Protect, o termo *log de recuperação* compreende o log ativo, o log de archive, o espelho do log ativo e o log de failover de archive. A quantia de espaço necessária para o log de recuperação depende de diversos fatores, incluindo, por exemplo, a quantia de atividade do cliente com o servidor.

Espaço de Log Ativo e de Archive

Ao estimar requisitos de espaço para logs ativos e de archive, inclua algum espaço extra para contingências, como cargas de trabalho pesadas ocasionais e failovers.

Em servidores IBM Spectrum Protect V7.1 e posterior, o log ativo pode ter um tamanho máximo de 512 GB. O tamanho do log de archive é limitado ao tamanho do sistema de arquivos no qual está instalado.

Utilize as seguintes diretrizes gerais ao estimar o tamanho do log ativo:

- O tamanho inicial sugerido para o log ativo é de 16 GB.
- Certifique-se de que o log ativo é pelo menos grande o suficiente para a quantidade de atividade simultânea que o servidor geralmente manipula. Como precaução, tente antecipar a maior quantia de trabalho que o servidor pode gerenciar por vez. Forneça espaço extra ao log ativo para que possa ser usado se necessário. Considere usar 20% de espaço extra.
- Monitore o espaço de log usado e ativo disponível. Ajuste o tamanho do log ativo se necessário, dependendo de fatores como atividade do cliente e o nível das operações do servidor.
- Certifique-se de que o diretório que armazena o log ativo seja tão grande ou maior que o tamanho do log ativo. Um diretório maior que o log ativo pode acomodar failovers, se ocorrerem.
- Certifique-se de que o sistema de arquivos que contém o diretório de log ativo tenha pelo menos 8 GB de espaço livre para os requisitos de movimento de log temporário.

O tamanho inicial sugerido para o log de archive é de 48 GB.

O diretório de log de archive deve ser grande o bastante para conter os arquivos de log que são gerados desde o backup completo anterior. Por exemplo, se você executar um backup completo do banco de dados todos os dias, o diretório de log do archive deverá ser grande o suficiente para conter os arquivos de log para toda a atividade do cliente que ocorrer durante 24 horas. Para recuperar espaço, o servidor exclui arquivos de log de archive obsoletos após um backup completo do banco de dados. Se o diretório de log de archive ficar cheio e um diretório para logs de failover de archive não existir, os arquivos de log permanecerão no diretório de log ativo. Essa condição pode fazer com que o diretório de log ativo fique cheio e pare o servidor. Quando o servidor reinicia, uma parte do espaço de log ativo existente é liberada.

Após o servidor ser instalado, é possível monitorar a utilização do log de archive e o espaço no diretório de log de archive. Se o espaço no diretório de log de archive for preenchido, isso pode causar os problemas a seguir:

- O servidor não pôde executar backups completos do banco de dados. Investigue e resolva este problema.
- Outros aplicativos gravam no diretório de log de archive, consumindo o espaço que é necessário pelo log de archive. Não compartilhe o espaço de log do archive com outros aplicativos que incluam outros servidores IBM Spectrum Protect. Certifique-se de que cada servidor tenha um local de armazenamento separado possuído e gerenciado por esse servidor específico.

Exemplo: Estimando tamanhos de log ativos e de archive para operações básicas de armazenamento de clientes

As operações básicas de armazenamento de clientes incluem backup, archive e gerenciamento de espaço. O espaço de log deve ser suficiente para manipular todas as transações de armazenamento que estiverem em andamento de uma só vez.

Para determinar os tamanhos dos logs ativos e de archive para operações básicas de armazenamento de clientes, use o seguinte cálculo:

```
número de clientes x arquivos armazenados
durante cada transação
  x  espaço de log necessário para cada arquivo
```

Esse cálculo é usado no exemplo da tabela a seguir.

Tabela 9. Operações básicas de armazenamento de clientes

Item	Valores de exemplo	Descrição
Número máximo de nós clientes que efetuam backup, archive ou migração de arquivos simultaneamente a qualquer momento	300	O número de nós clientes que fazem backup, archive ou migram arquivos toda noite.
Arquivos armazenados durante cada transação	4096	O valor padrão da opção do servidor TXNGROUPMAX é 4096.
O espaço de log requerido para cada arquivo	3053 bytes	O valor de 3053 bytes para cada arquivo em uma transação representa os bytes do log necessários ao efetuar backup de arquivos de um cliente do Windows em que os nomes do arquivo sejam de 12 - 120 bytes. Esse valor é baseado nos resultados de testes executados em condições de laboratório. Os testes consistiam em clientes de backup-archive executando operações de backup em um conjunto de armazenamento de disco de acesso aleatório (DISK). Conjuntos DISK resultam em mais uso do log que os conjuntos de armazenamentos de acesso sequencial. Considere um valor maior que 3053 bytes se os dados armazenados tiverem nomes de arquivos maiores que 12 - 120 bytes.

Log ativo: Tamanho sugerido	19.5 GB [1]	Use o cálculo a seguir para determinar o tamanho do log ativo. Um GB é igual a 1.073.741.824 bytes.
		`(300 clientes x 4096 arquivos armazenados durante cada transação x 3053 bytes para cada arquivo) ÷ 1.073.741.824 bytes = 3.5 GB`
		Aumente essa quantidade no tamanho inicial sugerido de 16 GB:
		`3.5 + 16 = 19.5 GB`

Tabela 9. Operações básicas de armazenamento de clientes (continuação)

Item	Valores de exemplo	Descrição

Log de archive: Tamanho sugerido	58.5 GB [1]	Devido ao requisito poder armazenar logs de archive em três ciclos de backup do banco de dados do servidor, multiplique a estimativa para o log ativo por 3 para estimar o requisito de log de archive total.
		`3.5 x 3 = 10.5 GB`
		Aumente essa quantidade no tamanho inicial sugerido de 48 GB:
		`10.5 + 48 = 58.5 GB`

[1] Os valores de exemplo desta tabela são usados para ilustrar como os tamanhos para os logs ativos e logs de archive são calculados. Em um ambiente de produção que não use deduplicação, 16 GB é o tamanho mínimo sugerido para um log ativo. O tamanho mínimo sugerido para um log de archive em um ambiente de produção que não use deduplicação é de 48 GB. Se você substituir os valores de seu ambiente e os resultados forem maiores que 16 GB e 48 GB, use seus resultados para dimensionar o log ativo e o log de archive.

Monitore seus logs e ajuste seu tamanho se necessário.

Exemplo: Estimando tamanhos de log ativos e de archive para clientes que usam diversas sessões

Se a opção do cliente RESOURCEUTILIZATION for configurada para um valor maior que o padrão, a carga de trabalho simultânea para o servidor aumentará.

Para determinar os tamanhos dos logs ativo e de archive quando os clientes usarem diversas sessões, use o seguinte cálculo:

```
número de clientes x sessões para cada cliente x arquivos
armazenados
  durante cada transação x espaço de log necessário para cada
arquivo
```

Esse cálculo é usado no exemplo da tabela a seguir.

Tabela 10. Diversas Sessões do Cliente

Item	Valores de exemplo		Descrição
Número máximo de nós clientes que efetuam backup, archive ou migração de arquivos simultaneamente a qualquer momento	300	1000	O número de nós clientes que fazem backup, archive ou migram arquivos toda noite.
Sessões possíveis para cada cliente	3	3	A configuração da opção do cliente RESOURCEUTILIZATION é maior que o padrão. Cada sessão do cliente executa um máximo de três sessões em paralelo.
Arquivos armazenados durante cada transação	4096	4096	O valor padrão da opção do servidor TXNGROUPMAX é 4096.

Tabela 10. Diversas Sessões do Cliente (continuação)			
Item	**Valores de exemplo**		**Descrição**
O espaço de log requerido para cada arquivo	3053	3053	O valor de 3053 bytes para cada arquivo de uma transação representa os bytes de log necessários ao realizar backup de arquivos de um cliente do Windows em que os nomes do arquivo têm 12 - 120 bytes. Esse valor é baseado nos resultados de testes executados em condições de laboratório. Os testes consistiam em clientes que estavam executando operações de backup para um conjunto de armazenamentos de disco de acesso aleatório (DISK). Conjuntos DISK resultam em mais uso do log que os conjuntos de armazenamentos de acesso sequencial. Considere um valor maior que 3053 bytes se os dados armazenados tiverem nomes de arquivos maiores que 12 - 120 bytes.

Log ativo: Tamanho sugerido	26.5 GB [1]	51 GB [1]	O seguinte cálculo foi usado para 300 clientes. Um GB é igual a 1.073.741.824 bytes.
			`(300 clientes x 3 sessões para cada cliente x 4096 arquivos armazenados durante cada transação x 3053 bytes para cada arquivo) ÷ 1.073.741.824 = 10.5 GB`
			Aumente essa quantidade no tamanho inicial sugerido de 16 GB:
			`10.5 + 16 = 26.5 GB`
			O seguinte cálculo foi usado para 1000 clientes. Um GB é igual a 1.073.741.824 bytes.
			`(1000 clientes x 3 sessões para cada cliente x 4096 armazenamentos de arquivos durante cada transação x 3053 bytes para cada arquivo) ÷ 1.073.741.824 = 35 GB`
			Aumente essa quantidade no tamanho inicial sugerido de 16 GB:
			`35 + 16 = 51 GB`

Log de archive: Tamanho sugerido	79.5 GB [1]	153 GB [1]	Devido ao requisito de poder armazenar logs de archive em três ciclos de backup do banco de dados do servidor, a estimativa para o log ativo é multiplicada por 3:
			`10.5 x 3 = 31.5 GB`
			`35 x 3 = 105 GB`
			Aumente essas quantidades no tamanho inicial sugerido de 48 GB:
			`31.5 + 48 = 79.5 GB`
			`105 + 48 = 153 GB`

Tabela 10. Diversas Sessões do Cliente (continuação)		
Item	**Valores de exemplo**	**Descrição**
[1] Os valores de exemplo desta tabela são usados para ilustrar como os tamanhos para os logs ativos e logs de archive são calculados. Em um ambiente de produção que não use deduplicação, 16 GB é o tamanho mínimo sugerido para um log ativo. O tamanho mínimo sugerido para um log de archive em um ambiente de produção que não use deduplicação é de 48 GB. Se você substituir os valores de seu ambiente e os resultados forem maiores que 16 GB e 48 GB, use seus resultados para dimensionar o log ativo e o log de archive. Monitore seu log ativo e ajuste seu tamanho se necessário.		

Exemplo: Estimando tamanhos de log ativos e de archive para operações simultâneas de gravação

Se as operações de backup do cliente usarem conjuntos de armazenamentos configurados para gravação simultânea, a quantidade de espaço de log requerida para cada arquivo aumenta.

O espaço de log requerido para cada arquivo aumenta aproximadamente 200 bytes para cada conjunto de armazenamentos de cópias que é usado para uma operação de gravação simultânea. No exemplo da tabela a seguir, os dados são armazenados em dois conjuntos de armazenamentos de cópias além de um conjunto de armazenamentos primário. O tamanho do log estimado aumenta em 400 bytes para cada arquivo. Se você usar o valor sugerido de 3053 bytes de espaço de log para cada arquivo, o número total de bytes requerido será de 3453.

Esse cálculo é usado no exemplo da tabela a seguir.

Tabela 11. Operações simultâneas de gravação		
Item	**Valores de exemplo**	**Descrição**
Número máximo de nós clientes que efetuam backup, archive ou migração de arquivos simultaneamente a qualquer momento	300	O número de nós clientes que fazem backup, archive ou migram arquivos toda noite.
Arquivos armazenados durante cada transação	4096	O valor padrão da opção do servidor TXNGROUPMAX é 4096.
O espaço de log requerido para cada arquivo	3453 bytes	3053 bytes mais 200 bytes para cada conjunto de armazenamentos de cópias. O valor de 3053 bytes para cada arquivo em uma transação representa os bytes do log necessários ao efetuar backup de arquivos de um cliente do Windows em que os nomes do arquivo sejam de 12 - 120 bytes. Esse valor é baseado nos resultados de testes executados em condições de laboratório. Os testes consistiam em clientes de backup-archive executando operações de backup em um conjunto de armazenamento de disco de acesso aleatório (DISK). Conjuntos DISK resultam em mais uso do log que os conjuntos de armazenamentos de acesso sequencial. Considere um valor maior que 3053 bytes se os dados armazenados tiverem nomes de arquivos maiores que 12 - 120 bytes.

Tabela 11. Operações simultâneas de gravação (continuação)

Item	Valores de exemplo	Descrição

Log ativo: Tamanho sugerido	20 GB [1]	Use o cálculo a seguir para determinar o tamanho do log ativo. Um GB é igual a 1.073.741.824 bytes.
		`(300 clientes x 4096 arquivos armazenados durante cada transação x 3453 bytes para cada arquivo) ÷ 1.073.741.824 bytes = 4.0 GB`
		Aumente essa quantidade no tamanho inicial sugerido de 16 GB:
		`4 + 16 = 20 GB`

Log de archive: Tamanho sugerido	60 GB [1]	Devido ao requisito poder armazenar logs de archive em três ciclos de backup do banco de dados do servidor, multiplique a estimativa para o log ativo por 3 para estimar o requisito de log de archive:
		`4 GB x 3 = 12 GB`
		Aumente essa quantidade no tamanho inicial sugerido de 48 GB:
		`12 + 48 = 60 GB`

[1] Os valores de exemplo desta tabela são usados para ilustrar como os tamanhos para os logs ativos e logs de archive são calculados. Em um ambiente de produção que não use deduplicação, 16 GB é o tamanho mínimo sugerido para um log ativo. O tamanho mínimo sugerido para um log de archive em um ambiente de produção que não use deduplicação é de 48 GB. Se você substituir os valores de seu ambiente e os resultados forem maiores que 16 GB e 48 GB, use seus resultados para dimensionar o log ativo e o log de archive.

Monitore seus logs e ajuste seu tamanho se necessário.

Exemplo: Estimando tamanhos de log ativos e de archive para operações básicas de armazenamento de clientes e operações do servidor

Migração de dados no armazenamento do servidor, processos de identificação para deduplicação de dados, reclamação e expiração podem ser executados simultaneamente com operações de armazenamento de clientes. Tarefas administrativas como comandos administrativos ou consultas SQL de clientes administrativos também podem ser executados simultaneamente com operações de armazenamento de clientes. Operações do servidor e tarefas administrativas que são executadas simultaneamente podem aumentar o espaço de log ativo requerido.

Por exemplo, a migração de arquivos do conjunto de armazenamentos de acesso aleatório (DISK) para um conjunto de armazenamentos de disco de acesso sequencial(FILE) usa aproximadamente 110 bytes de espaço de log para cada arquivo que é migrado. Por exemplo, suponha que você tenha 300 clientes de backup-archive e cada um deles faça backup de 100.000 arquivos cada noite. Os arquivos são inicialmente armazenados no DISK e, em seguida, migrados para um conjunto de armazenamentos FILE. Para estimar a quantidade de espaço de log ativo requerido para a migração de dados, use o seguinte cálculo. O número de clientes do cálculo representa o número máximo de nós clientes que realiza backup, archive ou migra arquivos simultaneamente a qualquer momento.

```
300 clientes x 100.000 arquivos para cada cliente
x 110 bytes = 3.1 GB
```

Inclua este valor na estimativa para o tamanho do log ativo calculado para operações básicas de armazenamento de clientes.

Exemplo: Estimando tamanhos de log ativos e de archive sob condições de extrema variação

Podem ocorrer problemas de esgotamento de espaço de log ativo se você tiver muitas transações concluídas rapidamente e algumas transações que levem muito tempo para serem concluídas. Um caso típico ocorre quando muitas sessões de backup do servidor de arquivos ou da estação de trabalho estão ativos e poucas sessões grandes de backup do servidor do banco de dados estão ativas. Se essa situação se aplicar a seu ambiente, talvez você precise aumentar o tamanho do log ativo para que o trabalho seja concluído com êxito.

Exemplo: Estimando tamanhos de log do archive com backups completos de banco de dados

O servidor IBM Spectrum Protect exclui arquivos desnecessários do log de archive somente quando ocorre um backup completo do banco de dados. Consequentemente, quando você estima o espaço requerido para o log de archive, você também deve considerar a frequência dos backups completos do banco de dados.

Por exemplo, se ocorrer um backup completo do banco de dados uma vez por semana, o espaço de log do archive deverá poder conter as informações no log de archive para uma semana inteira.

A diferença no tamanho de log de archive para backups diários e completos do banco de dados é exibido no exemplo da tabela a seguir.

Tabela 12. Backups Completos do Banco de Dados

Item	Valores de exemplo	Descrição
Número máximo de nós clientes que efetuam backup, archive ou migração de arquivos simultaneamente a qualquer momento	300	O número de nós clientes que fazem backup, archive ou migram arquivos toda noite.
Arquivos armazenados durante cada transação	4096	O valor padrão da opção do servidor TXNGROUPMAX é 4096.
O espaço de log requerido para cada arquivo	3453 bytes	3053 bytes para cada arquivo mais 200 bytes para cada conjunto de armazenamentos de cópia. O valor de 3053 bytes para cada arquivo de uma transação representa os bytes de log necessários ao realizar backup de arquivos de um cliente do Windows em que os nomes do arquivo têm 12 - 120 bytes. Esse valor é baseado nos resultados de testes executados em condições de laboratório. Os testes consistiam em clientes que estavam executando operações de backup para um conjunto de armazenamentos de disco de acesso aleatório (DISK). Conjuntos DISK resultam em mais uso do log que os conjuntos de armazenamentos de acesso sequencial. Considere um valor maior que 3053 bytes se os dados armazenados tiverem nomes de arquivos maiores que 12 - 120 bytes.

Tabela 12. Backups Completos do Banco de Dados (continuação)

Item	Valores de exemplo	Descrição

Log ativo: Tamanho sugerido	20 GB [1]	Use o cálculo a seguir para determinar o tamanho do log ativo. Um GB é igual a 1.073.741.824 bytes.
		`(300 clientes x 4096 arquivos por transação x 3453 bytes por arquivo) ÷ 1.073.741.824 bytes = 4.0 GB`
		Aumente essa quantidade no tamanho inicial sugerido de 16 GB:
		`4 + 16 = 20 GB`

Log de archive: Tamanho sugerido com um backup completo do banco de dados todos os dias	60 GB [1]	Devido ao requisito de poder armazenar logs de archive em três ciclos de backup, multiplique a estimativa para o log ativo por 3 para estimar o requisito de log de archive total:
		`4 GB x 3 = 12 GB`
		Aumente essa quantidade no tamanho inicial sugerido de 48 GB:
		`12 + 48 = 60 GB`

Log de archive: Tamanho sugerido com um banco de dados completo toda semana	132 GB [1]	Devido ao requisito poder armazenar logs de archive em três ciclos de backup do banco de dados do servidor, multiplique a estimativa para o log ativo por 3 para estimar o requisito de log de archive total. Multiplique o resultado pelo número de dias entre os backups completos do banco de dados:
		`(4 GB x 3 ) x 7 = 84 GB`
		Aumente essa quantidade no tamanho inicial sugerido de 48 GB:
		`84 + 48 = 132 GB`

[1] Os valores de exemplo desta tabela são usados para ilustrar como os tamanhos para os logs ativos e logs de archive são calculados. Em um ambiente de produção que não use deduplicação, 16 GB é o tamanho mínimo sugerido para um log ativo. O tamanho inicial sugerido para um log de archive em um ambiente de produção que não use deduplicação é de 48 GB. Se você substituir os valores de seu ambiente e os resultados forem maiores que 16 GB e 48 GB, use seus resultados para dimensionar o log ativo e o log de archive.

Monitore seus logs e ajuste seu tamanho se necessário.

Exemplo: Estimando tamanhos de logs ativos e de archive para operações de deduplicação de dados

Se você deduplicar dados, deverá considerar seus efeitos nos requisitos de espaço para logs ativos e de archive.

Os fatores a seguir afetam requisitos para o espaço de logs ativos e de archive:

A quantidade de dados deduplicados

O efeito da deduplicação de dados no log ativo e no espaço de log do archive dependem da porcentagem de dados elegíveis para deduplicação. Se a porcentagem de dados que pode ser deduplicada for relativamente alta, mais espaço de log será requerido.

O tamanho e o número de extensões

Aproximadamente 1.500 bytes de espaço de log ativo são requeridos para cada extensão identificada por um processo de identificação de deduplicações. Por exemplo, se 250.000 extensões forem identificadas por um processo de identificação de deduplicações, o tamanho estimado do log ativo será 358 MB:

```
250.000 extensões identificadas durante cada processo x 1.500 bytes
 para cada extensão = 358 MB
```

Considere o seguinte cenário. Trezentos clientes de backup-archive fazem backup de 100.000 arquivos a cada noite. Essa atividade cria uma carga de trabalho de 30.000.000 de arquivos. O tamanho médio de extensões de cada arquivo é dois. Assim, o número total de extensões é 60.000.000 e o requisito de espaço para o log de archive é de 84 GB:

```
60.000.000 de extensões x 1.500 bytes para cada extensão = 84 GB
```

Um processo de identificação de duplicações opera em agregados de arquivos. Um agregado consiste em arquivos que são armazenados em uma determinada transação, conforme especificado pela opção do servidor TXNGROUPMAX. Suponha que a opção do servidor TXNGROUPMAX seja configurada para o padrão 4096. Se o número médio de extensões para cada arquivo for dois, o número total de extensões em cada agregado será 8192 e o espaço requerido para o log ativo será de 12 MB:

```
8192 extensões em cada
agregado x 1500 bytes para cada extensão =
   12 MB
```

Sincronização e número de processos de identificação de deduplicações

A sincronização e o número de processos de identificação de deduplicações também afeta o tamanho do log ativo. Usando o tamanho de log ativo de 12 MB que foi calculado no exemplo anterior, o carregamento simultâneo no log ativo será de 120 MB se 10 processos de identificação de deduplicações estiverem em execução em paralelo:

```
12 MB para cada processo x 10 processos = 120 MB
```

Tamanho do arquivo

Arquivos grandes que são processados para identificação duplicada também podem afetar o tamanho do log ativo. Por exemplo, suponha que um cliente de backup-archive faça backup de uma imagem do sistema de arquivos de 80 GB. Esse objeto pode ter um número elevado de extensões duplicadas se, por exemplo, for feito backup, de forma incremental, dos arquivos incluídos na imagem do sistema de arquivos. Por exemplo, suponha que uma imagem do sistema de arquivos tenha 1,2 milhões de extensões duplicadas. Os 1,2 milhões de extensões deste arquivo grande representam uma única transação para um processo de identificação de deduplicações. O espaço total no log ativo que é requerido para este único objeto é de 1.7 GB:

```
1.200.000 de
extensões x 1.500 bytes para cada extensão = 1.7 GB
```

Se ocorrerem outros processos menores de identificação de deduplicação ao mesmo tempo que o processo de identificação de deduplicação para um único objeto grande, o log ativo talvez não tenha espaço suficiente. Por exemplo, suponha que o conjunto de armazenamentos esteja ativado para deduplicação. O conjunto de armazenamentos possui uma mistura de dados, incluindo muitos arquivos relativamente pequenos que vão de 10 KB a várias centenas de KB. O conjunto de armazenamentos também possui poucos objetos grandes que têm uma alta porcentagem de extensões duplicadas.

Para levar em conta não apenas os requisitos de espaço, mas também a sincronização e duração de transações simultâneas, aumente o tamanho estimado do log ativo em um fator de dois. Por exemplo, suponha que seus cálculos para os requisitos de espaço sejam de 25 GB (23.3 GB + 1.7 GB para deduplicação de um objeto grande). Se os processos de deduplicação estiverem em execução simultaneamente, o tamanho sugerido do log ativo será de 50 GB. O tamanho sugerido do log de archive é de 150 GB.

Os exemplos das tabelas a seguir mostram os cálculos para logs ativos e de archive. O exemplo da primeira tabela usa um tamanho médio de 700 KB para extensões. O exemplo na segunda tabela usa um tamanho médio de 256 KB. Como os exemplos mostram, o tamanho médio da extensão de deduplicação de 256 KB indica um tamanho estimado maior para o log ativo. Para minimizar ou evitar problemas operacionais para o servidor, use 256 KB para estimar o tamanho do log ativo em seu ambiente de produção.

Tabela 13. Tamanho médio da extensão de deduplicação de 700 KB

Item	**Valores de exemplo**		**Descrição**
Tamanho do maior objeto único para deduplicação	800 GB	4 TB	A granularidade de processamento para deduplicação está no nível do arquivo. Assim, o maior arquivo único para deduplicação representa a maior transação e um carregamento correspondentemente grande nos logs ativos e de archive.
Tamanho médio das extensões	700 KB	700 KB	Os algoritmos de deduplicação usam um método de bloqueio variável. Nem todas as extensões deduplicadas para um determinado arquivo são do mesmo tamanho, assim, esse cálculo presume um tamanho médio para as extensões.
Extensões para um determinado arquivo	1.198.372 bits	6.135.667 bits	Usando um tamanho de extensão médio (700 KB), esses cálculos representam o número total de extensões para um determinado objeto. O cálculo a seguir foi usado para um objeto de 800 GB: `(800 GB ÷ 700 KB) = 1.198.372 bits` O cálculo a seguir foi usado para um objeto de 4 TB: `(4 TB ÷ 700 KB) = 6,135,667 bits`
Log ativo: Tamanho sugerido requerido para a deduplicação de um único objeto grande durante um processo único de identificação de deduplicação	1.7 GB	8.6 GB	O espaço de log ativo estimado necessário para esta transação.

Tabela 13. Tamanho médio da extensão de deduplicação de 700 KB (continuação)

Item	Valores de exemplo		Descrição

Log ativo: Tamanho total sugerido	66 GB [1]	79.8 GB [1]	Após considerar outros aspectos da carga de trabalho no servidor além da deduplicação, multiplique a estimativa existente por um fator de dois. Nesses exemplos, o espaço de log ativo requerido para deduplicar um único objeto grande é considerado juntamente com estimativas anteriores para o tamanho de log ativo requerido.
			O cálculo a seguir foi usado para diversas transações e um objeto de 800 GB:
			`(23,3 GB + 1,7 GB) x 2 = 50 GB`
			Aumente essa quantidade no tamanho inicial sugerido de 16 GB:
			`50 + 16 = 66 GB`
			O cálculo a seguir foi usado para diversas transações e um objeto de 4 TB:
			`(23.3 GB + 8.6 GB) x 2 = 63.8 GB`
			Aumente essa quantidade no tamanho inicial sugerido de 16 GB:
			`63.8 + 16 = 79.8 GB`

Log de archive: Tamanho sugerido	198 GB [1]	239.4 GB [1]	Multiplique o tamanho estimado do log ativo por um fator de 3.
			O cálculo a seguir foi usado para diversas transações e um objeto de 800 GB:
			`50 GB x 3 = 150 GB`
			Aumente essa quantidade no tamanho inicial sugerido de 48 GB:
			`150 + 48 = 198 GB`
			O cálculo a seguir foi usado para diversas transações e um objeto de 4 TB:
			`63.8 GB x 3 = 191.4 GB`
			Aumente essa quantidade no tamanho inicial sugerido de 48 GB:
			`191.4 + 48 = 239.4 GB`

[1] Os valores de exemplo desta tabela são usados para ilustrar como os tamanhos para os logs ativos e logs de archive são calculados. Em um ambiente de produção que usa deduplicação, 32 GB é o tamanho mínimo sugerido para um log ativo. O tamanho mínimo sugerido para um log de archive em um ambiente de produção que usa deduplicação é de 96 GB. Se você substituir os valores de seu ambiente e os resultados forem maiores que 32 GB e 96 GB, use seus resultados para dimensionar o log ativo e o log de archive.

Monitore seus logs e ajuste seu tamanho se necessário.

Tabela 14. Tamanho médio da extensão de deduplicação de 256 KB

Item	**Valores de exemplo**		**Descrição**
Tamanho do maior objeto único para deduplicação	800 GB	4 TB	A granularidade de processamento para deduplicação está no nível do arquivo. Assim, o maior arquivo único para deduplicação representa a maior transação e um carregamento correspondentemente grande nos logs ativos e de archive.
Tamanho médio das extensões	256 KB	256 KB	Os algoritmos de deduplicação usam um método de bloqueio variável. Nem todas as extensões deduplicadas para um determinado arquivo são do mesmo tamanho, assim, esse cálculo presume um tamanho médio de extensão.

Extensões para um determinado arquivo	3.276.800 bits	16.777.216 bits	Usando o tamanho médio de extensão, esses cálculos representam o número total de extensões para um determinado objeto.
			O cálculo a seguir foi usado para diversas transações e um objeto de 800 GB:
			`(800 GB ÷ 256 KB) = 3.276.800 bits`
			O cálculo a seguir foi usado para diversas transações e um objeto de 4 TB:
			`(4 TB ÷ 256 KB) = 16.777.216 bits`

Log ativo: Tamanho sugerido requerido para a deduplicação de um único objeto grande durante um processo único de identificação de deduplicação	4.5 GB	23.4 GB	O tamanho estimado do espaço de log ativo que é requerido para essa transação.

Log ativo: Tamanho total sugerido	71.6 GB [1]	109.4 GB [1]	Após considerar outros aspectos da carga de trabalho no servidor além da deduplicação, multiplique a estimativa existente por um fator de 2. Nesses exemplos, o espaço de log ativo requerido para deduplicar um único objeto grande é considerado juntamente com estimativas anteriores para o tamanho de log ativo requerido.
			O cálculo a seguir foi usado para diversas transações e um objeto de 800 GB:
			`(23.3 GB + 4.5 GB) x 2 = 55.6 GB`
			Aumente essa quantidade no tamanho inicial sugerido de 16 GB:
			`55.6 + 16 = 71.6 GB`
			O cálculo a seguir foi usado para diversas transações e um objeto de 4 TB:
			`(23.3 GB + 23.4 GB) x 2 = 93.4 GB`
			Aumente essa quantidade no tamanho inicial sugerido de 16 GB:
			`93.4 + 16 = 109.4 GB`

Tabela 14. Tamanho médio da extensão de deduplicação de 256 KB (continuação)

Item	Valores de exemplo		Descrição

Log de archive: Tamanho sugerido	214.8 GB [1]	328.2 GB [1]	O tamanho estimado do log ativo multiplicado por um fator de 3.
			O cálculo a seguir foi usado para um objeto de 800 GB:
			`55.6 GB x 3 = 166.8 GB`
			Aumente essa quantidade no tamanho inicial sugerido de 48 GB:
			`166.8 + 48 = 214.8 GB`
			O cálculo a seguir foi usado para um objeto de 4 TB:
			`93.4 GB x 3 = 280.2 GB`
			Aumente essa quantidade no tamanho inicial sugerido de 48 GB:
			`280.2 + 48 = 328.2 GB`

[1] Os valores de exemplo desta tabela são usados para ilustrar como os tamanhos para os logs ativos e logs de archive são calculados. Em um ambiente de produção que usa deduplicação, 32 GB é o tamanho mínimo sugerido para um log ativo. O tamanho mínimo sugerido para um log de archive em um ambiente de produção que usa deduplicação é de 96 GB. Se você substituir os valores de seu ambiente e os resultados forem maiores que 32 GB e 96 GB, use seus resultados para dimensionar o log ativo e o log de archive.

Monitore seus logs e ajuste seu tamanho se necessário.

Espaço do Espelho de Log Ativo

O log ativo pode ser espelhado para que a cópia espelhada possa ser usada se os arquivos de log ativos não puderem ser lidos. Pode haver somente um espelho de log ativo.

A criação de um espelho de log é uma opção sugerida. Se você aumentar o tamanho do log ativo, o tamanho de espelho do log ativo será aumentado automaticamente. O espelhamento de log pode afetar o desempenho, devido à atividade duplicada de E/S requerida para manter o espelho. O espaço adicional que o espelho de log requer é outro fator a considerar ao decidir se um espelho de log deve ser criado.

Se o diretório de log do espelho ficar cheia, o servidor emitirá mensagens de erro para o log da atividade e para o `db2diag.log`. A atividade do servidor continua.

Espaço de Log de Failover do Archive

O log de archive de failover é usado pelo servidor se o diretório do log de archive ficar sem espaço.

Especificar um diretório de log de archive de failover pode evitar problemas que ocorrem se o log de archive ficar sem espaço. Se o diretório do log de archive e a unidade ou sistema de arquivos onde o diretório do log de archive de failover está localizado ficarem cheios, os dados permanecerão no diretório de log ativo. Essa condição pode fazer com que o log ativo fique cheio, o que causa a parada do servidor.

Monitorando a utilização de espaço para o banco de dados e os logs de recuperação

Para determinar a quantidade de espaço de log ativo usado e disponível, é necessário emitir o comando **QUERY LOG**. Para monitorar a utilização de espaço no banco de dados e nos logs de recuperação, também é possível verificar o log de atividade para as mensagens.

Log ativo

Se a quantidade de espaço de log ativo disponível for muito baixa, as seguintes mensagens serão exibidas no log de atividade:

ANR4531I: IC_AUTOBACKUP_LOG_USED_SINCE_LAST_BACKUP_TRIGGER

Essa mensagem é exibida quando o espaço de log ativo exceder o tamanho máximo especificado. O servidor IBM Spectrum Protect inicia um backup completo do banco de dados.

Para alterar o tamanho máximo de log, pare o servidor. Abra o arquivo `dsmserv.opt` e especifique um novo valor para a opçãoACTIVELOGSIZE. Quando tiver concluído, reinicie o servidor.

ANR0297I: IC_BACKUP_NEEDED_LOG_USED_SINCE_LAST_BACKUP

Essa mensagem é exibida quando o espaço de log ativo exceder o tamanho máximo especificado. Você deve fazer backup do banco de dados manualmente.

Para alterar o tamanho máximo de log, pare o servidor. Abra o arquivo `dsmserv.opt` e especifique um novo valor para a opçãoACTIVELOGSIZE. Quando tiver concluído, reinicie o servidor.

ANR4529I: IC_AUTOBACKUP_LOG_UTILIZATION_TRIGGER

A proporção de espaço de log ativo usado para o espaço de log ativo disponível excede o limite de utilização do log. Se pelo menos um backup completo do banco de dados tiver ocorrido, o servidor IBM Spectrum Protect iniciará um backup incremental do banco de dados. Caso contrário, o servidor iniciará um backup completo do banco de dados.

ANR0295I: IC_BACKUP_NEEDED_LOG_UTILIZATION

A proporção de espaço de log ativo usado para o espaço de log ativo disponível excede o limite de utilização do log. Você deve fazer backup do banco de dados manualmente.

Log de archive

Se a quantidade de espaço de log disponível do archive for muito baixa, a seguinte mensagem será exibida no log da atividade:

ANR0299I: IC_BACKUP_NEEDED_ARCHLOG_USED

A proporção de espaço usado de log de archive para o espaço de log de archive disponível excede o limite de utilização do log. O servidor IBM Spectrum Protect inicia um backup completo automático do banco de dados.

Banco de Dados

Se a quantidade de espaço disponível para as atividades do banco de dados for muito baixa, as seguintes mensagens serão exibidas no log de atividade:

ANR2992W: IC_LOG_FILE_SYSTEM_UTILIZATION_WARNING_2

O espaço usado do banco de dados excede o limite para utilização do espaço do banco de dados. Para aumentar o espaço para o banco de dados, use o comando **EXTEND DBSPACE**, o comando **EXTEND DBSPACE** ou o utilitário DSMSERV FORMAT com o parâmetro **DBDIR**.

ANR1546W: FILESYSTEM_DBPATH_LESS_1GB

O espaço disponível no diretório em que os arquivos do banco de dados do servidor estão localizados é menor que 1 GB.

Quando um servidor IBM Spectrum Protect é criado com o utilitário DSMSERV FORMAT ou com o assistente de configuração, um banco de dados do servidor e um log de recuperação também são criados. Além disso, os arquivos são criados para manter informações do banco de dados usadas pelo gerenciador do banco de dados. O caminho especificado nesta mensagem indica o local das informações do banco de dados usado pelo gerenciador do banco de dados. Se o espaço não estiver disponível no caminho, o servidor não poderá mais funcionar.

Você deve incluir espaço no sistema de arquivos ou disponibilizar espaço no sistema de arquivos ou disco.

Excluindo arquivos de retrocesso de instalação

É possível excluir certos arquivos de instalação que foram salvos durante o processo de instalação para liberar espaço no diretório de recurso compartilhado. Por exemplo, os arquivos que talvez tenham sido necessários para uma operação de retrocesso são os tipos de arquivos que você pode excluir.

Sobre Esta Tarefa

Para excluir os arquivos que não são mais necessários, use o assistente gráfico de instalação ou a linha de comandos no modo do console.

Excluindo arquivos de retrocesso de instalação usando um assistente gráfico

É possível excluir certos arquivos de instalação que foram salvos durante o processo de instalação, usando a interface com o usuário do IBM Installation Manager.

Procedimento

1. Abra o IBM Installation Manager.

   No diretório em que o IBM Installation Manager está instalado, acesse o subdiretório `eclipse` (por exemplo, `/opt/IBM/InstallationManager/eclipse`) e emita o comando a seguir para iniciar o IBM Installation Manager:

   ```
   ./IBMIM
   ```

2. Clique em **Arquivo** > **Preferências**.
3. Selecione **Arquivos para recuperação**.
4. Clique em **Excluir arquivos salvos** e clique em **OK**

Excluindo os arquivos de retrocesso de instalação usando a linha de comandos

É possível excluir certos arquivos de instalação que foram salvos durante o processo de instalação, usando a linha de comandos.

Procedimento

1. No diretório onde o IBM Installation Manager está instalado, acesse o seguinte subdiretório:

   ```
   eclipse/tools
   ```

   Por exemplo:

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```

2. No diretório `tools`, emita o comando a seguir para iniciar uma linha de comandos do IBM Installation Manager:

   ```
   ./imcl -c
   ```

3. Insira P para selecionar **Preferências**.
4. Insira 3 para selecionar **Arquivos para recuperação**.
5. Insira D para **Excluir** os **Arquivos para recuperação**.
6. Insira A para **Aplicar mudanças e retornar ao menu de preferências**.
7. Insira C para sair do **Menu de Preferência**.
8. Insira X para **Sair do Installation Manager**.

Boas Práticas de Nomenclatura do Servidor

Use estas descrições como referência ao instalar ou fazer upgrade de um servidor IBM Spectrum Protect.

ID do Usuário da Instância

O ID de usuário da instância é usado como a base para outros nomes relacionados à instância do servidor. O ID de usuário da instância também é chamado de proprietário da instância.

Por exemplo: tsminst1

O ID do usuário da instância é o ID do usuário que deve ter propriedade ou autoridade de acesso de leitura/gravação a todos os diretórios criados para o banco de dados e para o log de recuperação. A maneira padrão de executar o servidor é no ID do usuário da instância. Esse ID do usuário também deve ter acesso de leitura/gravação para os diretórios usados para quaisquer classes do dispositivo**FILE**.

Diretório inicial para o ID do usuário da instância

O diretório inicial pode ser criado ao criar o ID do usuário da instância, usando a opção (`-m`) para criar um diretório inicial se ainda não existir um. Dependendo das configurações locais, o diretório inicial pode ter a forma: `/home/`*`instance_user_ID`*

Por exemplo: `/home/tsminst1`

O diretório inicial é usado primariamente para conter o perfil para o ID do usuário e para as configurações de segurança.

Nome da Instância de Banco de Dados

O nome da instância de banco de dados deve ser igual ao ID de usuário da instância sob o qual a instância do servidor é executada.

Por exemplo: `tsminst1`

Diretório de Instâncias

O diretório da instância é um diretório que contém arquivos especificamente para uma instância do servidor (o arquivo de opções do servidor e outros arquivos específicos do servidor). Ele pode ter qualquer nome que você deseje. Para uma identificação mais fácil, use um nome que faça a correspondência do diretório com o nome da instância.

É possível criar o diretório de instâncias como um subdiretório do diretório inicial para o ID do usuário da instância. Por exemplo: `/home/`*`instance_user_ID`*`/`*`instance_user_ID`*

O exemplo a seguir coloca o diretório de instâncias no diretório inicial do ID de usuário tsminst1: `/home/tsminst1/tsminst1`

É possível também criar o diretório em outro local, por exemplo: `/tsmserver/tsminst1`

O diretório de instâncias armazena os seguintes arquivos para a instância do servidor:

- O arquivo de opções do servidor, `dsmserv.opt`
- O arquivo de banco de dados de chave do servidor, `cert.kdb` e os arquivos `.arm` (utilizados pelos clientes e outros servidores para importar os certificados Secure Sockets Layer do servidor)
- O arquivo de configuração do dispositivo, se a opção do servidor `DEVCONFIG` não especificar um nome completo
- O arquivo do histórico de volume, se a opção do servidor `VOLUMEHISTORY` não especificar um nome completo
- Volumes para conjuntos de armazenamentos **DEVTYPE**=**FILE**, se o diretório para a classe de dispositivo não estiver especificado integralmente ou não estiver completo
- Saídas de usuário
- Saída de rastreio (se não estiver completo)

Nome do Banco de Dados

O nome do banco de dados é sempre TSMDB1, para cada instância do servidor. Este nome não pode ser alterado.

Nome do Servidor

O nome do servidor é um nome interno para IBM Spectrum Protect e é usado para operações que envolvem comunicação entre vários servidores IBM Spectrum Protect. Exemplos incluem a comunicação servidor-para-servidor e o compartilhamento de bibliotecas.

O nome do servidor é usado também quando você inclui o servidor no Operations Center para que ele possa ser gerenciado usando essa interface. Use um nome exclusivo para cada servidor. Para uma fácil identificação no Operations Center (ou a partir de um comando **QUERY SERVER**), use um nome que reflita o local ou a finalidade do servidor. Não mude o nome de um servidor IBM Spectrum Protect após ser configurado como um hub ou um servidor spoke.

Se você usar o assistente, o nome padrão que é sugerido é o nome do host do sistema que você está usando. É possível usar um nome diferente que seja significativo em seu ambiente. Se você tiver mais de um servidor no sistema e usar o assistente, é possível usar o nome padrão para somente um dos servidores. Você deve inserir um nome exclusivo para cada servidor.

Por exemplo:

```
PAYROLL
SALES
```

Diretórios para Espaço de Banco de Dados e Log de Recuperação

Os diretórios podem ser nomeados de acordo com práticas locais. Para uma identificação mais fácil, considere o uso de nomes que façam a correspondência dos diretórios com a instância do servidor.

Por exemplo, para o log de archive:

```
/tsminst1_archlog
```

Diretórios de Instalação

Os diretórios de instalação para o servidor IBM Spectrum Protect incluem o servidor, o IBM Db2, o dispositivo, a linguagem e outros diretórios. Cada um contém vários diretórios adicionais.

(`/opt/tivoli/tsm/server/bin`) é o diretório padrão que contém o código do servidor e o licenciamento.

O produto Db2 que é instalado como parte da instalação do servidor IBM Spectrum Protect tem a estrutura de diretórios conforme documentado nas fontes de informações do Db2. Proteja esses diretórios e arquivos como você faz com os diretórios do servidor. O diretório padrão é `/opt/tivoli/tsm/db2`.

É possível usar inglês dos EUA, alemão, francês, italiano, espanhol, português do Brasil, coreano, japonês, chinês tradicional, chinês simplificado, chinês GBK, chinês Big5 e russo.

Capítulo 2. Instalando os Componentes do Servidor

Para instalar os componentes do servidor do IBM Spectrum Protect, é possível usar o assistente de instalação ou a linha de comandos em modo do console.

Sobre Esta Tarefa

Usando o software de instalação do IBM Spectrum Protect, é possível instalar os componentes a seguir:

- servidor

  Dica: O banco de dados (IBM Db2), o Global Security Kit (GSKit) e o IBM Java Runtime Environment (JRE) são instalados automaticamente quando você seleciona o componente do servidor.
- idiomas do servidor
- licença
- dispositivos
- IBM Spectrum Protect for SAN
- Operations Center

Permita aproximadamente 30 a 45 minutos para instalar um servidor, utilizando este guia.

Obtendo o Pacote de Instalação

É possível obter o pacote de instalação do IBM Spectrum Protect a partir de um site de download da IBM, como o Passport Advantage ou o IBM Fix Central.

Antes de Iniciar

Se você planeja fazer download dos arquivos, configure o limite do usuário do sistema para o tamanho máximo do arquivo como ilimitado, para assegurar que os arquivos possam ser transferidos por download corretamente:

1. Para consultar o valor do tamanho máximo do arquivo, emita o comando a seguir:

   ```
   ulimit -Hf
   ```
2. Se o limite do usuário do sistema para o tamanho máximo do arquivo não estiver configurado como ilimitado, altere-o para ilimitado seguindo as instruções na documentação para seu sistema operacional.

Procedimento

1. Faça download do arquivo do pacote apropriado a partir de um dos websites a seguir.
   - Faça download do pacote do servidor a partir de Passport Advantage ou de Fix Central.
   - Para as informações, atualizações e correções de manutenção mais recentes, acesse IBM Support Portal.
2. Se você fez download do pacote de um site de download da IBM, conclua as seguintes etapas:
   a. Verifique se você tem espaço suficiente para armazenar os arquivos de instalação quando eles forem extraídos do pacote do produto. Consulte o documento do download para conhecer os requisitos de espaço:
      - IBM Spectrum Protect nota técnica 588021
      - IBM Spectrum Protect Extended Edition nota técnica 588023
      - IBM Spectrum Protect for Data Retention nota técnica 588025

b. Faça download do arquivo de pacote para o diretório de sua opção. O caminho deve conter menos que 128 caracteres. Certifique-se de extrair os arquivos de instalação em um diretório vazio. Não extraia em um diretório que contenha arquivos extraídos anteriormente ou quaisquer outros arquivos.

c. Certifique-se de que a permissão executável esteja configurada para o pacote. Se necessário, altere as permissões de arquivo, emitindo o comando a seguir:

```
chmod a+x package_name.bin
```

d. Extraia o pacote emitindo o seguinte comando:

```
./package_name.bin
```

em que *package_name* é o nome do arquivo transferido por download, por exemplo:

```
8.1.x.000-IBM-SPSRV-AIX.bin
```

3. Assegure-se de que o seguinte comando esteja ativado para que os assistentes do IBM Spectrum Protect funcionem adequadamente:

```
lsuser
```

Por padrão, o comando está ativado.

4. Selecione um dos métodos a seguir de instalar o IBM Spectrum Protect:
   - “Instalando o IBM Spectrum Protect Usando o Assistente de Instalação” na página 76
   - “Instalando o IBM Spectrum Protect Usando o Modo do Console” na página 77
   - “Instalando o IBM Spectrum Protect no Modo Silencioso” na página 78
5. Após você instalar o IBM Spectrum Protect e antes de customizá-lo para o seu uso, acesse o IBM Support Portal. Clique em **Suporte e Downloads** e aplique todas as correções aplicáveis.

Instalando o IBM Spectrum Protect Usando o Assistente de Instalação

É possível instalar o servidor usando o assistente gráfico do IBM Installation Manager.

Antes de Iniciar

Execute as seguintes ações antes de iniciar a instalação:

- Se os seguintes arquivos RPM não estiverem instalados no sistema, será necessário instalá-los.

  Dica: Não é necessário instalar arquivos RPM se você usa o assistente de console.

  Para obter informações sobre como instalar arquivos GTK2, consulte o tópico da IBM, Instalando e configurando o GTK2 no IBM AIX.

```
atk-1.12.3-2.aix5.2.ppc.rpm
cairo-1.8.8-1.aix5.2.ppc.rpm
expat-2.0.1-1.aix5.2.ppc.rpm
fontconfig-2.4.2-1.aix5.2.ppc.rpm
freetype2-2.3.9-1.aix5.2.ppc.rpm
gettext-0.10.40-6.aix5.1.ppc.rpm
glib2-2.12.4-2.aix5.2.ppc.rpm
gtk2-2.10.6-4.aix5.2.ppc.rpm
libjpeg-6b-6.aix5.1.ppc.rpm
libpng-1.2.32-2.aix5.2.ppc.rpm
libtiff-3.8.2-1.aix5.2.ppc.rpm
pango-1.14.5-4.aix5.2.ppc.rpm
```

```
pixman-0.12.0-3.aix5.2.ppc.rpm
xcursor-1.1.7-3.aix5.2.ppc.rpm
xft-2.1.6-5.aix5.1.ppc.rpm
xrender-0.9.1-3.aix5.2.ppc.rpm
zlib-1.2.3-3.aix5.1.ppc.rpm
```

- Verifique se o sistema operacional está configurado para o idioma que você precisa. Por padrão, o idioma do sistema operacional é o idioma do assistente de instalação.

Procedimento

Instale o IBM Spectrum Protect usando este método:

Opção	Descrição
Instalando o software a partir de um pacote transferido por download:	a. Altere para o diretório no qual você fez download do pacote. b. Inicie o assistente de instalação emitindo o seguinte comando: `./install.sh`

O que Fazer Depois

- Se ocorrerem erros durante o processo de instalação, eles serão registrados nos arquivos de log que estão armazenados no diretório de logs do IBM Installation Manager.

  É possível visualizar arquivos de log de instalação clicando em **Arquivo** > **Visualizar Log** na ferramenta Installation Manager. Para coletar estes arquivos de log, clique em **Ajuda** > **Exportar Dados para Análise de Problemas** na ferramenta Installation Manager.
- Depois de instalar o servidor e os componentes e antes de customizá-los para seu uso, acesse IBM Support Portal. Clique em **Downloads (correções e PTFs)** e aplique as correções aplicáveis.
- Após você instalar um novo servidor, revise Capítulo 3, “Executando as Primeiras Etapas após a Instalação do IBM Spectrum Protect”, na página 83 para aprender sobre a configuração de seu servidor.

Instalando o IBM Spectrum Protect Usando o Modo do Console

É possível instalar o IBM Spectrum Protect usando a linha de comandos no modo do console.

Antes de Iniciar

Execute as seguintes ações antes de iniciar a instalação:

- Verifique se o sistema operacional está configurado para o idioma que você precisa. Por padrão, o idioma do sistema operacional é o idioma do assistente de instalação.

Procedimento

Instale o IBM Spectrum Protect usando este método:

Opção	Descrição
Instalando o software a partir de um pacote transferido por download:	a. Altere para o diretório no qual você fez download do pacote. b. Inicie o assistente de instalação no modo do console emitindo o seguinte comando: `./install.sh -c`

Opção	Descrição
	Opcional: Gere um arquivo de resposta como parte de uma instalação do modo do console. Conclua as opções de instalação do modo do console e no painel **Resumo**, especifique G para gerar as respostas.

O que Fazer Depois

- Se ocorrerem erros durante o processo de instalação, eles serão registrados nos arquivos de log que estão armazenados no diretório de logs do IBM Installation Manager, por exemplo:

  ```
  /var/ibm/InstallationManager/logs
  ```

- Depois de instalar o servidor e os componentes e antes de customizá-los para seu uso, acesse IBM Support Portal. Clique em **Downloads (correções e PTFs)** e aplique as correções aplicáveis.
- Após você instalar um novo servidor, revise Capítulo 3, “Executando as Primeiras Etapas após a Instalação do IBM Spectrum Protect”, na página 83 para aprender sobre a configuração de seu servidor.

Instalando o IBM Spectrum Protect no Modo Silencioso

É possível instalar ou fazer upgrade do servidor em modo silencioso. No modo silencioso, a instalação não envia as mensagens para um console, mas, em vez disso, armazena as mensagens e os erros nos arquivos de log.

Antes de Iniciar

Para fornecer entrada de dados ao usar o método de instalação silenciosa, é possível usar um arquivo de resposta. Os arquivos de resposta de amostra a seguir são fornecidos no diretório `input` em que o pacote de instalação é extraído:

`install_response_sample.xml`
Use este arquivo para instalar os componentes do IBM Spectrum Protect.

`update_response_sample.xml`
Use este arquivo para fazer upgrade dos componentes do IBM Spectrum Protect.

Esses arquivos contêm valores padrão que podem ajudar a evitar quaisquer avisos desnecessários. Para usar esses arquivos, siga as instruções fornecidas nos arquivos.

Se você quiser customizar um arquivo de resposta, é possível modificar as opções que estão no arquivo. Para obter informações sobre arquivos de resposta, acesse Arquivos de respostas.

Procedimento

1. Crie um arquivo de resposta.

   É possível modificar o arquivo de resposta de amostra ou criar seu próprio arquivo.
2. Se você instalar o servidor e o Operations Center em modo silencioso, crie uma senha para o armazenamento confiável do Operations Center no arquivo de resposta.

   Se você está usando o arquivo `install_response_sample.xml`, inclua a senha na linha a seguir do arquivo, em que *`mypassword`* representa a senha:

   ```
   <variable name='ssl.password' value='mypassword'/>
   ```

   Para obter mais informações sobre esta senha, consulte Lista de verificação de instalação

   Dica: Para fazer upgrade do Operations Center, a senha do armazenamento confiável não será necessária se você estiver usando o arquivo `update_response_sample.xml`.
3. Inicie a instalação silenciosa emitindo o comando a seguir a partir do diretório em que o pacote de instalação é extraído. O valor *response_file* representa o caminho do arquivo e o nome do arquivo:

- `./install.sh -s -input response_file -acceptLicense`

O que Fazer Depois

- Se ocorrerem erros durante o processo de instalação, eles serão registrados nos arquivos de log que estão armazenados no diretório de logs do IBM Installation Manager, por exemplo:

  ```
  /var/ibm/InstallationManager/logs
  ```

- Depois de instalar o servidor e os componentes e antes de customizá-los para seu uso, acesse IBM Support Portal. Clique em **Downloads (correções e PTFs)** e aplique as correções aplicáveis.
- Após você instalar um novo servidor, revise Capítulo 3, “Executando as Primeiras Etapas após a Instalação do IBM Spectrum Protect”, na página 83 para aprender sobre a configuração de seu servidor.

Instalando os Pacotes de Idioma do Servidor

Traduções para o servidor permitem que o servidor exiba mensagens e ajuda em idiomas que não o inglês dos EUA. As traduções também permitem o uso de convenções do código do idioma para horário, data e formatação de número.

Antes de Iniciar

Para obter instruções sobre como instalar pacotes de idiomas do agente de armazenamento, consulte Configuração de pacote de idiomas para agentes de armazenamento.

Códigos do Idioma da Linguagem do Servidor

Use a opção do pacote de idiomas padrão ou selecione outro pacote de idiomas para exibir as mensagens do servidor e a ajuda.

Este pacote de idiomas é instalado automaticamente para a seguinte opção de idioma padrão para mensagens e ajuda do servidor IBM Spectrum Protect:

- LANGUAGE en_US

Para idiomas ou códigos de idioma diferentes do padrão, instale o pacote de idioma que a instalação requeira.

É possível usar os idiomas que são mostrados:

Tabela 15. Idiomas do Servidor para o AIX

idioma	**Valor da opção LANGUAGE**
Chinês, Simplificado	zh_CN
Chinês, Simplificado (UTF-8)	ZH_CN
Chinês, Tradicional (Big5)	Zh_TW
Chinês, Tradicional (UTF-8)	ZH_TW
Chinês, Tradicional (euc_tw)	zh_TW
Inglês	en_US
Inglês (UTF-8)	EN_US
Francês	fr_FR
Francês (UTF-8)	FR_FR
Alemão	de_DE

Tabela 15. Idiomas do Servidor para o AIX (continuação)	
idioma	**Valor da opção LANGUAGE**
Alemão (UTF-8)	DE_DE
Italiano	it_IT
Italiano (UTF-8)	IT_IT
Japonês, EUC	ja_JP
Japonês, PC	Ja_JP
Japonês, UTF8	JA_JP
Coreano	ko_KR
Coreano (UTF-8)	KO_KR
Português, Brasileiro	pt_BR
Português do Brasil (UTF-8)	PT_BR
Russo	ru_RU
Russo (UTF-8)	RU_RU
Espanhol	es_ES
Espanhol (UTF-8)	ES_ES

Restrição: Para usuários Operations Center, alguns caracteres podem não ser corretamente exibidos se o navegador da web não usar o mesmo idioma que o servidor. Se este problema ocorrer, configure o navegador para usar o mesmo idioma que o servidor.

Configurando um Pacote de Idiomas

Após configurar um pacote de idiomas, as mensagens e a ajuda são mostradas no servidor em idiomas que não o inglês dos EUA. Os pacotes de instalação são fornecidos com o IBM Spectrum Protect.

Sobre Esta Tarefa

Para ativar suporte para um código de idioma específico, conclua uma das seguintes tarefas:

- Configure a opção LANGUAGE no arquivo de opções do servidor para o nome do código do idioma que você deseja usar. Por exemplo:

  Para usar o código do idioma `it_IT`, configure a opção LANGUAGE para `it_IT`. Consulte "Códigos do Idioma da Linguagem do Servidor" na página 79.
- Se você estiver iniciando o servidor em primeiro plano, configure a variável de ambiente LC_ALL para corresponder ao valor que é configurado no arquivo de opções do servidor. Por exemplo, para configurar a variável de ambiente para italiano, insira o seguinte valor:

```
export LC_ALL=it_IT
```

Se o código do idioma for inicializado com êxito, ele formata a data, a hora e o número para o servidor. Se o código de idioma não for inicializado com sucesso, o servidor usará os arquivos de mensagens em inglês dos EUA e o formato de data, hora e numérico.

Atualizando um Pacote de Idiomas

É possível modificar ou atualizar um pacote de idiomas usando o IBM Installation Manager.

Sobre Esta Tarefa

É possível instalar outro pacote de idiomas dentro da mesma instância do IBM Spectrum Protect.

- Use a função **Modificar** do IBM Installation Manager para instalar outro pacote de idiomas.
- Use a função **Atualizar** do IBM Installation Manager para atualizar para versões mais recentes dos pacotes de idiomas.

Dica: No IBM Installation Manager, o termo *atualizar* significa descobrir e instalar atualizações e correções para pacotes de software instalados. Nesse contexto, *atualizar* e *fazer upgrade* são sinônimos.

Capítulo 3. Executando as Primeiras Etapas após a Instalação do IBM Spectrum Protect

Após você instalar o IBM Spectrum Protect, prepare-se para a configuração. Usar o assistente de configuração é o método preferencial de configuração da instância do IBM Spectrum Protect.

Sobre Esta Tarefa

1. Crie os diretórios e o ID do usuário para a instância do servidor. Consulte a seção "Criando o ID do Usuário e os Diretórios para a Instância do Servidor" na página 83.
2. Configure uma instância do servidor. Selecione uma das seguintes opções:
   - Use o assistente de configuração, o método preferencial. Consulte "Configurando IBM Spectrum Protect usando o assistente de configuração" na página 85.
   - Configure manualmente a nova instância. Consulte a seção "Configurando a Instância do Servidor Manualmente" na página 86. Conclua as etapas a seguir durante uma configuração manual.
     a. Configure seus diretórios e crie a instância do IBM Spectrum Protect. Consulte a seção "Criando a Instância do Servidor" na página 86.
     b. Crie um novo arquivo de opções do servidor copiando o arquivo de amostras para configurar a comunicação entre o servidor e os clientes. Consulte a seção "Configurando Comunicações de Servidor e Cliente" na página 88.
     c. Emita o comando **DSMSERV FORMAT** para formatar o banco de dados. Consulte a seção "Formatando o Banco de Dados e o Log" na página 90.
     d. Configure o sistema para backup de banco de dados. Consulte a seção "Preparando o Gerenciador do Banco de Dados para o Backup de Banco de Dados" na página 92.
3. Configure opções para controlar quando a reorganização do banco de dados é executada. Consulte a seção "Configurando as Opções do Servidor para Manutenção do Banco de Dados do Servidor" na página 94.
4. Inicie a instância do servidor se ainda não estiver iniciada.

   Consulte a seção "Iniciando a Instância do Servidor" na página 95.
5. Registre sua licença. Consulte a seção "Registrando Licenças" na página 100.
6. Prepare seu sistema para backups de banco de dados. Consulte a seção "Preparando o servidor para operações de backup de banco de dados " na página 100.
7. Para facilitar a resolução de problemas em caso de problemas futuros, assegure-se de que haja espaço suficiente alocado para um core dump. Para obter mais informações, consulte a nota técnica 6357399.
8. Monitore o servidor. Consulte a seção "Monitorando o Servidor" na página 101.

Criando o ID do Usuário e os Diretórios para a Instância do Servidor

Crie o ID do usuário para a instância do servidor do IBM Spectrum Protect e crie os diretórios que a instância do servidor precisa para o banco de dados e logs de recuperação.

Antes de Iniciar

Revise as informações sobre o espaço de planejamento para o servidor antes de concluir esta tarefa. Consulte "Planilhas para planejar detalhes para o servidor" na página 52.

Procedimento

1. Crie o ID do usuário que possuirá a instância do servidor.

   Você usa este ID do usuário ao criar a instância do servidor em uma etapa posterior.

   Crie um ID do usuário e um grupo que serão o proprietário da instância do servidor.

   a. Os comandos a seguir podem ser executados a partir de um ID do usuário administrativo que irá configurar o usuário e o grupo. Criar o ID do usuário e o grupo no diretório inicial do usuário.

      Restrição: No ID do usuário, somente letras em minúsculas (a-z), números (0-9) e o caractere sublinhado (_) podem ser usados. O ID do usuário e o nome do grupo devem estar em conformidade com as seguintes regras:

      - O comprimento deve ser 8 caracteres ou menos.
      - Não podem iniciar com *ibm*, *sql*, *sys* ou numeral.
      - O ID do usuário e o nome do grupo não podem ser *user*, *admin*, *guest*, *public*, *local* ou qualquer palavra reservada de SQL.

      Por exemplo, crie o ID do usuário `tsminst1` no grupo `tsmsrvrs`. Os exemplos a seguir mostram como criar esse ID do usuário e grupo usando os comandos do sistema operacional.

      ```
      mkgroup id=1001 tsmsrvrs
      mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
      passwd tsminst1
      ```

      Restrição: O IBM Db2 não suporta autenticação direta do usuário do sistema operacional por meio de LDAP.

   b. Efetue logoff e, em seguida, efetue login em seu sistema. Altere para a conta do usuário que você acabou de criar. Use um programa de login interativo, como telnet, para que você solicite a senha e possa alterá-la se necessário.

2. Crie os diretórios requeridos pelo servidor.

Crie diretórios vazios para cada item na tabela e certifique-se de que os diretórios pertençam ao novo ID do usuário criado. Monte o armazenamento associado a cada diretório para o log ativo, log de archive e diretórios do banco de dados.		
Item	**Comandos de exemplo para criar os diretórios**	**Seus diretórios**
O *diretório de instâncias* para o servidor, que é um diretório que conterá arquivos especificamente para essa instância do servidor (o arquivo de opções do servidor e outros arquivos específicos do servidor)	`mkdir /tsminst1`	

Os diretórios do banco de dados	`mkdir /tsmdb001`
	`mkdir /tsmdb002`
	`mkdir /tsmdb003`
	`mkdir /tsmdb004`	

Diretório do log ativo	`mkdir /tsmlog`	
Diretório do log de archive	`mkdir /tsmarchlog`	

Crie diretórios vazios para cada item na tabela e certifique-se de que os diretórios pertençam ao novo ID do usuário criado. Monte o armazenamento associado a cada diretório para o log ativo, log de archive e diretórios do banco de dados. *(continuação)*		
Item	**Comandos de exemplo para criar os diretórios**	**Seus diretórios**
Opcional: O diretório para o espelho do log para o log ativo	`mkdir /tsmlogmirror`	
Opcional: Diretório do log de archive secundário (local de failover para o log de archive)	`mkdir /tsmarchlogfailover`	

Quando um servidor é criado inicialmente usando o utilitário **DSMSERV FORMAT** ou o assistente de configuração, um banco de dados do servidor e um log de recuperação são criados. Além disso, os arquivos são criados para conter informações do banco de dados usadas pelo gerenciador do banco de dados.

3. Efetue logoff no novo ID do usuário.

Configurando o Servidor IBM Spectrum Protect

Depois de instalar o servidor e preparar-se para a configuração, configure a instância do servidor.

Sobre Esta Tarefa

Configure uma instância do servidor IBM Spectrum Protect selecionando uma das opções a seguir:

- Use o assistente de configuração do IBM Spectrum Protect em seu sistema local. Consulte “Configurando IBM Spectrum Protect usando o assistente de configuração” na página 85.
- Configure manualmente a nova instância do IBM Spectrum Protect. Consulte “Configurando a Instância do Servidor Manualmente” na página 86. Conclua as seguintes etapas durante uma configuração manual.
  1. Configure os diretórios e crie a instância do IBM Spectrum Protect. Consulte “Criando a Instância do Servidor” na página 86.
  2. Crie um novo arquivo de opções do servidor copiando o arquivo de amostras para configurar a comunicação entre o servidor IBM Spectrum Protect e os clientes. Consulte a seção “Configurando Comunicações de Servidor e Cliente” na página 88 .
  3. Emita o comando DSMSERV FORMAT para formatar o banco de dados. Consulte “Formatando o Banco de Dados e o Log” na página 90.
  4. Configure o sistema para backup de banco de dados. Consulte “Preparando o Gerenciador do Banco de Dados para o Backup de Banco de Dados” na página 92.

Configurando IBM Spectrum Protect usando o assistente de configuração

O assistente oferece uma abordagem orientada para a configuração de um servidor. Usando a interface gráfica com o usuário (GUI), é possível evitar algumas etapas de configuração que são complexas quando executadas manualmente. Inicie o assistente no sistema em que instalou o programa do servidor IBM Spectrum Protect.

Antes de Iniciar

Antes de usar o assistente de configuração, você deve concluir todas as etapas anteriores para preparar-se para a configuração. Essas etapas incluem a instalação do IBM Spectrum Protect, a criação do banco de dados e dos diretórios de log e a criação dos diretórios e do ID do usuário para a instância do servidor.

Procedimento

1. Certifique-se de que os requisitos a seguir sejam atendidos:
   - O sistema em que você instalou o IBM Spectrum Protect deve ter o cliente X Window System. Você deve também estar executando um servidor X Window System em seu desktop.
   - O sistema deve ter o protocolo Shell Seguro (SSH) ativado. Certifique-se de que a porta esteja configurada para o valor padrão, 22, e que a porta não esteja bloqueada por um firewall. É necessário ativar a autenticação de senha no arquivo `sshd_config` no diretório `/etc/ssh/`. Além disso, certifique-se de que o serviço de daemon SSH tenha direitos de acesso para conectar-se ao sistema usando o valor `localhost`.
   - Você deve ser capaz de efetuar login no sistema com o ID do usuário que foi criado para a instância do servidor, usando o protocolo SSH. Ao usar o assistente, é necessário fornecer este ID do usuário e a senha para acessar esse sistema.
2. Inicie a versão local do assistente:

   Abra o programa `dsmicfgx` no diretório `/opt/tivoli/tsm/server/bin`. Este assistente pode ser executado apenas usando o ID do usuário raiz.

   Siga as instruções para concluir a configuração. O assistente pode ser interrompido e reiniciado, mas o servidor não estará operacional até que todo o processo de configuração esteja concluído.

Configurando a Instância do Servidor Manualmente

Após instalar o IBM Spectrum Protect, é possível configurar o IBM Spectrum Protect manualmente em vez de usar o assistente de configuração.

Criando a Instância do Servidor

Crie uma instância do IBM Spectrum Protect emitindo o comando **db2icrt**.

Sobre Esta Tarefa

Você pode ter uma ou mais instâncias do servidor em uma estação de trabalho.

Importante: Antes de executar o comando **db2icrt**, verifique os seguintes itens:

- O diretório inicial do usuário (`/home/tsminst1`) existe. Se não houver um diretório inicial, crie-o.

  O diretório de instâncias armazena os seguintes arquivos que são gerados pelo servidor IBM Spectrum Protect:

  – O arquivo de opções do servidor, `dsmserv.opt`
  – O arquivo de banco de dados de chave do servidor, `cert.kdb` e os arquivos `.arm` (utilizados pelos clientes e outros servidores para importar os certificados Secure Sockets Layer do servidor)
  – O arquivo de configuração do dispositivo, se a opção do servidor `DEVCONFIG` não especificar um nome completo
  – O arquivo do histórico de volume, se a opção do servidor `VOLUMEHISTORY` não especificar um nome completo
  – Volumes para conjuntos de armazenamentos **DEVTYPE**=**FILE**, se o diretório para a classe de dispositivo não estiver especificado integralmente ou não estiver completo
  – Saídas de usuário
  – Saída de rastreio (se não estiver completo)
- Uma cópia de backup dos seguintes arquivos deve ser salva em um local protegido e seguro:
  – Arquivos da chave mestra de criptografia (`dsmkeydb.*`)
  – Arquivos de certificado do servidor e de chave privada (`cert.*`)

- O usuário raiz e o ID do usuário da instância devem ter permissão de gravação para o arquivo de configuração de shell. O arquivo de configuração shell (por exemplo, `.profile`) existe no diretório inicial. Para obter mais informações, consulte o Informações do produto DB2. Procure por configurações de variável de ambiente do Linux® e UNIX.

1. Efetue login usando o ID do usuário raiz e crie uma instância do IBM Spectrum Protect. O nome da instância deve ter o mesmo nome que o usuário que possui a instância. Use o comando **db2icrt** e insira o comando em uma linha:

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   instance_name instance_name
   ```

   Por exemplo, se seu ID do usuário para essa instância for tsminst1, use o comando a seguir para criar a instância. Insira o comando em uma linha.

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   tsminst1 tsminst1
   ```

   Lembre-se: A partir deste ponto, use esse novo ID do usuário ao configurar o servidor IBM Spectrum Protect. Efetue logout do ID do usuário raiz e efetue login com o novo ID do usuário da instância.

2. Altere o diretório padrão para o banco de dados para que seja igual ao diretório de instâncias para o servidor. Se você tiver diversos servidores, efetue login sob o ID da instância para cada servidor. Emita este comando:

   ```
   db2 update dbm cfg using dftdbpath instance_directory
   ```

   Por exemplo, em que instance_directory é o ID do usuário da instância:

   ```
   db2 update dbm cfg using dftdbpath /tsminst1
   ```

3. Modifique o caminho da biblioteca para incluir bibliotecas que são necessárias para operações do servidor.

   Dica: Nos exemplos a seguir, aqui estão os diretórios:

   - *server_bin_directory* é um subdiretório do diretório de instalação do servidor. Por exemplo, `/opt/tivoli/tsm/server/bin`.
   - *instance_users_home_directory* é o diretório inicial do usuário da instância. Por exemplo, `/home/tsminst1`.

   .

   - Emita o seguinte comando em uma linha:

     ```
     export LIBPATH=server_bin_directory/dbbkapi:
     /usr/opt/ibm/gsk8_64/lib64:$LIBPATH
     ```

   - Deve-se atualizar um dos arquivos a seguir para configurar o caminho da biblioteca quando o IBM Db2 ou o servidor são iniciados. Atualize conforme o shell que o usuário da instância é configurado para usar.

     Shell Bash ou Korn:

     ```
     instance_users_home_directory/sqllib/userprofile
     ```

     Shell C:

     ```
     instance_users_home_directory/sqllib/usercshrc
     ```

   - Atualize conforme o shell que o usuário da instância é configurado para usar.

     Shell Bash ou Korn:

Inclua a seguinte entrada no arquivo *instance_users_home_directory*/sqllib/userprofile, em uma linha:

```
export LIBPATH=server_bin_directory/
dbbkapi:/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```

Shell C:

Inclua a entrada a seguir no arquivo *instance_users_home_directory*/sqllib/usercshrc em uma linha:

```
setenv LIBPATH server_bin_directory/dbbkapi:
/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```

Lembre-se: As seguintes entradas devem estar no caminho da biblioteca, precedendo quaisquer outras entradas no caminho da biblioteca:

- server_bin_directory/dbbkapi
- /usr/local/ibm/gsk8_64/lib64

4. Crie um novo arquivo de opções do servidor.

Configurando Comunicações de Servidor e Cliente

Um arquivo de opções do servidor dsmserv.opt.smp de amostra é criado durante a instalação do IBM Spectrum Protect no diretório /opt/tivoli/tsm/server/bin. Você deve configurar comunicações entre o servidor e os clientes, criando um novo arquivo de opções do servidor. Para fazer isso, copie o arquivo de amostra para o diretório para a instância do servidor.

Sobre Esta Tarefa

Assegure que você tenha um diretório de instância do servidor, por exemplo /tsminst1, e copie o arquivo de amostra neste diretório. Nomeie o arquivo como dsmserv.opt e edite as opções. Conclua essa configuração antes de inicializar o banco de dados do servidor. Cada entrada de exemplo ou padrão no exemplo do arquivo de opções é um comentário, uma linha que começa com um asterisco (*). As opções não fazem distinção entre maiúsculas e minúsculas e um ou mais espaços em branco são permitidos entre as palavras-chave e os valores.

Ao editar o arquivo de opções, siga estas orientações:

- Remova o asterisco do início da linha para ativar uma opção.
- Comece a inserir as opções em qualquer coluna.
- Digite apenas uma opção por linha e a opção deve estar apenas em uma linha.
- Se você fizer várias entradas para uma palavra-chave, o servidor IBM Spectrum Protect utilizará a última entrada.

Se você alterar o arquivo de opções do servidor, deverá reiniciar o servidor para que as mudanças sejam efetivadas.

Você pode especificar um ou mais dos seguintes métodos de comunicação:

- TCP/IP Versão 4 ou Versão 6
- Memória compartilhada
- Secure Sockets Layer (SSL)

  Dica: É possível autenticar senhas com o servidor de diretório LDAP, ou autenticar senhas com o servidor IBM Spectrum Protect. Senhas que são autenticadas com o servidor de diretório LDAP podem fornecer segurança do sistema aprimorada.

Configurando as Opções de TCP/IP

Selecione de um intervalo de opções de TCP/IP para o servidor IBM Spectrum Protect ou retenha o padrão.

Sobre Esta Tarefa

A seguir há um exemplo de uma lista de opções de TCP/IP que podem ser usadas para configurar seu sistema.

```
commmethod                  tcpip
  tcpport          1500
  tcpwindowsize    0
  tcpnodelay       yes
```

Dica: Você pode utilizar o TCP/IP Versão 4, Versão 6, ou ambos.

TCPPORT
O endereço da porta do servidor para comunicação TCP/IP e SSL. O valor padrão é 1500.

TCPWINDOWSIZE
Especifica o tamanho do buffer de TCP/IP usado ao enviar ou receber dados. O tamanho da janela usado em uma sessão é o menor dos tamanhos de janela do servidor e do cliente. Tamanhos de janela maiores usam memória adicional, mas pode melhorar o desempenho.

Você pode especificar um inteiro de 0 a 2048. Para usar o tamanho de janela padrão para o sistema operacional, especifique 0.

TCPNODELAY
Especifica se o servidor envia ou não mensagens pequenas ou permite que TCP/IP armazene as mensagens em buffer. Enviar mensagens pequenas pode melhorar o rendimento, mas aumenta o número de pacotes enviados pela rede. Especifique YES para enviar pequenas mensagens ou NO para deixá-las no buffer TCP/IP. O padrão é YES.

TCPADMINPORT
Especifica o número da porta na qual o driver de comunicação TCP/IP do servidor deve aguardar solicitações de comunicação ativadas por TCP/IP ou SSL diferentes de sessões do cliente. O padrão é o valor TCPPORT.

SSLTCPPORT
(Somente para SSL) Especifica o número da porta de Secure Sockets Layer (SSL) na qual o driver de comunicação TCP/IP do servidor aguarda pedidos para sessões ativadas por SSL para o cliente de backup da linha de comando e o cliente administrativo da linha de comandos.

SSLTCPADMINPORT
(Apenas SSL) Especifica o endereço de porta no qual o driver de comunicação TCP/IP do servidor aguarda solicitações para sessões ativadas por SSL para o cliente administrativo da linha de comandos.

Configurando as Opções da Memória Compartilhada

É possível usar comunicações de memória compartilhada entre clientes e servidores no mesmo sistema. Para usar memória compartilhada, o TCP/IP Versão 4 deve estar instalado no sistema.

Sobre Esta Tarefa

O exemplo a seguir mostra uma configuração de memória compartilhada:

```
commmethod      sharedmem
   shmport      1510
```

Nesse exemplo, o **SHMPORT** especifica o endereço de porta TCP/IP de um servidor quando usar memória compartilhada. Use a opção **SHMPORT** para especificar uma porta TCP/IP diferente. O endereço padrão da porta é 1510.

COMMMETHOD pode ser usado diversas vezes no arquivo de opções do servidor do IBM Spectrum Protect com um valor diferente todas as vezes. Por exemplo, o exemplo a seguir é possível:

```
commmethod        tcpip
commmethod sharedmem
```

O número máximo de sessões simultâneas de memória compartilhada baseia-se nos recursos disponíveis do sistema. Cada sessão de memória compartilhada utiliza uma região de memória compartilhada de até 4 MB e quatro filas de mensagens IPCS, dependendo do nível do cliente do IBM Spectrum Protect.

Se o servidor e o cliente não estiverem sendo executados no mesmo ID do usuário, o servidor deverá ser raiz. Isso impede erros de comunicação de memória compartilhada.

Configurando Opções do Secure Sockets Layer

É possível incluir mais proteção para seus dados e senhas usando o Secure Sockets Layer (SSL).

Antes de Iniciar

SSL é a tecnologia padrão para criar sessões criptografadas entre servidores e clientes. O SSL fornece um canal seguro para servidores e clientes para comunicação por caminhos de comunicação aberta. Com o SSL, a identidade do servidor é verificada por meio do uso de certificados digitais.

Para assegurar melhor desempenho do sistema, use SSL apenas para sessões quando ele for necessário. Considere a inclusão de recursos adicionais do processador no servidor IBM Spectrum Protect para gerenciar o aumento de requisitos.

Formatando o Banco de Dados e o Log

Se você configurar o servidor manualmente, deverá formatar o banco de dados do servidor e o log de recuperação. O banco de dados é usado para armazenar informações sobre dados do cliente e operações do servidor e o log de recuperação pode ser usado para recuperar-se de falhas no sistema e na mídia. Use o utilitário **DSMSERV FORMAT** para formatar e inicializar o banco de dados do servidor e o log de recuperação. Nenhuma outra atividade do servidor é permitida ao inicializar o banco de dados e o log de recuperação.

Após configurar as comunicações do servidor, você está pronto para inicializar o banco de dados. Não coloque os diretórios nos sistemas de arquivos que podem ficar sem espaço. Se determinados diretórios, como o log de archive, não estiverem mais disponíveis ou estiverem cheios, o servidor será interrompido. Consulte Planejamento de Capacidade para obter mais detalhes.

Configurando o manipulador da lista de saída

Configure a variável de registro **DB2NOEXITLIST** para ON para cada instância de servidor. Efetue logon no sistema usando o ID do usuário da instância e execute o comando a seguir:

```
db2set -i server_instance_name DB2NOEXITLIST=ON
```

Exemplo:

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```

Inicializando o banco de dados do servidor e o log de recuperação

Use o utilitário **DSMSERV FORMAT** para formatar e inicializar o banco de dados do servidor, que é um banco de dados IBM Db2, e o log de recuperação. Por exemplo, se o diretório de instância do servidor for */tsminst1*, execute os comandos a seguir:

```
cd /tsminst1
dsmserv format dbdir=/tsmdb001 activelogsize=32768
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Dica: Se você especificar vários diretórios, assegure-se de que os sistemas de arquivos subjacentes sejam de igual tamanho para assegurar um grau consistente de paralelismo para as operações do banco de dados. Se um ou mais diretórios do banco de dados forem menores que os outros, eles reduzirão o potencial de pré-busca e distribuição paralela otimizada do banco de dados.

Se o banco de dados Db2 não for iniciado após a execução do comando **DSMSERV FORMAT**, talvez seja necessário desativar a opção de montagem do sistema de arquivos NOSUID. Deve-se desativar a opção para iniciar o sistema nas seguintes circunstâncias:

- Se a opção for configurada no sistema de arquivos que contém o diretório do proprietário da instância do Db2.
- Se a opção for configurada em qualquer sistema de arquivos que contenha o banco de dados Db2 , logs ativos, logs de archive, logs de failover ou logs espelhados.

Depois de desativar a opção NOSUID, remonte o sistema de arquivos e, em seguida, inicie o banco de dados Db2 executando o comando a seguir:

```
db2start
```

Criando um usuário administrativo

Após a conclusão da formatação do banco de dados e do log de recuperação, deve-se criar um usuário administrativo que possa efetuar login no servidor e também ativar o IBM Spectrum Protect Operations Center para conectar-se ao servidor. Use os comandos a seguir em uma macro para configurar um usuário administrativo:

REGISTER ADMIN
O comando **REGISTER ADMIN** usa os parâmetros a seguir:

```
register admin administrator_user_id administrator_user_password
```

A senha deve atender a regras de comprimento específicas. Para obter mais informações, consulte REGISTER ADMIN (Registrar um ID de administrador)

GRANT AUTH
O comando **GRANT AUTH** usa os parâmetros a seguir:

```
grant auth administrator_user_id classes=administrator_user_class
```

Para obter mais informações, consulte GRANT AUTHORITY (Incluir a autoridade de administrador).

Conclua as etapas a seguir para configurar um usuário administrativo:

1. Crie uma macro, por exemplo, `setup.mac`.
2. Edite a macro para registrar um usuário administrativo e conceda a autoridade do sistema para o usuário, com as credenciais a seguir:
   - ID do usuário administrativo: `adminadmin`
   - Senha para o usuário administrativo: `adminadmin1`

   ```
   register admin adminadmin adminadmin1
   grant auth adminadmin classes=system
   ```

   Deve-se criar o usuário administrativo com a opção **classes=system** para que o usuário administrativo possa criar outros possíveis usuários administrativos, por exemplo, com privilégios limitados. Assim, qualquer um desses usuários administrativos poderá se conectar ao IBM Spectrum Protect Operations Center.
3. Para criar o usuário administrativo e conceder autoridade do sistema a ele, execute o comando **DSMSERV** com a opção **runfile** e o arquivo macro, por exemplo:

   ```
   dsmserv runfile setup.mac
   ```

Assim, o usuário administrativo poderá iniciar a instância do servidor e conectar-se ao servidor para concluir outras etapas necessárias, como configurar o backup do banco de dados.

Preparando o Gerenciador do Banco de Dados para o Backup de Banco de Dados

Para fazer backup dos dados no banco de dados para IBM Spectrum Protect, é necessário ativar o gerenciador de banco de dados e configurar a interface de programação de aplicativos (API) do IBM Spectrum Protect.

Sobre Esta Tarefa

Iniciando o IBM Spectrum Protect V7.1, não é mais necessário configurar a senha de API durante uma configuração manual do servidor. Se você configurar a senha de API durante o processo de configuração manual, as tentativas para fazer backup do banco de dados podem falhar.

Se você usar o assistente de configuração para criar uma instância do servidor IBM Spectrum Protect, não precisará concluir estas etapas. Se você estiver configurando uma instância manualmente, conclua as etapas a seguir antes de emitir os comandos **BACKUP DB** ou **RESTORE DB**.

Atenção: Se o banco de dados não puder ser utilizado, todo o servidor IBM Spectrum Protect estará indisponível. Se um banco de dados for perdido e não puder ser recuperado, poderá ser difícil ou impossível recuperar dados gerenciados por esse servidor. Assim, é criticamente importante fazer backup do banco de dados.

Nos comandos a seguir, substitua os valores de exemplo pelos valores reais. O exemplo usa `tsminst1` para o ID do usuário da instância do servidor, `/tsminst1` para o diretório de instância do servidor e `/home/tsminst1` como o diretório inicial de usuários da instância do servidor.

1. Defina a configuração da variável de ambiente da API do IBM Spectrum Protect para a instância do banco de dados:
   a. Efetue login usando o ID do usuário `tsminst1`.
   b. Quando o usuário `tsminst1` estiver com login efetuado, assegure-se de que o ambiente do IBM Db2 seja inicializado de forma adequada. O ambiente do Db2 é inicializado executando o script `/home/tsminst1/sqllib/db2profile`, que normalmente é executado automaticamente no perfil do ID do usuário. Assegure-se de que o arquivo `.profile` exista no diretório inicial de usuários da instância, por exemplo, `/home/tsminst1/.profile`. Se `.profile` não executar o script `db2profile`, inclua as linhas a seguir:

```
if [ -f /home/tsminst1/sqllib/db2profile ]; then
      . /home/tsminst1/sqllib/db2profile
  fi
```

   c. No arquivo `instance_directory/sqllib/userprofile`, inclua as seguintes linhas:

```
DSMI_CONFIG=server_instance_directory/tsmdbmgr.opt
DSMI_DIR=server_bin_directory/dbbkapi
DSMI_LOG=server_instance_directory
export DSMI_CONFIG DSMI_DIR DSMI_LOG
```

   onde:

   - *instance_directory* é o diretório inicial do usuário da instância do servidor.
   - *server_instance_directory* é o diretório de instância do servidor.
   - *server_bin_directory* é o diretório bin do servidor. O local padrão é `/opt/tivoli/tsm/server/bin`.

   No arquivo `instance_directory/sqllib/usercshrc`, inclua as seguintes linhas:

```
setenv DSMI_CONFIG=server_instance_directory/tsmdbmgr.opt
setenv DSMI_DIR=server_bin_directory/dbbkapi
setenv DSMI_LOG=server_instance_directory
```

2. Efetue logoff e login novamente como `tsminst1` ou emita esse comando:

```
. ~/.profile
```

Dica: Assegure-se de inserir um espaço após o caractere de ponto inicial (.).

3. Crie um arquivo denominado `tsmdbmgr.opt` no diretório *server_instance*, que está no diretório / `tsminst1` neste exemplo, e inclua a seguinte linha:

```
SERVERNAME TSMDBMGR_TSMINST1
```

Lembre-se: O valor para SERVERNAME deve ser consistente nos arquivos `tsmdbmgr.opt` e `dsm.sys`.

4. Como usuário raiz, inclua as linhas a seguir no arquivo de configuração IBM Spectrum Protect API `dsm.sys`. Por padrão, o arquivo de configuração `dsm.sys` está no local padrão a seguir:

   server_bin_directory/dbbkapi/dsm.sys

```
servername TSMDBMGR_TSMINST1
commmethod         tcpip
tcpserveraddr localhost
tcpport          1500
errorlogname /tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

   em que:

   - *servername* corresponde ao valor `servername` no arquivo `tsmdbmgr.opt`.
   - *commethod* especifica a API do cliente usada para entrar em contato com o servidor para backup de banco de dados. Este valor pode ser `tcpip` ou `sharedmem`. Para obter informações adicionais sobre memória compartilhada, consulte a etapa 5.
   - *tcpserveraddr* especifica o endereço do servidor que a API do cliente usa para entrar em contato com o servidor para backup de banco de dados. Para assegurar que seja feito backup do banco de dados, este valor deve ser `localhost`.

     Importante: Se o seu servidor estiver usando um certificado assinado por CA, você deverá especificar o endereço IP externo do servidor para a opção *tcpserveraddr*.
   - *tcpport* especifica o número da porta que a API do cliente usa para entrar em contato com o servidor para backup de banco de dados. Assegure-se de inserir o mesmo valor `tcpport` especificado no arquivo de opções do servidor `dsmserv.opt`.
   - *errorlogname* especifica o log de erros onde a API do cliente registra erros encontrados durante um backup de banco de dados. Este log geralmente fica no diretório de instância do servidor. No entanto, este log pode ser colocado em qualquer local onde o ID do usuário da instância tenha permissão de gravação.
   - *nodename* especifica o nome do nó que a API do cliente usa para conectar-se ao servidor durante um backup de banco de dados. Para assegurar que possa ser feito backup do banco de dados, este valor deve ser `$$_TSMDBMGR_$$`.

5. Opcional: Configure o servidor para fazer backup do banco de dados usando a memória compartilhada. Desta maneira, você pode conseguir reduzir a carga do processador e melhorar o rendimento. Execute as etapas a seguir:

   a. Revise o arquivo `dsmserv.opt`. Se as linhas a seguir não estiverem no arquivo, inclua-as:

```
commmethod      sharedmem
shmport port_number
```

      em que *port_number* especifica a porta a ser usada para a memória compartilhada.

   b. No arquivo de configuração `dsm.sys`, localize as linhas a seguir:

```
commmethod        tcpip
tcpserveraddr localhost
tcpport port_number
```

Substitua as linhas especificadas pelas linhas a seguir:

```
commmethod      sharedmem
shmport port_number
```

em que *port_number* especifica a porta a ser usada para a memória compartilhada.

Configurando as Opções do Servidor para Manutenção do Banco de Dados do Servidor

Para ajudar a evitar problemas com o crescimento do banco de dados e o desempenho do servidor, o servidor monitora automaticamente suas tabelas de banco de dados e as reorganiza quando necessário. Antes de iniciar o servidor para uso da produção, configure as opções do servidor para controlar quando a reorganização é executada. Se você planeja usar a deduplicação de dados, certifique-se de que a opção para executar a reorganização do índice esteja ativada.

Sobre Esta Tarefa

A reorganização da tabela e do índice exige recursos significativos do processador, espaço de log ativo e espaço de log de archive. Como o backup de banco de dados tem precedência sobre a reorganização, selecione o tempo e a duração para a reorganização para assegurar que os processos não sejam sobrepostos e a reorganização possa ser concluída.

É possível otimizar a reorganização de índice e de tabela para o banco de dados do servidor. Dessa maneira, é possível ajudar a evitar problemas inesperados no desenvolvimento e crescimento do banco de dados. Para obter instruções, consulte a nota técnica 1683633.

Se atualizar essas opções do servidor enquanto o servidor estiver em execução, você deverá parar e reiniciar o servidor antes de os valores atualizados entrarem em vigor.

Procedimento

1. Modifique as opções do servidor.

   Edite o arquivo de opções do servidor, `dsmserv.opt`, no diretório de instância do servidor. Siga essas diretrizes ao editar o arquivo de opções do servidor:

   - Para ativar uma opção, remova o asterisco no início da linha.
   - Insira uma opção em qualquer linha.
   - Insira apenas uma opção por linha. A opção inteira com seu valor deve estar em apenas uma linha.
   - Se houver diversas entradas para uma opção no arquivo, o servidor usará a última entrada.

   Para visualizar as opções de servidor disponíveis, consulte o arquivo de amostra, `dsmserv.opt.smp`, no diretório `/opt/tivoli/tsm/server/bin`.
2. Se planeja usar a deduplicação de dados, ative a opção do servidor **ALLOWREORGINDEX**.

   Inclua a opção e o valor a seguir no arquivo de opções do servidor:

   ```
   allowreorgindex yes
   ```
3. Configure as opções do servidor **REORGBEGINTIME** e **REORGDURATION** para controlar quando a reorganização inicia e por quanto tempo ela é executada. Selecione um tempo e a duração para que a reorganização seja executada quando você espera que o servidor esteja menos ocupado.

   Estas opções do servidor controlam os processos de reorganização da tabela e do índice.

   a) Configure o tempo para que a reorganização seja iniciada usando a opção do servidor **REORGBEGINTIME**. Especifique o tempo usando o sistema de 24 horas.
   Por exemplo, para configurar o horário de início para a reorganização como 8:30 p.m., especifique a opção e o valor a seguir no arquivo de opções do servidor:

   ```
   reorgbegintime 20:30
   ```

b) Configure o intervalo durante o qual o servidor poderá iniciar a reorganização.
Por exemplo, para especificar que o servidor pode iniciar a reorganização para quatro horas depois da hora configurada pela opção do servidor **REORGBEGINTIME**, especifique a opção e o valor a seguir no arquivo de opções do servidor:

```
reorgduration 4
```

4. Se o servidor estava em execução enquanto você atualizava o arquivo de opções do servidor, pare e reinicie o servidor.

Iniciando a Instância do Servidor

É possível iniciar o servidor usando o ID do usuário da instância, que é o método preferencial ou o ID do usuário raiz.

Antes de Iniciar

Assegure-se de que configurou corretamente as permissões de acesso e limites do usuário.

Sobre Esta Tarefa

Ao iniciar o servidor, usando o ID do usuário de instância, simplifique o processo de configuração e evite problemas em potencial. No entanto, em alguns casos, pode ser necessário iniciar o servidor com o ID do usuário raiz. Por exemplo, talvez você queira usar o ID do usuário raiz para assegurar que o servidor possa acessar os dispositivos específicos. É possível configurar o servidor para iniciar automaticamente, usando o ID do usuário da instância ou o ID do usuário raiz.

Se você tiver que concluir as tarefas de manutenção ou reconfiguração, inicie o servidor no modo de manutenção.

Procedimento

Para iniciar o servidor, execute uma das ações a seguir:

- Inicie o servidor usando o ID do usuário da instância.

  Para obter instruções, consulte “Iniciando o Servidor a partir do ID do Usuário da Instância” na página 97.
- Inicie o servidor usando o ID do usuário raiz.

  Para obter instruções sobre como autorizar os IDs do usuário raiz para iniciar o servidor, consulte Autorizando IDs de usuário raiz a iniciar o srevidor (V7.1.1). Para obter instruções sobre como iniciar o servidor usando o ID de usuário raiz, consulte Iniciando o servidor a partir do ID do usuário raiz (V7.1.1).
- Inicie o servidor automaticamente.

  Para obter instruções, consulte “Iniciando Servidores Automaticamente” na página 97.
- Inicie o servidor no modo de manutenção.

  Para obter instruções, consulte “Iniciando o servidor no modo de manutenção” na página 98.

Verificando Direitos de Acesso e Limites do Usuário

Antes de iniciar o servidor, verifique os direitos de acesso e os limites do usuário.

Sobre Esta Tarefa

Se você não verificar os limites do usuário, também conhecidos como *ulimits*, talvez encontre instabilidade do servidor ou falha do servidor ao responder. Você também deve verificar o limite de todo o

sistema para o número máximo de arquivos abertos. O limite de todo o sistema deve ser maior ou igual ao limite do usuário.

Procedimento

1. Verifique se o ID do usuário da instância do servidor possui permissões para iniciar o servidor.
2. Para a instância do servidor que você planeja iniciar, assegure-se de ter autoridade para ler e gravar os arquivos no diretório de instância do servidor.

   Verifique se o arquivo `dsmserv.opt` existe no diretório de instâncias do servidor e que o arquivo inclui parâmetros para a instância do servidor.
3. Se o servidor estiver conectado a uma unidade de fita, alterador de mídia ou dispositivo de mídia removível e você planejar iniciar o servidor usando o ID do usuário da instância, conceda acesso de leitura/gravação ao ID do usuário da instância para esses dispositivos. Para configurar as permissões, execute uma das ações a seguir:

   - Se o sistema for dedicado ao IBM Spectrum Protect e apenas o administrador do IBM Spectrum Protect tiver acesso, torne o arquivo especial do dispositivo gravável para todos. Na linha de comandos do sistema operacional, emita o comando a seguir:

     ```
     chmod +w /dev/rmtX
     ```

   - Se o sistema tiver vários usuários, você poderá restringir o acesso tornando o ID do usuário da instância do IBM Spectrum Protect o proprietário dos arquivos especiais do dispositivo. Na linha de comandos do sistema operacional, emita o comando a seguir:

     ```
     chmod u+w /dev/rmtX
     ```

   - Se várias instâncias de usuário estiverem executando no mesmo sistema, altere o nome do grupo, por exemplo TAPEUSERS, e inclua cada ID de usuário da instância do IBM Spectrum Protect nesse grupo. Em seguida, altere a propriedade dos arquivos especiais do dispositivo para pertencer ao grupo TAPEUSERS e torne-os graváveis no grupo. Na linha de comandos do sistema operacional, emita o comando a seguir:

     ```
     chmod g+w /dev/rmtX
     ```
4. Verifique os limites de usuário a seguir com base nas diretrizes na tabela.

Tabela 16. Valores de limite do usuário (ulimit)

Tipo de limite do usuário	Valor preferencial	Comando para consultar valor
Tamanho máximo dos arquivos principais criados	Sem limites	`ulimit -Hc`
Tamanho máximo de um segmento de dados para um processo	Sem limites	`ulimit -Hd`
Tamanho máximo do arquivo	Sem limites	`ulimit -Hf`
Número máximo de arquivos abertos	65536	`ulimit -Hn`
Quantidade máxima de tempo do processador em segundos	Sem limites	`ulimit -Ht`

   Para modificar os limites do usuário, siga as instruções na documentação para o sistema operacional.

   Dica: Se você planeja iniciar o servidor automaticamente usando um script, poderá configurar os limites do usuário no script.
5. Certifique-se de que o limite do usuário do máximo de processos do usuário (a configuração `nproc`) esteja configurado como o valor mínimo sugerido de 16384.

a) Para verificar o limite do usuário atual, emita o comando `ulimit -Hu` usando o ID do usuário da instância.
Por exemplo:

```
[user@Machine ~]$ ulimit -Hu
16384
```

b) Se o limite de processos máximos do usuário não for configurado para 16384, configure o valor para 16384.

Inclua a seguinte linha no arquivo `/etc/security/limits`:

```
instance_user_id         -    nproc           16384
```

em que *instance_user_id* especifica o ID do usuário da instância do servidor.

Iniciando o Servidor a partir do ID do Usuário da Instância

Para iniciar o servidor a partir do ID do usuário da instância, efetue login com o ID do usuário da instância e emita o comando apropriado a partir do diretório de instância do servidor.

Antes de Iniciar

Assegure-se de que os direitos de acesso e os limites do usuário estejam corretamente configurados.

Procedimento

1. Efetue login no sistema em que o IBM Spectrum Protect está instalado usando o ID do usuário da instância para o servidor.
2. Se você não tiver um perfil do usuário que executa o script `db2profile`, emita o seguinte comando:

   ```
   . /home/tsminst1/sqllib/db2profile
   ```

   Dica: Para obter instruções sobre a atualização do script de login do ID do usuário para a execução automática do script `db2profile`, consulte o Informações do produto DB2.
3. Inicie o servidor, emitindo o comando a seguir em uma linha a partir do diretório de instância do servidor:

   ```
   LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K
   usr/bin/dsmserv
   ```

   Assegure-se de incluir um espaço após SHMPSIZE=64K. Iniciando o servidor com esse comando, ative as páginas de memória de 64 KB para o servidor. Essa configuração ajuda a otimizar o desempenho do servidor.

   Dica: O comando é executado no primeiro plano, de forma que você possa configurar um ID do administrador e conectar à instância do servidor.

   Por exemplo, se o nome da instância do servidor for `tsminst1` e o diretório de instância do servidor for `/tsminst1`, é possível iniciar a instância emitindo os comandos a seguir:

   ```
   cd /tsminst1
    . ~/sqllib/db2profile
   LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K
   usr/bin/dsmserv
   ```

Iniciando Servidores Automaticamente

É possível configurar o servidor para iniciar automaticamente na inicialização do sistema. Use o script **`rc.dsmserv`**, que é fornecido para esse propósito.

Antes de Iniciar

Assegure-se de que os direitos de acesso e os limites do usuário estejam corretamente configurados.

Sobre Esta Tarefa

O script **rc.dsmserv** está no diretório de instalação do servidor, por exemplo, no diretório `/opt/tivoli/tsm/server/bin`.

Dica: Se você usou o assistente de configuração, é possível que tenha escolhido iniciar o servidor automaticamente na reinicialização do sistema. Se selecionou essa opção, uma entrada para iniciar o servidor foi incluída automaticamente no arquivo `/etc/inittab`.

Procedimento

Se você não usou um assistente para configura o servidor, inclua uma entrada no arquivo `/etc/inittab` para cada servidor que deseja iniciar automaticamente:

1. Configure o nível de execução com o valor correspondente ao modo multiusuário, com rede ativada. Normalmente, o nível de execução a ser usado é 2, 3 ou 5, dependendo do sistema operacional e de sua configuração. Certifique-se de que o nível de execução no arquivo `/etc/inittab` corresponda ao nível de execução do sistema operacional.

   Para obter informações adicionais sobre o modo de multiusuário e níveis de execução, consulte a documentação para seu sistema operacional.
2. No comando **rc.dsmserv** no arquivo `/etc/inittab`, especifique o ID do usuário da instância com a opção `-u` e o local do diretório de instância do servidor com a opção `-i`. Se você deseja iniciar mais de uma instância de servidor automaticamente, inclua uma entrada para cada instância de servidor automaticamente.

   Para verificar a sintaxe, consulte a documentação para o sistema operacional.

   Dica: Para iniciar automaticamente uma instância de servidor com o ID do usuário raiz, use a opção `-U`.

Exemplo

Por exemplo, se o proprietário da instância for tsminst1 e o diretório de instância do servidor for `/home/tsminst1/tsminst1`, inclua a seguinte entrada em `/etc/inittab`, em uma linha:

```
tsm1:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst1
   -i /home/tsminst1/tsminst1 -q >/dev/console 2>&1
```

Nesse exemplo, o ID para o processo é `tsm1`, e o nível de execução está configurado como 2.

Se houver mais de uma instância do servidor que você queira executar, inclua uma entrada para cada instância do servidor. Por exemplo, se tiver os IDs de proprietário de instância tsminst1 e tsminst2, e os diretórios de instância `/home/tsminst1/tsminst1` e `/home/tsminst2/tsminst2`, inclua as seguintes entradas em `/etc/inittab`. Cada entrada está em uma linha.

```
tsm1:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst1
   -i /home/tsminst1/tsminst1 -q >/dev/console 2>&1
tsm2:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst2
   -i /home/tsminst2/tsminst2 -q >/dev/console 2>&1
```

Iniciando o servidor no modo de manutenção

É possível iniciar o servidor no modo de manutenção para evitar interrupções durante tarefas de manutenção e de reconfiguração.

Sobre Esta Tarefa

Inicie o servidor no modo de manutenção, executando o utilitário **DSMSERV** com o parâmetro **MAINTENANCE**.

As operações a seguir são desativadas no modo de manutenção:

- Planejamentos de comandos administrativos
- Planejamentos de Clientes
- Reclamação do espaço de armazenamento no servidor
- Expiração de inventário
- Migração dos conjuntos de armazenamentos

Além disso, os clientes são impedidos de iniciar as sessões com o servidor.

Dicas:

- Não é necessário editar o arquivo de opções do servidor, `dsmserv.opt`, para iniciar o servidor no modo de manutenção.
- Enquanto o servidor estiver em execução no modo de manutenção, é possível iniciar manualmente a recuperação de espaço de armazenamento, expiração de inventário e processos de migração do conjunto de armazenamentos.

Procedimento

- Para iniciar o servidor no modo de manutenção, emita o comando a seguir:

  ```
  dsmserv maintenance
  ```

  Dica: Para visualizar um vídeo sobre como iniciar o servidor no modo de manutenção, veja Iniciando um servidor no modo de manutenção.

O que Fazer Depois

Para continuar as operações do servidor em modo de produção, conclua as etapas a seguir:

1. Encerre o servidor, emitindo o comando **HALT**:

   ```
   halt
   ```

2. Inicie o servidor, usando o método que você usa no modo de produção.

As operações que foram desativadas durante o modo de manutenção foram reativadas.

Parando o Servidor

É possível parar o servidor quando necessário para retornar o controle para o sistema operacional. Para evitar a perda de conexões de nó cliente e administrativas, pare o servidor apenas após as sessões atuais serem concluídas ou canceladas.

Sobre Esta Tarefa

Para parar o servidor, emita o comando a seguir na linha de comandos do IBM Spectrum Protect:

```
halt
```

Se não for possível se conectar ao servidor com um cliente administrador e desejar parar o servidor, deve-se cancelar o processo usando o comando **kill** com o número do ID do processo (pid). O ID do processo é exibido na inicialização.

Importante: Antes de emitir o comando **kill**, assegure-se de conhecer o ID de processo correto para o servidor IBM Spectrum Protect.

O arquivo `dsmserv.v6lock`, no diretório a partir do qual o servidor está executando, pode ser usado para identificar o ID de processo do processo de kill. Para exibir o arquivo, insira:

```
cat
/instance_dir/dsmserv.v6lock
```

Emita o seguinte comando para parar o servidor:

```
kill -36 dsmserv_pid
```

em que *dsmserv_pid* é o número do ID do processo.

Registrando Licenças

Registre imediatamente todas as funções licenciadas do IBM Spectrum Protect que você adquirir, para que não perca nenhum dado depois que iniciar as operações do servidor, como fazer backup dos dados.

Sobre Esta Tarefa

Utilize o comando **REGISTER LICENSE** para esta tarefa.

Exemplo: Registrar uma Licença

Registre a licença base do IBM Spectrum Protect.

```
register license file=tsmbasic.lic
```

Preparando o servidor para operações de backup de banco de dados

Para preparar o servidor para operações de backup do banco de dados manuais e automáticas, assegure-se de especificar uma fita, um arquivo ou uma classe de dispositivo de nuvem e de concluir outras etapas.

Procedimento

1. Assegure-se de que a configuração do servidor IBM Spectrum Protect esteja completa.

   Dica: É possível configurar o servidor para backups de banco de dados usando o assistente de configuração (`dsmicfgx`) ou concluir as etapas manualmente. Para obter mais informações sobre configuração, consulte a seção *Configurando servidores* em IBM Knowledge Center.
2. Selecione a classe de dispositivo a ser usada para backups de banco de dados, para proteger a chave mestra de criptografia e configurar uma senha.

   Assegure-se de que os arquivos-chave a seguir sejam protegidos:

   - Arquivos da chave mestra de criptografia (dsmkeydb.*)
   - Arquivos de certificado do servidor e de chave privada (cert.*)

   Para concluir essas ações, emita o comando **SET DBRECOVERY** a partir da linha de comandos administrativos:

   ```
   set dbrecovery device_class_name protectkeys=yes password=password_name
   ```

   em que *device_class_name* especifica a classe de dispositivo a ser usada para operações de backup de banco de dados e *password_name* especifica a senha.

   Deve-se especificar um nome da classe de dispositivo ou o backup falhará. Ao especificar **PROTECTKEYS=YES**, você assegura que a chave mestra de criptografia seja submetida a backup durante operações de backup de banco de dados. As classes de dispositivo de nuvem requerem o parâmetro **PROTECTKEYS=YES**.

Crie uma senha forte que tenha pelo menos 8 caracteres. Se você especificar uma senha para o backup de banco de dados, deve-se especificar a mesma senha no comando **RESTORE DB** para restaurar o banco de dados.

Atenção: Assegure-se de lembrar a senha e de manter uma cópia armazenada em um local seguro. Sem a senha, os dados não podem ser recuperados.

Exemplo

Para especificar que os backups de banco de dados incluam uma cópia da chave mestra de criptografia para o servidor, execute o seguinte comando:

```
set dbrecovery dbback protectkeys=yes password=protect8991
```

Executando Diversas Instâncias do Servidor em um Único Sistema

É possível criar mais de uma instância do servidor em seu sistema. Cada instância do servidor tem seu próprio diretório de instâncias e diretórios de banco de dados e de log.

Multiplique a memória e outros requisitos do sistema de um servidor pelo número de instâncias planejadas para o sistema.

O conjunto de arquivos para uma instância do servidor é armazenado separadamente dos arquivos usados por outra instância do servidor no mesmo sistema. Use as etapas em a seção Criando a instância do servidor para cada nova instância, incluindo a criação do novo usuário da instância.

Para gerenciar a memória do sistema que é usada por cada servidor, use a opção do servidor DBMEMPERCENT para limitar a porcentagem de memória do sistema. Se todos os servidores forem igualmente importantes, utilize o mesmo valor para cada servidor. Se um servidor for o servidor de produção e os outros servidores forem servidores de teste, configure o valor para o servidor de produção para um valor mais alto que dos servidores de teste.

É possível fazer upgrade diretamente da V7.1 para a V8.1. Consulte a seção de upgrade para obter mais detalhes. Quando fizer upgrade e tiver vários servidores em seu sistema, você deve executar o assistente de instalação apenas uma vez. O assistente de instalação coleta informações do banco de dados e das variáveis para todas as suas instâncias do servidor originais.

Monitorando o Servidor

Ao começar a usar o servidor em produção, monitore o espaço usado pelo servidor para assegurar que a quantidade de espaço esteja adequada. Ajuste o espaço, se necessário.

Procedimento

1. Monitore o log ativo para assegurar que o tamanho esteja correto para a carga de trabalho manipulada pela instância do servidor.

   Quando a carga de trabalho do servidor atingir seu nível típico esperado, o espaço usado pelo log ativo será 80% - 90% do espaço disponível para o diretório de log ativo. Nesse ponto, talvez seja necessário aumentar a quantia de espaço. A necessidade de aumentar o espaço depende dos tipos de transações na carga de trabalho do servidor. As características da transação afetam o modo como o espaço do log ativo é usado.

   As características da transação a seguir podem afetar o uso de espaço no log ativo:

   - O número e o tamanho dos arquivos em operações de backup
     - Clientes como servidores de arquivos que fazem backup de grandes números de arquivos pequenos podem causar grandes números de transações que são concluídas rapidamente. As transações podem usar uma grande quantia de espaço no log ativo, mas por um curto período de tempo.

  - Clientes como um servidor de e-mail ou um servidor de banco de dados que fazem backup de grandes quantias de dados em poucas transações podem causar pequenos números de transações que demoram muito tempo para serem concluídas. As transações podem usar uma pequena quantia de espaço no log ativo, mas por muito tempo.
- Tipos de conexão de rede
  - As operações de backup que ocorrem através de conexões de rede rápidas fazem com que as transações sejam concluídas mais rapidamente. As transações usam o espaço no log ativo por tempo mais curto.
  - As operações de backup que ocorrem através de conexões relativamente mais lentas fazem com que transações que levam um período mais longo sejam concluídas. As transações usam o espaço no log ativo por um período mais longo.

Se o servidor estiver manipulando transações com uma grande variedade de características, o espaço usado para o log ativo pode aumentar e diminuir significativamente com o tempo. Para tal servidor, pode ser necessário que o log ativo tenha tipicamente uma porcentagem menor de seu espaço usado. O espaço extra permite que o log ativo aumente para transações que demoram muito tempo para serem concluídas.

2. Monitore o log de archive para assegurar que o espaço sempre esteja disponível.

   Lembre-se: Se o log de archive e o log de archive de failover ficarem cheios, o log ativo poderá ficar cheio e o servidor parar. A meta é disponibilizar espaço suficiente para o log de archive de forma que nunca use todo o seu espaço disponível.

   Provavelmente você notará o seguinte padrão:

   a. Inicialmente, o log de archive cresce rapidamente à medida que operações típicas de backup ocorram.
   b. Os backups de banco de dados ocorrem regularmente, conforme planejado ou feitos manualmente.
   c. Depois de ocorrer pelo menos dois backups completos do banco de dados, ocorre a limpeza do log automaticamente. O espaço usado pelo log de archive diminui quando ocorre remoção.
   d. As operações normais do cliente continuam e o log de archive aumenta novamente.
   e. Os backups de banco de dados ocorrem regularmente e a limpeza de log ocorre com a mesma frequência que ocorrem os backups de banco de dados integrais.

   Com esse padrão, o log de archive aumenta inicialmente, diminui e depois pode aumentar novamente. Com o tempo, conforme as operações normais continuam, a quantia de espaço usada pelo log de archive deve atingir um nível relativamente constante.

   Se o log de archive continuar a crescer, considere executar uma ou ambas as ações a seguir:

   - Inclua espaço no log de archive. Talvez seja necessário mover o log de archive para um sistema de arquivos diferente.
   - Aumente a frequência de backups de banco de dados integrais, de forma que a limpeza de log ocorra mais frequentemente.
3. Se você tiver definido um diretório para o log de archive de failover, determine se algum log será armazenado nesse diretório durante as operações normais. Se o espaço do log de failover estiver sendo usado, considere aumentar o tamanho do log de archive.

   A meta é que o log de archive de failover seja usado somente sob condições fora do comum, não na operação normal.

Capítulo 4. Instalando um Fix Pack do Servidor IBM Spectrum Protect

Atualizações de manutenção do IBM Spectrum Protect, que são também mencionadas como fix packs, colocam seu servidor no nível de manutenção atual.

Antes de Iniciar

Para instalar um fix pack ou correção temporária no servidor, instale o servidor no nível em que deseja executá-lo. Você não tem de iniciar a instalação do servidor no nível de liberação de base. Por exemplo, se você tiver atualmente a V8.1.1 instalada, será possível ir diretamente para o fix pack mais recente da V8.1. Não será necessário iniciar com a instalação da V8.1.0 se uma atualização de manutenção estiver disponível.

Você deve ter o pacote de licença do IBM Spectrum Protect instalado. O pacote de licença é fornecido com a compra de um release básico. Ao fazer download de um fix pack ou correção temporária do Fix Central, instale a licença do servidor, que está disponível no website do Passport Advantage. Para exibir mensagens e ajuda em um idioma diferente do inglês dos EUA, instale o pacote de idiomas de sua escolha.

Se você fizer upgrade do servidor e, em seguida, reverter o servidor para um nível anterior, será necessário restaurar o banco de dados para um momento antes do upgrade. Durante o processo de upgrade, conclua as etapas necessárias para assegurar que o banco de dados possa ser restaurada: faça o backup do banco de dados, do arquivo do histórico de volume, do arquivo de configuração do dispositivo e do arquivo de opções do servidor.

Se você estiver usando o serviço de gerenciamento do cliente, assegure-se de atualizá-lo para a mesma versão do servidor IBM Spectrum Protect.

Assegure-se de reter a mídia de instalação da liberação base do servidor instalado. Se você instalou o IBM Spectrum Protect a partir de um pacote transferido por download, certifique-se de que os arquivos transferidos por download estejam disponíveis. Se o upgrade falhar, e o módulo de licença do servidor for desinstalado, a mídia de instalação da liberação de base do servidor será necessária para a reinstalação da licença.

Visite o IBM Support Portal para obter as informações a seguir:

- Uma lista da manutenção mais recente e download de correções. Clique em **Downloads** e aplique todas as correções aplicáveis.
- Detalhes sobre a obtenção de um pacote de licença de base. Procure por **Downloads > Passport Advantage**.
- Plataformas suportadas e requisitos do sistema. Procure por **Sistemas operacionais do IBM Spectrum Protect suportados**.

Assegure-se de fazer upgrade do servidor antes de fazer upgrade dos clientes de backup-archive. Se você não fizer primeiro o upgrade do servidor, a comunicação entre o servidor e os clientes poderá ser interrompida.

Atenção: Não mude o software Db2 que está instalado com os pacotes de instalação e fix packs do IBM Spectrum Protect. Não instale ou atualize para uma versão, liberação ou fix pack diferente do software Db2, pois fazer isso pode danificar o banco de dados.

Procedimento

Para instalar um fix pack ou uma correção temporária, conclua as etapas a seguir:

1. Faça backup do banco de dados. O método preferencial é usar um backup de captura instantânea. Um backup de captura instantânea é um backup completo de banco de dados que não interrompe

nenhum backup de banco de dados planejado. Por exemplo, emita o comando administrativo do IBM Spectrum Protect a seguir:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Faça backup das informações de configuração do dispositivo. Emita o comando administrativo do IBM Spectrum Protect a seguir:

   ```
   backup devconfig filenames=file_name
   ```

   em que *file_name* especifica o nome do arquivo no qual armazenar informações sobre a configuração do dispositivo.
3. Salve o arquivo do histórico de volume em outro diretório ou renomeie o arquivo. Emita o comando administrativo do IBM Spectrum Protect a seguir:

   ```
   backup volhistory filenames=file_name
   ```

   em que *file_name* especifica o nome do arquivo no qual armazenar as informações do histórico do volume.
4. Salve uma cópia do arquivo de opções do servidor, geralmente denominado `dsmserv.opt`. O arquivo está no diretório de instância do servidor.
5. Pare o servidor antes de instalar um fix pack ou correção temporária.

   Use o comando **HALT**.
6. Assegure-se de que o espaço extra esteja disponível no diretório de instalação.

   A instalação deste fix pack pode requerer espaço em disco adicional temporário no diretório de instalação do servidor. A quantia de espaço em disco adicional pode ser tanto quanto a requerida para a instalação de um novo banco de dados como parte de uma instalação do IBM Spectrum Protect. O assistente de instalação do IBM Spectrum Protect exibe a quantidade de espaço requerido para instalação do fix pack e a quantidade disponível. Se a quantidade de espaço requerida for maior que a quantidade disponível, a instalação irá parar. Se a instalação parar, inclua o espaço em disco requerido para o sistema de arquivos e reinicie a instalação.
7. Efetue login como usuário root.
8. Obtenha o arquivo de pacote para o fix pack ou correção temporária a ser instalada a partir do IBM Support Portal, do Passport Advantage ou do Fix Central.
9. Vá para o diretório onde colocou o arquivo executável e conclua as etapas a seguir.

   Dica: Os arquivos são extraídos para o diretório atual. Assegure-se de que o arquivo executável esteja no diretório onde você deseja que os arquivos extraídos sejam localizados.

   a. Altere as permissões do arquivo digitando o seguinte comando:

      ```
      Chmod a + x 8.x.x.x-IBM-SPSRV-platform.bin
      ```

      onde *platform* denota a arquitetura na qual o IBM Spectrum Protect deve ser instalado.

   b. Emita o seguinte comando para extrair os arquivos de instalação:

      ```
      ./8.x.x.x-IBM-SPSRV-platform.bin
      ```
10. Selecione uma das seguintes maneiras de instalar o IBM Spectrum Protect.

    Importante: Depois que um fix pack for instalado, não será necessário passar pela configuração novamente. É possível parar após a conclusão da instalação, corrigir quaisquer erros e, em seguida, reiniciar seus servidores.

    Instale o software IBM Spectrum Protect usando um dos métodos a seguir:

    Assistente de instalação

    Siga as instruções para o seu sistema operacional:

    "Instalando o IBM Spectrum Protect Usando o Assistente de Instalação" na página 76

Dica: Depois de iniciar o assistente, na janela **IBM Installation Manager**, clique no ícone **Atualizar**; não clique no ícone **Instalar** ou **Modificar**.

Linha de comandos no modo do console

Siga as instruções para o seu sistema operacional:

"Instalando o IBM Spectrum Protect Usando o Modo do Console" na página 77

Dica: Se você tiver diversas instâncias do servidor em seu sistema, execute o assistente de instalação apenas uma vez. O assistente de instalação atualiza todas as instâncias do servidor.

Resultados

Corrija os erros detectados durante o processo de instalação.

Se você instalou o servidor usando o assistente de instalação, será possível visualizar os logs de instalação usando a ferramenta IBM Installation Manager. Clique em **Arquivo** > **Visualizar Log**. Para coletar os arquivos de log, na ferramenta IBM Installation Manager, clique em **Ajuda** > **Dados de Exportação para Análise de Problemas**.

Se você instalou o servidor usando o modo de console ou o modo silencioso, será possível visualizar os logs de erro no diretório de log do IBM Installation Manager, por exemplo:

```
/var/ibm/InstallationManager/logs
```

Aplicando um fix pack no IBM Spectrum Protect em um ambiente em cluster

Atualizações de manutenção do IBM Spectrum Protect, que são também mencionadas como fix packs, colocam seu servidor no nível de manutenção atual. É possível aplicar um fix pack em um ambiente em cluster para o AIX.

Antes de Iniciar

Para instalar um fix pack ou correção temporária no servidor, instale o servidor no nível em que deseja executá-lo. Você não tem de iniciar a instalação do servidor no nível de liberação de base. Por exemplo, se você tiver atualmente a V8.1.1 instalada, será possível ir diretamente para o fix pack mais recente da V8.1. Não será necessário iniciar com a instalação da V8.1.0 se uma atualização de manutenção estiver disponível.

Procedimento

1. Faça backup do banco de dados. O método preferencial é usar um backup de captura instantânea. Um backup de captura instantânea é um backup completo de banco de dados que não interrompe nenhum backup de banco de dados planejado. Por exemplo, emita o seguinte comando:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

   Se tiver que reverter o servidor para o nível anterior, é necessário ter o backup de banco de dados e os arquivos de configuração para restaurar o servidor para o nível anterior.
2. Faça backup das informações de configuração do dispositivo. Emita o seguinte comando:

   ```
   backup devconfig filenames=file_name
   ```

   em que *file_name* especifica o nome do arquivo no qual armazenar informações sobre a configuração do dispositivo.
3. Faça backup das informações do histórico do volume. Emita o seguinte comando:

   ```
   backup volhistory filenames=file_name
   ```

   em que *file_name* especifica o nome do arquivo no qual armazenar as informações do histórico do volume.

4. Salve uma cópia do arquivo de opções do servidor, geralmente denominado `dsmserv.opt`. O arquivo está no diretório de instância do servidor.
5. Se estiver usando o monitoramento de nível do aplicativo do servidor IBM Spectrum Protect, no nó primário, suspenda o monitoramento do recurso do aplicativo dsmserv. Para suspender o monitoramento, use o menu smitty do IBM PowerHA.
6. Pare o servidor IBM Spectrum Protect.
7. Verifique se o gerenciador do banco de dados não está executando.
8. Monte todos os recursos compartilhados no nó primário.

   Verifique se nenhum outro nó tem acesso de gravação a esses recursos durante a instalação do fix pack. Se seu ambiente incluir diversas instâncias do IBM Spectrum Protect, os recursos compartilhados para todas as instâncias devem ser acessíveis ao nó primário durante a instalação do fix pack.
9. Instale o servidor IBM Spectrum Protect no nó primário.
10. Inicie o servidor IBM Spectrum Protect.
11. Pare o servidor IBM Spectrum Protect. Acesse o nó secundário.
12. No nó secundário, instale o servidor IBM Spectrum Protect.

Capítulo 5. Fazendo upgrade para a V8.1

Para tirar vantagem de novos recursos e atualizações do produto, atualize o servidor do IBM Spectrum Protect.

Antes de Iniciar

Revise as informações de planejamento de atualizações de segurança no "O que é necessário saber sobre segurança antes de instalar ou fazer upgrade do servidor" na página 3.

Sobre Esta Tarefa

Para fazer upgrade do servidor no mesmo sistema operacional, consulte as instruções de upgrade. Para obter instruções sobre a migração do servidor para um sistema operacional diferente, consulte IBM Spectrum Protect Processo de upgrade e de migração - perguntas mais frequentes.

Tabela 17. Instruções de Upgrade

Para atualizar a partir dessa versão	Para esta versão	Consulte estas informações
V8.1	Fix pack ou correção temporária da V8.1	Capítulo 4, "Instalando um Fix Pack do Servidor IBM Spectrum Protect", na página 103
V7.1	V8.1	"Instalando o servidor e verificando o upgrade" na página 110
V7.1	Fix pack ou correção temporária da V8.1	Capítulo 4, "Instalando um Fix Pack do Servidor IBM Spectrum Protect", na página 103
V5.5, V6.2, ou V6.3	V8.1	IBM Spectrum Protect Processo de upgrade e migração - Perguntas mais frequentes

Um upgrade da V7 para a V8.1 leva aproximadamente de 20 a 50 minutos. Seu ambiente poderá produzir resultados diferentes dos resultados que foram obtidos nos laboratórios.

Para obter informações sobre atualizações em um ambiente em cluster, consulte "Atualizando o Servidor em um Ambiente em Cluster" na página 113.

Para reverter para uma versão anterior do servidor após um upgrade ou migração, deve-se ter um backup de banco de dados integral e o software de instalação para o servidor original. Deve-se também ter os seguintes arquivos de configuração de teclas:

- Arquivo de Histórico de Volumes
- Arquivo de Configuração de Dispositivo
- Arquivo de opções do servidor

Informações relacionadas

Processo de upgrade e migração do IBM Spectrum Protect - perguntas mais frequentes

Fazendo upgrade para a V8.1

É possível fazer upgrade do servidor diretamente da V7.1 para a V8.1. Não é necessário desinstalar a V7.1.

Antes de Iniciar

Assegure que a mídia de instalação da liberação de base do servidor da qual você está fazendo upgrade seja retida. Se você instalou os componentes do servidor a partir de um DVD, assegure-se de que o DVD esteja disponível. Se você instalou os componentes do servidor a partir de um pacote transferido por download, assegure-se de que os arquivos transferidos por download estejam disponíveis. Se o upgrade falhar, e o módulo de licença do servidor for desinstalado, a mídia de instalação da liberação de base do servidor será necessária para a reinstalação da licença.

Dica: DVDs não estão mais disponíveis com a V8.1 e posterior.

Procedimento

Para fazer upgrade do servidor para a V8.1, conclua as tarefas a seguir:

1. “Planejando o Upgrade” na página 108
2. “Preparando o Sistema” na página 108
3. “Instalando o servidor e verificando o upgrade” na página 110

Planejando o Upgrade

Antes de fazer upgrade do servidor da V7.1 para a V8.1, deve-se revisar as informações de planejamento relevantes, como os requisitos do sistema e as notas sobre a liberação. Em seguida, selecione um dia e hora apropriados para fazer upgrade do sistema para que você possa minimizar o impacto nas operações de produção.

Sobre Esta Tarefa

Nos testes de laboratório, o processo de upgrade do servidor da V7.1 para a V8.1 leva de 14 a 45 minutos. Os resultados que você alcança podem ser diferentes, dependendo do seu ambiente de hardware e de software e do tamanho do banco de dados do servidor.

Procedimento

1. Revise os requisitos de hardware e de software:

   Requisitos do sistema para os sistemas AIX

   Para obter as atualizações mais recentes relacionadas aos requisitos do sistema, consulte o website de suporte do IBM Spectrum Protect na nota técnica 1243309.
2. Para obter instruções especiais ou informações específicas para seu sistema operacional, revise as notas sobre a liberação (http://www.ibm.com/support/knowledgecenter/SSEQVQ_8.1.11/srv.common/r_relnotes_srv.html) e os arquivos leia-me para componentes do servidor.
3. Revise as informações de planejamento de atualizações de segurança no “O que é necessário saber sobre segurança antes de instalar ou fazer upgrade do servidor” na página 3.
4. Selecione um dia e hora apropriados para fazer upgrade de seu sistema para minimizar o impacto em operações de produção. A quantia de tempo necessária para atualizar o sistema depende do tamanho do banco de dados e de vários outros fatores. Ao iniciar o processo de upgrade, os clientes não podem se conectar ao servidor até que o novo software esteja instalado e as licenças necessárias sejam registradas novamente.
5. Se você estiver fazendo upgrade do servidor da V7 para a V8.1, verifique se tem o ID do sistema e a senha para a instância do IBM Db2 do servidor IBM Spectrum Protect. Essas credenciais são necessárias para fazer upgrade do sistema.

Preparando o Sistema

Para preparar o sistema para o upgrade da V7.1 para a V8.1, deve-se reunir informações sobre cada instância do IBM Db2. Em seguida, faça backup do banco de dados do servidor, salve os arquivos de configuração de teclas, cancele sessões e pare o servidor.

Procedimento

1. Efetue logon no computador no qual o servidor está instalado.

   Assegure-se de ter efetuado logon com o ID do usuário da instância.
2. Obtenha uma lista de instâncias do Db2. Emita o comando do sistema a seguir:

   ```
   /opt/tivoli/tsm/db2/instance/db2ilist
   ```

   A saída pode ser semelhante ao exemplo a seguir:

   ```
   tsminst1
   ```

   Assegure-se de que cada instância corresponda a um servidor que esteja em execução no sistema.
3. Para cada instância do Db2, observe o caminho do banco de dados padrão, o caminho do banco de dados real, o nome do banco de dados, o alias do banco de dados e quaisquer variáveis do Db2 que estejam configuradas para a instância. Guarde o registro para referência futura. Essas informações são necessárias para restaurar o banco de dados V7.1.
4. Conecte-se ao servidor usando um ID do usuário administrativo.
5. Faça backup do banco de dados usando o comando **BACKUP DB**.

   O método preferencial é criar um backup de captura instantânea, que é um backup de banco de dados completo que não interrompe os backups de banco de dados planejados.

   Por exemplo, é possível criar um backup de captura instantânea emitindo o seguinte comando:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```
6. Faça backup das informações de configuração do dispositivo em outro diretório emitindo o comando administrativo a seguir:

   ```
   backup devconfig filenames=file_name
   ```

   em que *file_name* especifica o nome do arquivo no qual armazenar informações sobre a configuração do dispositivo.

   Dica: Se você decidir restaurar o banco de dados V7.1, esse arquivo será necessário.
7. Faça backup do arquivo do histórico de volume para outro diretório. Emita o seguinte comando administrativo:

   ```
   backup volhistory filenames=file_name
   ```

   em que *file_name* especifica o nome do arquivo no qual armazenar as informações do histórico do volume.

   Dica: Se você decidir restaurar o banco de dados V7.1, esse arquivo será necessário.
8. Salve uma cópia do arquivo de opções do servidor, normalmente denominado `dsmserv.opt`. O arquivo está no diretório de instância do servidor.
9. Evite a atividade no servidor desativando novas sessões. Emita os comandos administrativos a seguir:

   ```
   disable sessions client
   disable sessions server
   ```
10. Verifique se existe alguma sessão e notifique os usuários de que o servidor será interrompido. Para verificar sessões existentes, emita o comando administrativo a seguir:

    ```
    query session
    ```
11. Cancele as sessões emitindo o comando administrativo a seguir:

    ```
    cancel session all
    ```

Este comando cancela todas as sessões, exceto para sua sessão atual.

12. Pare o servidor emitindo o comando administrativo a seguir:

```
halt
```

13. Verifique se o servidor está encerrado e nenhum processo está em execução.

    Emita o seguinte comando:

```
ps -ef | grep dsmserv
```

14. No diretório de instância do servidor de sua instalação, localize o arquivo NODELOCK e mova-o para outro diretório, no qual você está salvando arquivos de configuração.

    O arquivo NODELOCK contém as informações sobre licença anteriores para a sua instalação. Essas informações sobre licença são substituídas quando a atualização é concluída.

Instalando o servidor e verificando o upgrade

Para concluir o processo de upgrade do servidor para a V8.1, deve-se instalar o servidor V8.1. Em seguida, verifique se o upgrade foi bem-sucedido, iniciando a instância do servidor.

Antes de Iniciar

Você deve ter efetuado logon no sistema usando o ID do usuário raiz.

É possível obter o pacote de instalação a partir de um site de download da IBM.

Configure o limite do usuário do sistema para o tamanho máximo do arquivo como ilimitado, para assegurar que os arquivos possam ser transferidos por download corretamente.

1. Para consultar o valor do tamanho máximo do arquivo, execute o comando a seguir:

```
ulimit -Hf
```

2. Se o limite do usuário do sistema para o tamanho máximo do arquivo não estiver configurado como ilimitado, altere a configuração para ilimitada concluindo as instruções na documentação para seu sistema operacional.

Sobre Esta Tarefa

Ao usar o software de instalação IBM Spectrum Protect, é possível instalar os componentes a seguir:

- Servidor

  Dica: O banco de dados (IBM Db2), o Global Security Kit (GSKit) e o IBM Java Runtime Environment (JRE) são instalados automaticamente quando você seleciona o componente do servidor.
- Idiomas do servidor
- Licença
- Dispositivos
- IBM Spectrum Protect for SAN
- Operations Center

Procedimento

1. Faça download do arquivo de pacote apropriado a partir de um dos websites a seguir:
   - Faça download do pacote do servidor a partir do Passport Advantage ou do Fix Central.
   - Para obter as informações mais recentes, atualizações e correções de manutenção, acesse o IBM Support Portal.
2. Execute as etapas a seguir:

a. Verifique se você tem espaço suficiente para armazenar os arquivos de instalação quando eles forem extraídos do pacote do produto. Para requisitos de espaço, consulte o documento de download para seu produto.

- IBM Spectrum Protect nota técnica 588021
- IBM Spectrum Protect Extended Edition nota técnica 588023
- IBM Spectrum Protect for Data Retention nota técnica 588025

b. Faça download do arquivo de pacote para o diretório de sua opção. O caminho deve conter menos que 128 caracteres. Certifique-se de extrair os arquivos de instalação em um diretório vazio. Não extraia em um diretório que contenha arquivos extraídos anteriormente ou quaisquer outros arquivos.

Além disso, assegure-se de ter a permissão executável para o arquivo de pacote.

c. Se necessário, execute o comando a seguir para alterar as permissões de arquivo:

```
chmod a+x package_name.bin
```

em que *package_name* é como o exemplo a seguir:

```
8.1.x.000-IBM-SPSRV-AIX.bin
```

Nos exemplos, *8.1.x.000* representa o nível de liberação do produto.

d. Extraia os arquivos de instalação executando o seguinte command:

```
./package_name.bin
```

O pacote é grande. Portanto, a extração demora algum tempo.

3. Para assegurar que os assistentes do IBM Spectrum Protect funcionem corretamente, verifique se o seguinte comando está ativado: `lsuser`
4. Instale o software IBM Spectrum Protect, usando um dos métodos a seguir. Instale a licença do IBM Spectrum Protect durante o processo de instalação.

Dica: Se você tiver diversas instâncias do servidor em seu sistema, instale o software IBM Spectrum Protect apenas uma vez para atualizar todas as instâncias do servidor.

Assistente de instalação

Para instalar o servidor usando o assistente gráfico do IBM Installation Manager, siga as instruções em “Instalando o IBM Spectrum Protect Usando o Assistente de Instalação” na página 76.

Assegure-se de que seu sistema atende os pré-requisitos para usar o assistente de instalação. Em seguida, conclua o procedimento de instalação. Na janela **IBM Installation Manager**, clique no ícone **Atualizar** ou **Modificar**.

Instalando o servidor usando o modo do console

Para instalar o servidor usando o modo do console, siga as instruções em “Instalando o IBM Spectrum Protect Usando o Modo do Console” na página 77.

Revise as informações sobre como instalar o servidor no modo do console e, em seguida, conclua o procedimento de instalação.

Modo silencioso

Para instalar o servidor usando o modo silencioso, siga as instruções em “Instalando o IBM Spectrum Protect no Modo Silencioso” na página 78.

Revise as informações sobre como instalar o servidor no modo silencioso e, em seguida, conclua o procedimento de instalação.

Após instalar o software, você não tem que reconfigurar o sistema.

5. Corrija os erros detectados durante o processo de instalação.

   Se você instalou o servidor usando o assistente de instalação, será possível visualizar os logs de instalação usando a ferramenta IBM Installation Manager. Clique em **Arquivo** > **Visualizar Log**. Para coletar os arquivos de log, na ferramenta IBM Installation Manager, clique em **Ajuda** > **Dados de Exportação para Análise de Problemas**.

   Se você instalou o servidor usando o modo de console ou o modo silencioso, será possível visualizar os logs de erro no diretório de log do IBM Installation Manager, por exemplo:

   ```
   /var/ibm/InstallationManager/logs
   ```

6. Acesse o IBM Support Portal para obter correções. Clique em **Correções, atualizações e drivers** e aplique todas as correções aplicáveis.
7. Verifique se o upgrade foi bem-sucedido:
   a) Inicie a instância do servidor.
   b) Monitore as mensagens que o servidor emite conforme é iniciado. Observe as mensagens de erro e de aviso e resolva quaisquer problemas.
   c) Verifique se é possível se conectar ao servidor usando o cliente administrativo. Para iniciar uma sessão administrativa do cliente, execute o seguinte comando administrativo do IBM Spectrum Protect:

      ```
      dsmadmc
      ```

   d) Para obter informações sobre o sistema com upgrade feito, execute os comandos **QUERY**.
      Por exemplo, para obter informações consolidadas sobre o sistema, execute o seguinte comando administrativo do IBM Spectrum Protect: command:

      ```
      query system
      ```

      Para obter informações sobre o banco de dados, execute o seguinte comando administrativo do IBM Spectrum Protect command:

      ```
      query db format=detailed
      ```

8. Registre as licenças para os componentes do servidor IBM Spectrum Protect instalados no sistema executando o comando **REGISTER LICENSE** command:

   ```
   register license file=installation_directory/server/bin/component_name.lic
   ```

   onde: *installation_directory* especifica o diretório no qual você instalou o componente e *component_name* especifica a abreviação do componente.

   Por exemplo, se você instalou o servidor no diretório padrão, `/opt/tivoli/tsm`, execute o comando a seguir para registrar a licença:

   ```
   register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
   ```

   Por exemplo, se você instalou o IBM Spectrum Protect Extended Edition no diretório `/opt/tivoli/tsm`, execute o seguinte command:

   ```
   register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
   ```

   Por exemplo, se você instalou o IBM Spectrum Protect for Data Retention no diretório `/opt/tivoli/tsm`, execute o seguinte command:

   ```
   register license file=/opt/tivoli/tsm/server/bin/dataret.lic
   ```

   Restrição:

   Não é possível usar o servidor IBM Spectrum Protect para registrar licenças para os produtos a seguir:

- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for ERP
- IBM Spectrum Protect for Space Management

O comando **REGISTER LICENSE** não se aplica a essas licenças. O licenciamento para esses produtos é feito por clientes IBM Spectrum Protect.

9. Prepare o servidor para operações de backup de banco de dados automáticas e manuais.

   Para obter instruções, consulte “Preparando o servidor para operações de backup de banco de dados ” na página 100.
10. Opcional: Para instalar um pacote de idiomas adicional, use a função modificar do IBM Installation Manager.
11. Opcional: Para fazer upgrade para uma versão mais nova de um pacote de idiomas, use a função atualizar do IBM Installation Manager.
12. Para facilitar a resolução de problemas futuros, assegure-se de que haja espaço suficiente alocado para um core dump. Para obter mais informações, consulte a nota técnica 6357399.

O que Fazer Depois

É possível autenticar senhas com o servidor de diretório LDAP, ou autenticar senhas com o servidor IBM Spectrum Protect. Senhas que são autenticadas com o servidor de diretório LDAP podem fornecer segurança do sistema aprimorada.

Atualizando o Servidor em um Ambiente em Cluster

Para fazer upgrade de um servidor em um ambiente em cluster, deve-se concluir as tarefas de preparação e instalação. Os procedimentos variam, dependendo do sistema operacional e da liberação.

Procedimento

Siga o procedimento para o seu sistema operacional, a liberação de origem e a liberação de destino:

Tabela 18. Procedimentos para atualizar o servidor em um ambiente em cluster em um sistema operacional AIX

Liberação de origem	Liberação de destino	Procedimento
V8.1	Fix pack V8.1	“Aplicando um fix pack no IBM Spectrum Protect em um ambiente em cluster ” na página 105
V6.3 ou V7.1	V8.1	• “Fazendo upgrade do IBM Spectrum Protect de V7.1 para V8.1 em um ambiente em cluster com uma instância de banco de dados compartilhado” na página 114 • Fazendo upgrade em um ambiente em cluster do AIX com instâncias de banco de dados separadas
V5.5, V6.1, V6.2	V7.1.1 ou mais recente	IBM Spectrum Protect Processo de upgrade e migração - Perguntas mais frequentes

Fazendo upgrade do IBM Spectrum Protect de V7.1 para V8.1 em um ambiente em cluster com uma instância de banco de dados compartilhado

É possível fazer upgrade de um servidor do IBM Spectrum Protect da V7.1 para V8.1 em um ambiente em cluster no AIX com uma instância de banco de dados compartilhado. Dessa maneira, é possível aproveitar os novos recursos no IBM Spectrum Protect.

Antes de Iniciar

Assegure-se de reter a mídia de instalação da liberação de base do servidor V7.1 que você está atualizando. Se você instalou o IBM Spectrum Protect a partir de um DVD, certifique-se de que o DVD esteja disponível. Se você instalou o IBM Spectrum Protect a partir de um pacote transferido por download, certifique-se de que os arquivos transferidos por download estejam disponíveis. Se o upgrade falhar, e o módulo de licença do servidor for desinstalado, você deve reinstalar a licença a partir da mídia de instalação da liberação base do servidor.

Sobre Esta Tarefa

Use o procedimento a seguir quando o diretório de instâncias do IBM Db2 for compartilhado entre os nós no cluster. O diretório de instâncias do Db2 está no local a seguir:

```
/home/tsminst1/sqllib
```

Se o diretório de instâncias do Db2 não for compartilhado entre os nós, siga as instruções em “Fazendo upgrade em um ambiente em cluster com instâncias de banco de dados separadas” na página 116.

Procedimento

1. Faça backup do banco de dados usando o comando **BACKUP DB**.

   O método preferencial é usar um backup de captura instantânea, que cria um backup de banco de dados completo, sem interromper nenhum backup planejado.

   Por exemplo, é possível criar um backup de captura instantânea executando o comando a seguir:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Faça backup das informações de configuração do dispositivo em outro diretório executando o seguinte comando:

   ```
   backup devconfig filenames=file_name
   ```

   Em que *file_name* especifica o nome do arquivo no qual armazenar informações de configuração do dispositivo.

3. Faça backup do arquivo do histórico de volume em outro diretório executando o seguinte comando:

   ```
   backup volhistory filenames=file_name
   ```

   Em que *file_name* especifica o nome do arquivo no qual armazenar as informações do histórico do volume.

4. Salve uma cópia do arquivo de opções do servidor, geralmente denominado `dsmserv.opt`, que está no diretório de instância do servidor.
5. Pare todas as instâncias do servidor. Verifique se nenhum processo do servidor está em execução. Se você estiver usando o monitoramento de nível do aplicativo do servidor IBM Spectrum Protect, use a ferramenta de cluster para suspender o monitoramento do recurso do aplicativo **dsmserv**.
6. Verifique se o gerenciador do banco de dados não está executando para nenhuma instância. Determine se algum processo `db2sysc` está em execução.

O proprietário dos processos em execução indica quais instâncias estão ativas. Para cada proprietário da instância do servidor, execute o comando a seguir para parar o Db2:

```
db2stop
```

7. No nó primário, instale o servidor do IBM Spectrum Protect executando o comando **./install.sh**. Para obter instruções, consulte Capítulo 2, “Instalando os Componentes do Servidor”, na página 75.

   Após iniciar o assistente, clique no ícone **Atualizar** ou no ícone **Modificar** na janela **IBM Installation Manager**.
8. Inicie cada servidor no primeiro plano:
   a) Verifique se você efetuou login com o ID do proprietário da instância.
   b) Navegue para o diretório da instância e execute o comando a seguir:

      ```
      /opt/tivoli/tsm/server/bin/dsmserv
      ```

      Aguarde até ver o prompt do servidor, que indica que o servidor foi iniciado.
9. Pare o servidor para cada instância do IBM Spectrum Protect do qual está sendo feito upgrade. Emita o seguinte comando:

   ```
   halt
   ```

   Dica: Como o diretório de instâncias do Db2 é compartilhado entre os nós no cluster, você não precisa mover os recursos compartilhados para o nó secundário no cluster.
10. Em cada nó secundário do cluster, conclua as seguintes etapas:
    a) Instale o servidor do IBM Spectrum Protect executando o comando **./install.sh**. Para obter instruções, consulte Capítulo 2, “Instalando os Componentes do Servidor”, na página 75.
       i) Se estiver executando o assistente de instalação, clique no ícone **Atualizar** ou no ícone **Modificar** na janela **IBM Installation Manager**.
       ii) Se estiver executando o assistente de instalação, no painel **Credenciais da instância**, desmarque a caixa de seleção **Atualizar essa instância** para cada instância.
       iii) Se estiver instalando o servidor no modo do console, no prompt `Deseja atualizar esta instância?`, insira NO para cada instância.
       iv) Se estiver instalando o servidor no modo silencioso, especifique FALSE para o valor da variável `user.`*`instance_name`*`_update` para cada instância.
    b) Certifique-se de que cada servidor do IBM Spectrum Protect seja iniciado. Se você estiver usando o monitoramento de nível do aplicativo, use a ferramenta de cluster para iniciar o servidor.

       Para obter instruções sobre iniciar o servidor, consulte “Iniciando a Instância do Servidor” na página 95.
11. Registre as licenças para os componentes do servidor que estão instalados em seu sistema executando o comando **REGISTER LICENSE**:

    ```
    register license file=installation_directory/server/bin/component_name.lic
    ```

    Em que *installation_directory* especifica o diretório no qual você instalou o componente e *component_name* especifica a abreviação para o componente.

    Por exemplo, se você instalou o servidor no diretório padrão, `/opt/tivoli/tsm`, execute o comando a seguir para registrar a licença:

    ```
    register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
    ```

    Por exemplo, se você instalou o IBM Spectrum Protect Extended Edition no diretório `/opt/tivoli/tsm`, execute o comando a seguir:

    ```
    register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
    ```

Por exemplo, se você instalou o IBM Spectrum Protect for Data Retention no diretório `/opt/tivoli/tsm`, execute o comando a seguir:

```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

Restrição:

Não é possível usar o servidor IBM Spectrum Protect para registrar licenças para os produtos a seguir:

- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for ERP
- IBM Spectrum Protect for Space Management

O comando **REGISTER LICENSE** não se aplica a essas licenças. O licenciamento para esses produtos é feito por clientes IBM Spectrum Protect.

Fazendo upgrade em um ambiente em cluster com instâncias de banco de dados separadas

É possível fazer upgrade de um servidor em um ambiente em cluster no AIX com instâncias de banco de dados separadas. Dessa maneira, é possível aproveitar os novos recursos.

Antes de Iniciar

Assegure-se de reter a mídia de instalação da liberação de base do servidor V7.1 que você está atualizando. Se você instalou o IBM Spectrum Protect a partir de um DVD, certifique-se de que o DVD esteja disponível. Se você instalou o IBM Spectrum Protect a partir de um pacote transferido por download, certifique-se de que os arquivos transferidos por download estejam disponíveis. Se o upgrade falhar, e o módulo de licença do servidor for desinstalado, você deve reinstalar a licença a partir da mídia de instalação da liberação base do servidor.

Sobre Esta Tarefa

Use o procedimento a seguir quando o diretório de instâncias do IBM Db2 não for compartilhado entre os nós no cluster. O diretório de instâncias do Db2 está no local a seguir:

```
/home/tsminst1/sqllib
```

Se o diretório de instâncias do Db2 for compartilhado entre os nós no cluster, siga as instruções em "Fazendo upgrade do IBM Spectrum Protect de V7.1 para V8.1 em um ambiente em cluster com uma instância de banco de dados compartilhado" na página 114.

Procedimento

1. Faça backup do banco de dados usando o comando **BACKUP DB**.

   O método preferencial é usar um backup de captura instantânea, que cria um backup de banco de dados completo, sem interromper nenhum backup planejado.

   Por exemplo, é possível criar um backup de captura instantânea executando o comando a seguir:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Faça backup das informações de configuração do dispositivo em outro diretório executando o seguinte comando:

   ```
   backup devconfig filenames=file_name
   ```

   Em que *file_name* especifica o nome do arquivo no qual armazenar informações de configuração do dispositivo.

3. Faça backup do arquivo do histórico de volume em outro diretório executando o seguinte comando:

   ```
   backup volhistory filenames=file_name
   ```

   Em que *file_name* especifica o nome do arquivo no qual armazenar as informações do histórico do volume.
4. Salve uma cópia do arquivo de opções do servidor, geralmente denominado `dsmserv.opt`, que está no diretório de instância do servidor.
5. Pare todas as instâncias do servidor. Verifique se nenhum processo do servidor está em execução. Se você estiver usando o monitoramento de nível do aplicativo do servidor IBM Spectrum Protect, use a ferramenta de cluster para suspender o monitoramento do recurso do aplicativo **dsmserv**.
6. Verifique se o gerenciador do banco de dados não está executando para nenhuma instância. Determine se algum processo `db2sysc` está em execução.

   O proprietário dos processos em execução indica quais instâncias estão ativas. Para cada proprietário da instância do servidor, execute o comando a seguir para parar o Db2:

   ```
   db2stop
   ```
7. Assegure que os recursos compartilhados por todas as instâncias do IBM Spectrum Protect estejam no nó primário.

   Verifique se nenhum outro nó possui acesso de gravação nesses recursos durante o upgrade. Se o ambiente incluir diversas instâncias do servidor, os recursos compartilhados para todas as instâncias deverão ser acessíveis ao nó primário.
8. No nó primário, instale o servidor executando o comando **./install.sh**. Para obter instruções, consulte Capítulo 2, “Instalando os Componentes do Servidor”, na página 75.

   Depois de iniciar o assistente, na janela **IBM Installation Manager**, clique no ícone **Instalar**; não clique no ícone **Atualizar** ou **Modificar**. Para concluir o upgrade, deve-se instalar o servidor.
9. Inicie cada servidor no primeiro plano:
   a) Verifique se você efetuou login com o ID do proprietário da instância.
   b) Navegue para o diretório da instância e execute o comando a seguir:

      ```
      /opt/tivoli/tsm/server/bin/dsmserv
      ```

      Aguarde até ver o prompt do servidor, que indica que o servidor foi iniciado.
10. Pare o servidor para cada instância do IBM Spectrum Protect do qual está sendo feito upgrade. Execute o seguinte comando:

    ```
    halt
    ```
11. Em cada nó secundário do cluster, conclua as seguintes etapas:
    a) Mova todos os recursos compartilhados para o nó secundário.

       Se o ambiente incluir diversas instâncias do servidor, os recursos compartilhados para todas as instâncias deverão ser acessíveis aos nós secundários durante o upgrade.
    b) Pare todas as instâncias do servidor. Verifique se nenhum processo do servidor está em execução.
    c) Verifique se o gerenciador do banco de dados não está executando para nenhuma instância. Determine se algum processo `db2sysc` está em execução.

       O proprietário dos processos em execução indica quais instâncias estão ativas. Para cada proprietário da instância do servidor, execute o comando a seguir para parar o Db2:

       ```
       db2stop
       ```
    d) Instale o servidor executando o comando **./install.sh**. Para obter instruções, consulte Capítulo 2, “Instalando os Componentes do Servidor”, na página 75.
       i) Se você estiver usando o assistente de instalação, na janela **IBM Installation Manager**, clique no ícone **Instalar**; não clique no ícone **Atualizar** ou **Modificar**.

ii) Se estiver usando o assistente de instalação, na página **Credenciais da Instância**, marque a caixa de seleção **Configurar essa instância em um nó secundário do cluster** de cada instância que estiver configurando

iii) Se estiver instalando o servidor no modo do console, no prompt `Configurar esta instância em um nó secundário do cluster?`, insira YES para cada instância.

iv) Se estiver instalando o servidor no modo silencioso, especifique TRUE para o valor da variável `user.`*`instance_name`*`_secondaryNode` para cada instância.

e) Assegure-se de que cada servidor V8.1.7 tenha sido iniciado. Se você estiver usando o monitoramento de nível do aplicativo, use a ferramenta de cluster para iniciar o servidor.

Para obter instruções sobre como iniciar o servidor, consulte Iniciando a instância do servidor.

12. Registre as licenças para os componentes do servidor que estão instalados em seu sistema executando o comando **REGISTER LICENSE**:

```
register license file=installation_directory/server/bin/component_name.lic
```

Em que *installation_directory* especifica o diretório no qual você instalou o componente e *component_name* especifica a abreviação para o componente.

Por exemplo, se você instalou o servidor no diretório padrão, `/opt/tivoli/tsm`, execute o comando a seguir para registrar a licença:

```
register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
```

Por exemplo, se você instalou o IBM Spectrum Protect Extended Edition no diretório `/opt/tivoli/tsm`, execute o comando a seguir:

```
register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
```

Por exemplo, se você instalou o IBM Spectrum Protect for Data Retention no diretório `/opt/tivoli/tsm`, execute o comando a seguir:

```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

Restrição:

Não é possível usar o servidor IBM Spectrum Protect para registrar licenças para os produtos a seguir:

- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for ERP
- IBM Spectrum Protect for Space Management

O comando **REGISTER LICENSE** não se aplica a essas licenças. O licenciamento para esses produtos é feito por clientes IBM Spectrum Protect.

Capítulo 6. Referência: Comandos do IBM Db2 para bancos de dados do servidor IBM Spectrum Protect

Use esta lista como referência quando for orientado a emitir comandos do Db2 pelo suporte IBM.

Finalidade

Depois de usar os assistentes para instalar e configurar o IBM Spectrum Protect, raramente é necessário emitir comandos do Db2. Um conjunto limitado de comandos do Db2 que você pode usar ou ser solicitado a emitir são listados na tabela.

Essa lista é apenas material complementar e não é uma lista completa. Não há nenhuma implicação de que um administrador do IBM Spectrum Protect a usará diariamente ou de forma contínua. Amostras de alguns comandos são fornecidas. Detalhes de saída não são listados.

Para obter uma explicação integral dos comandos descritos aqui e de sua sintaxe, veja a documentação do produto Db2.

Tabela 19. Comandos do Db2

Comando	Descrição	Exemplo
db2icrt	Cria instâncias do Db2 no diretório inicial do proprietário da instância. **Dica:** O assistente de configuração do IBM Spectrum Protect cria a instância usada pelo servidor e banco de dados. Depois que um servidor está instalado e configurado por meio do assistente de configuração, o comando **db2icrt** geralmente não é usado. Esse utilitário está no diretório `DB2DIR/instance`, em que `DB2DIR` representa o local de instalação no qual a versão atual do sistema de banco de dados Db2 está instalado.	Crie manualmente uma instância do IBM Spectrum Protect.Insira o comando em uma linha: `/opt/tivoli/tsm/db2/instance/db2icrt -a server -u instance_name instance_name`
db2set	Exibe as variáveis do Db2.	Liste as variáveis do Db2: `db2set`
CATALOG DATABASE	Armazena informações de localização do banco de dados no diretório de banco de dados do sistema. O banco de dados pode ser localizado na estação de trabalho local ou em um servidor de partição do banco de dados remoto. O assistente de configuração do servidor cuida de qualquer catálogo necessário para usar o banco de dados do servidor. Execute este comando manualmente, depois que um servidor está configurado e em execução, apenas se algo no ambiente for alterado ou está danificado.	Catalogue o banco de dados: `db2 catalog database tsmdb1`
CONNECT TO DATABASE	Conecta-se a um banco de dados especificado para uso da interface da linha de comandos (CLI) uso.	Conecte-se ao banco de dados do IBM Spectrum Protect por meio de uma CLI do Db2: `db2 connect to tsmdb1`

Tabela 19. Comandos do Db2 (continuação)

Comando	Descrição	Exemplo

GET DATABASE CONFIGURATION	Retorna os valores das entradas individuais em um arquivo de configuração do banco de dados específico.
	Importante: Esse comando e os parâmetros são configurados e gerenciados diretamente pelo Db2. Eles estão listados aqui para fins informativos e um meio para visualizar as configurações existentes. Alterar essas configurações pelo suporte IBM ou por meio de boletins de serviço, como APARs ou documentos Técnicos (notas Técnicas). Não altere essas configurações manualmente. Alterá-las apenas na direção da IBM e apenas por meio do uso de procedimentos ou comandos do servidor IBM Spectrum Protect.
		Mostre as informações de configuração para um alias do banco de dados:
		`db2 get db cfg for tsmdb1`
		Recupere informações sobre configurações, como modo de log de configuração do banco de dados e manutenção.
		`db2 get db config for tsmdb1 show detail`

GET DATABASE MANAGER CONFIGURATION	Retorna os valores das entradas individuais em um arquivo de configuração do banco de dados específico. **Importante:** Esse comando e os parâmetros são configurados e gerenciados diretamente pelo Db2. Eles estão listados aqui para fins informativos e um meio para visualizar as configurações existentes. Alterar essas configurações pelo suporte IBM ou por meio de boletins de serviço, como APARs ou documentos Técnicos (notas Técnicas). Não altere essas configurações manualmente. Alterá-las apenas na direção da IBM e apenas por meio do uso de procedimentos ou comandos do servidor IBM Spectrum Protect.	Recupera informações de configuração para o gerenciador de banco de dados: `db2 get dbm cfg`
GET HEALTH SNAPSHOT	Recupera as informações de status de funcionamento para o gerenciador de banco de dados e seus bancos de dados. As informações retornadas representam uma captura instantânea do estado de funcionamento no momento em que o comando foi emitido. O IBM Spectrum Protect monitora o estado do banco de dados usando a captura instantânea de funcionamento e outros mecanismos fornecidos pelo Db2. Pode haver casos em que a captura instantânea de funcionamento ou outra documentação indique que um item ou recurso de banco de dados possa estar em um estado de alerta. Tal caso indica que a ação deve ser considerada para solucionar a situação. O IBM Spectrum Protect monitora a condição e responde de maneira apropriada. Nem todos os alertas declarados pelo banco de dados Db2 são concretizados.	Receba um relatório sobre os indicadores do monitor de funcionamento do Db2: `db2 get health snapshot for database on tsmdb1`

GRANT (Autoridades de Banco de Dados)	Concede as autoridades que se aplicam a todo o banco de dados, em vez de privilégios que se aplicam a objetos específicos dentro do banco de dados.	Conceder acesso para o ID de usuário itmuser:
		`db2 GRANT CONNECT ON DATABASE TO USER itmuser`
		`db2 GRANT CREATETAB ON DATABASE TO USER itmuser`

Tabela 19. Comandos do Db2 (continuação)

Comando	Descrição	Exemplo
RUNSTATS	Atualiza as estatísticas sobre as características de uma tabela e dos índices associados ou visualizações estatísticas. Essas características incluem número de registros, número de páginas e comprimento médio do registro. Para consultar uma tabela, emita este utilitário depois de atualizar ou reorganização da tabela. A visualização deve ser ativada para otimização antes de sua estatísticas poder ser usada para otimizar uma consulta. Uma visualização que é ativada para otimização é conhecida como uma visualização de estatística. Use a instrução Db2 **ALTER VIEW** para ativar uma visualização para otimização. Emita o utilitário **RUNSTATS** quando as mudanças em tabelas subjacentes afetam substancialmente as linhas retornadas pela visualização. **Dica:** O servidor configura o Db2 para executar o comando **RUNSTATS** conforme necessário.	Atualize as estatísticas em uma única tabela. `db2 runstats on table SCHEMA_NAME.TABLE_NAME with distribution and sampled detailed indexes all`
SET SCHEMA	Muda o valor do registro especial **CURRENT SCHEMA**, em preparação para emitir comandos SQL diretamente pela CLI do Db2. **Dica:** Um registro especial é uma área de armazenamento definida para um processo de aplicativo pelo gerenciador de bancos de dados. Ele é usado para armazenar as informações que podem ser referenciadas em instruções SQL.	Configure o esquema para IBM Spectrum Protect: `db2 set schema tsmdb1`
START DATABASE MANAGER	Inicia os processos de segundo plano da instância do gerenciador de banco de dados atual processos em segundo plano. O servidor inicia e para a instância e o banco de dados sempre que o servidor é iniciado e parado. **Importante:** Permita que o servidor gerencie o início e a parada da instância e do banco de dados a menos que seja direcionado de outra forma pelo suporte IBM.	Inicie o gerenciador do banco de dados: `db2start`

Tabela 19. Comandos do Db2 (continuação)

Comando	Descrição	Exemplo
STOP DATABASE MANAGER	Para a instância atual do gerenciador de banco de dados. A menos que seja explicitamente interrompido, o gerenciador do banco de dados continua ativo. Esse comando não para a instância do gerenciador de banco de dados se os aplicativos estão conectados a bancos de dados. Se não houver conexões com o banco de dados, mas houver conexões de instância, o comando forçará as conexões de instância a parar primeiro. Em seguida, ele para o gerenciador do banco de dados. Esse comando também desativa as ativações de banco de dados pendentes antes de parar o gerenciador de banco de dados. Este comando não é válido em um cliente. O servidor inicia e para a instância e o banco de dados sempre que o servidor é iniciado e parado. **Importante:** Permita que o servidor gerencie o início e a parada da instância e do banco de dados a menos que seja direcionado de outra forma pelo suporte IBM.	Pare o gerenciador do banco de dados: `db2 stop dbm`

Capítulo 7. Desinstalando o IBM Spectrum Protect

É possível usar os procedimentos a seguir para desinstalar o IBM Spectrum Protect. Antes de remover o IBM Spectrum Protect, assegure-se de não perder seus dados de backup e archive.

Antes de Iniciar

Conclua as seguintes etapas antes de desinstalar o IBM Spectrum Protect:

- Execute um backup completo do banco de dados.
- Salve uma cópia dos arquivos de histórico do volume e de configuração de dispositivos.
- Armazene os volumes de saída em um local seguro.

Sobre Esta Tarefa

É possível desinstalar o IBM Spectrum Protect usando alguns dos métodos a seguir: um assistente gráfico, a linha de comandos no modo do console ou modo silencioso.

O que Fazer Depois

Reinstale os componentes do IBM Spectrum Protect.

Desinstalando o IBM Spectrum Protect Usando um Assistente Gráfico

É possível desinstalar o IBM Spectrum Protect usando o assistente de instalação do IBM Installation Manager.

Procedimento

1. Inicie o Installation Manager.

   No diretório em que o Installation Manager está instalado, acesse o subdiretório `eclipse` (por exemplo, `/opt/IBM/InstallationManager/eclipse`) e emita o comando a seguir:

   ```
   ./IBMIM
   ```

2. Clique em **Desinstalar**.
3. Selecione **Servidor IBM Spectrum Protect** e clique em **Avançar**.
4. Clique em **Desinstalar**.
5. Clique em **Concluir**.

Desinstalando o IBM Spectrum Protect no Modo do Console

Para desinstalar o IBM Spectrum Protect usando a linha de comandos, é necessário executar o programa de desinstalação do IBM Installation Manager a partir da linha de comandos com o parâmetro para o modo do console.

Procedimento

1. No diretório onde o IBM Installation Manager está instalado, acesse o seguinte subdiretório:

   ```
   eclipse/tools
   ```

   Por exemplo:

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```

2. No diretório `tools`, emita o comando a seguir:

   ```
   ./imcl -c
   ```
3. Para desinstalar, insira 5.
4. Escolha desinstalar do grupo de pacotes do IBM Spectrum Protect.
5. Insira N para Avançar.
6. Escolha desinstalar o pacote do servidor IBM Spectrum Protect.
7. Insira N para Avançar.
8. Insira U para Desinstalar.
9. Insira F para Concluir.

Desinstalando o IBM Spectrum Protect no Modo Silencioso

Para desinstalar o IBM Spectrum Protect em modo silencioso, é necessário executar o programa de desinstalação do IBM Installation Manager a partir da linha de comandos com os parâmetros para o modo silencioso.

Antes de Iniciar

Você pode utilizar um arquivo de resposta para fornecer entrada de dados para instalar silenciosamente osIBM Spectrum Protect componentes do servidor. IBM Spectrum Protect inclui um arquivo de resposta como amostra, `uninstall_response_sample.xml`, no diretório de `entrada` onde o pacote de instalação está extraído. Esses arquivos contém valores padrão para ajudar você a evitar quaisquer avisos desnecessários.

Se você quiser desinstalar todos os componentes IBM Spectrum Protect, deixe `modify="false"` configurado para cada componente no arquivo de resposta. Se você não deseja instalar um componente, configure o valor para `modify="true"`.

Se você quiser customizar um arquivo de resposta, é possível modificar as opções que estão no arquivo. Para obter informações sobre arquivos de resposta, acesse Arquivos de respostas.

Procedimento

1. No diretório onde o IBM Installation Manager está instalado, acesse o seguinte subdiretório:

   ```
   eclipse/tools
   ```

   Por exemplo:

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```
2. No diretório `tools`, emita o comando a seguir, em que *response_file* representa o caminho do arquivo de resposta, incluindo o nome do arquivo:

   ```
   ./imcl -input response_file -silent
   ```

   O comando a seguir é um exemplo:

   ```
   ./imcl -input /tmp/input/uninstall_response.xml -silent
   ```

Desinstalando e Reinstalando o IBM Spectrum Protect

Se você planejar reinstalar manualmente o IBM Spectrum Protect em vez de usar o assistente, há diversas etapas para preservar os nomes das instâncias do servidor e os diretórios do banco de dados. Durante a desinstalação, quaisquer instâncias do servidor anteriormente configuradas são removidas, mas os catálogos de banco de dados dessas instâncias ainda existem.

Sobre Esta Tarefa

Para desinstalar manualmente e reinstalar o IBM Spectrum Protect, conclua as etapas a seguir:

1. Faça uma lista de suas instâncias do servidor atual antes de continuar com a desinstalação. Execute o seguinte comando:

   ```
   /opt/tivoli/tsm/db2/instance/db2ilist
   ```

2. Execute os seguintes comandos para cada instância do servidor:

   ```
   db2 attach para
   instance_name
   mostrar detalhes de db2 get dbm cfg
   db2 detach
   ```

   Mantenha um registro do caminho do banco de dados para cada instância.

3. Desinstale o IBM Spectrum Protect.
4. Ao desinstalar qualquer versão suportada do IBM Spectrum Protect, incluindo um fix pack, um arquivo de instância é criado. O arquivo de instância é criado para ajudar a reinstalar o IBM Spectrum Protect. Verifique esse arquivo e use as informações quando for solicitado a você as credenciais da instância ao reinstalar. No modo de instalação silenciosa, você fornece essas credenciais usando a variável `INSTANCE_CRED`.

   Você pode localizar o arquivo de instância no seguinte local:

   `/etc/tivoli/tsm/instanceList.obj`

5. Reinstale o IBM Spectrum Protect.

   Se o arquivo `instanceList.obj` não existir, será necessário recriar suas instâncias de servidor, usando as etapas a seguir:

   a. Recrie as instâncias do servidor.

      Dica: O assistente de instalação configura as instâncias do servidor, mas você deve verificar se elas existem. Se não existirem, você deve configurá-las manualmente.

   b. Catalogue o banco de dados. Efetue login em cada instância do servidor como o usuário da instância, um de cada vez, e emita os seguintes comandos:

      ```
      db2 catalog database tsmdb1
      db2 attach para
      instance_name
      db2 update dbm cfg using dftdbpath instance_directory
      db2 detach
      ```

   c. Verifique se a instância de servidor foi criada com êxito.Emita este comando:

      ```
      /opt/tivoli/tsm/db2/instance/db2ilist
      ```

   d. Verifique se o IBM Spectrum Protect reconhece a instância do servidor listando seus diretórios. O seu diretório inicial aparecerá se você não o alterar. O seu diretório de instâncias aparecerá se você usou o assistente de configuração. Emita este comando:

      ```
      db2 list database directory
      ```

      Se você vir TSMDB1 listado, é possível iniciar o servidor.

Desinstalando o IBM Installation Manager

É possível desinstalar o IBM Installation Manager, se você não tiver mais nenhum dos produtos que foram instalados por IBM Installation Manager.

Antes de Iniciar

Antes de desinstalar o IBM Installation Manager, deve-se assegurar que todos os pacotes que foram instalados pelo IBM Installation Manager estão desinstalados. Feche o IBM Installation Manager antes de iniciar o processo de desinstalação.

Para visualizar os pacotes instalados, emita o comando a seguir a partir de uma linha de comandos:

```
cd /opt/IBM/InstallationManager/eclipse/tools
./imcl listInstalledPackages
```

Procedimento

Para desinstalar o IBM Installation Manager, conclua as etapas a seguir:

- 1. Abra uma linha de comandos e mude os diretórios para `/var/ibm/InstallationManager/uninstall`.
  2. Emita o seguinte comando:

     ```
     ./uninstall
     ```

     Restrição: Deve-se ter efetuado login no sistema como o ID do usuário `root`.

Parte 2. Instalando e Fazendo Upgrade do Operations Center

O IBM Spectrum Protect Operations Center é a interface baseada na web para gerenciar seu ambiente de armazenamento.

Antes de Iniciar

Antes de instalar e configurar o Operations Center, revise as informações a seguir:

- Requisitos do sistema para o Centro de operações
  - Requisitos do computador do Centro de operações
  - Requisitos do servidor hub e spoke
  - Requisitos do sistema operacional
  - Requisitos do navegador da web
  - Requisitos de linguagem
  - Requisitos e limitações para o IBM Spectrum Protect
- IDs de administrador que o Centro de operações requer
- IBM Installation Manager
- Lista de verificação de instalação
- Obtendo o pacote de instalação do Operations Center

Sobre Esta Tarefa

Tabela 20 na página 127 lista os métodos para instalar e desinstalar o Operations Center e indica onde localizar instruções associadas.

Para obter informações sobre como fazer upgrade do Operations Center, consulte Fazendo upgrade do Operations Center.

Tabela 20. Métodos para Instalar ou Desinstalar o Operations Center

Comunicação	**Instruções**
Assistente gráfico	• Instalando o Operations Center usando um assistente gráfico • Desinstalando o Operations Center usando um assistente gráfico
Modo do console	• Instalando o Operations Center em modo do console • Desinstalando o Operations Center em modo do console
Modo silencioso	• Instalando o Operations Center em modo silencioso • “Desinstalando o Operations Center no Modo Silencioso” na página 199

Capítulo 8. Planejando a instalação do Operations Center

Antes de instalar o Operations Center, você deve entender os requisitos do sistemas, os IDs do administrador que o Operations Center requer e as informações que você deve fornecer ao programa de instalação.

Sobre Esta Tarefa

No Operations Center, é possível gerenciar os aspectos principais a seguir do ambiente de armazenamento:

- Clientes e Servidores IBM Spectrum Protect
- Serviços como backup e restauração, archive e recuperação, e migração e rechamada
- Conjuntos de armazenamentos e dispositivos de armazenamento

O Operations Center inclui os recursos a seguir:

Interface com o usuário para vários servidores
É possível usar o Operations Center para gerenciar um ou mais servidores IBM Spectrum Protect.

Em um ambiente com diversos servidores, é possível designar um servidor como um *servidor do hub* e os outros como *servidores spoke*. O servidor do hub pode receber informações de alertas e status a partir dos servidores spoke e apresentar informações em uma visualização consolidada no Operations Center.

Monitoramento de Alerta

Um *alerta* é uma notificação de um problema relevante no servidor e é acionado por uma mensagem do servidor. É possível definir quais mensagens do servidor acionam os alertas e apenas as mensagens são relatadas como alertas no Operations Center ou em um email.

Esse monitoramento de alerta pode ajudar a identificar e controlar problemas relevantes no servidor.

Interface da linha de comandos conveniente
O Operations Center inclui uma interface da linha de comandos para recursos avançados e configuração.

Requisitos do sistema para Centro de Operações

Antes de instalar o Operations Center, assegure-se de que seu sistema atenda aos requisitos mínimos.

Use a Calculadora de Requisitos do Sistema do Centro de Operações para estimar os requisitos do sistema para executar o Centro de Operações e os servidores spoke e de hub que são monitorados pelo Centro de Operações.

Requisitos que são verificados durante a instalação

Tabela 21 na página 129 lista os requisitos obrigatórios que são verificados durante a instalação e indica onde localizar informações adicionais sobre esses requisitos.

Tabela 21. Requisitos que são verificados durante a instalação

Requirement	Detalhes
Requisito mínimo de memória	“Requisitos do Computador do Centro de Operações” na página 130

Tabela 21. Requisitos que são verificados durante a instalação (continuação)	
Requirement	**Detalhes**
Requisito do sistema operacional	“Requisitos de Sistema Operacional” na página 133
Nome do host para o computador no qual o Operations Center será instalado	“Lista de Verificação da Instalação” na página 138
Requisitos para o diretório de instalação Operations Center	“Lista de Verificação da Instalação” na página 138

Requisitos do Computador do Centro de Operações

É possível instalar o Operations Center em um computador que também está executando o servidor do IBM Spectrum Protect ou em um computador diferente. Se você instalar o Operations Center no mesmo computador que um servidor, esse computador deverá atender aos requisitos do sistema para ambos o Operations Center e o servidor.

Requisitos do recurso

Os recursos a seguir são necessários para executar o Operations Center:

- Um núcleo do processador
- 4 GB de memória
- 1 GB de espaço em disco

Os servidores de hub e spoke que são monitorados pelo Operations Center precisam de recursos adicionais, conforme descrito em “Requisitos de Servidor de Hub e Servidor Spoke” na página 130.

Requisitos de Servidor de Hub e Servidor Spoke

Ao abrir o Operations Center pela primeira vez, deve-se associar o Operations Center a um servidor IBM Spectrum Protect designado como o *servidor do hub*. Em um ambiente de vários servidores, é possível conectar-se a outros servidores, denominados *servidores spoke*, para o servidor do hub.

Os servidores spoke enviam alertas e informações de status para o servidor do hub. O Operations Center mostra uma visualização consolidada de alertas e informações de status para o servidor de hub e quaisquer servidores spoke.

Se apenas um servidor for monitorado pelo Operations Center, esse servidor ainda será chamado de um servidor do hub, mesmo que nenhum servidor spoke esteja conectado a ele.

O Tabela 22 na página 131 indica a versão do servidor IBM Spectrum Protect que deve estar instalada no servidor do hub e em cada servidor spoke gerenciado pelo Operations Center.

Tabela 22. Requisitos da versão do servidor IBM Spectrum Protect para servidores hub e spoke

Operations Center	Versão no servidor do hub	Versão em cada servidor spoke
V8.1.12	V8.1.12	V8.1.10 ou mais recente ========== ou Liberação V7.1.10 ou uma versão 7 mais recente **Restrições:** • Algumas funções do Operations Center não estão disponíveis para os servidores que usam uma versão anterior à V8.1.12. • Um servidor spoke não pode usar uma versão que seja posterior à versão no servidor do hub.

Para obter informações sobre requisitos de compatibilidade de servidores hub e spoke para outras versões do Operations Center, consulte a nota técnica 496593.

Número de servidores spoke que um servidor do hub pode suportar

O número de servidores spoke que um servidor do hub pode suportar depende da configuração e da versão do IBM Spectrum Protect em cada servidor spoke. No entanto, uma diretriz geral é que um servidor do hub em um sistema separado, como uma VM, pode suportar dezenas de servidores spoke V7.1 ou mais recentes.

Dicas para Projetar a Configuração do Servidor do Hub e Spoke

No design da configuração de hub e spoke, considere especialmente os requisitos de recurso para monitoramento de status. Além disso, considere como deseja agrupar os servidores spoke e de hub e se deseja usar vários servidores de hub.

Use a Calculadora de Requisitos do Sistema do Centro de Operações para estimar os requisitos do sistema para executar o Centro de Operações e os servidores spoke e de hub que são monitorados pelo Centro de Operações.

Principais Fatores que Afetam o Desempenho

Os fatores a seguir têm impacto mais significativo no desempenho do Operations Center:

- O processador e a memória no computador no qual o Operations Center está instalado
- Os recursos do sistema dos servidores do hub e spoke, incluindo o sistema de disco que está em uso para o banco de dados do servidor do hub
- O número de nós clientes e espaços de arquivos de máquina virtual que são gerenciados pelos servidores hub e spoke
- A frequência na qual os dados são atualizados no Operations Center

Como agrupar os servidores spoke e de hub

Considere agrupar servidores de hub e spoke por local geográfico. Por exemplo, gerenciar os servidores dentro do mesmo datacenter pode ajudar a evitar problemas que são causados por firewalls ou por largura da banda da rede inadequada entre diferentes locais. Se necessário, é possível dividir mais os servidores de acordo com uma ou mais das características a seguir:

- O administrador que gerencia os servidores
- A entidade organizacional que financia os servidores
- Sistema operacional do servidor
- O idioma no qual os servidores são executados

  Dica: Se os servidores spoke e de hub não estiverem sendo executados no mesmo idioma, você pode ver o texto corrompido no Operations Center.

Como agrupar os servidores spoke e do hub em uma configuração corporativa

Em uma configuração corporativa, uma rede de servidores IBM Spectrum Protect é gerenciada como um grupo. As mudanças feitas no *gerenciador de configuração* podem ser distribuídas automaticamente para um ou mais *servidores gerenciados* na rede.

O Operations Center normalmente registra e mantém um ID de administrador dedicado nos servidores do hub e spoke. Este *administrador de monitoramento* deve sempre ter a mesma senha em todos os servidores.

Se você usar uma configuração corporativa, será possível melhorar o processo pelo qual as credenciais do administrador são sincronizadas em servidores spoke. Para melhorar o desempenho e a eficiência de manter o ID do administrador de monitoramento, conclua as seguintes etapas:

1. Designe o servidor do gerenciador de configuração como o servidor do hub do Operations Center. Durante a configuração do servidor do hub, um ID de administrador de monitoramento chamado IBM-OC-*hub_server_name* é registrado.
2. No servidor do hub, inclua o ID de administrador de monitoramento em um perfil de configuração corporativa novo ou existente. Emita o comando NOTIFY SUBSCRIBERS para distribuir o perfil para os servidores gerenciados.
3. Inclua um ou mais dos servidores gerenciados como servidores spoke do Operations Center.

O Operations Center detecta essa configuração e permite que o gerenciador de configuração distribua a atualize o ID de administrador de monitoramento nos servidores spoke.

Quando usar múltiplos servidores do hub

Se você tiver mais de 10 a 20 servidores spoke V6.3.4, ou se limitações de recurso requererem que o ambiente seja particionado, será possível configurar diversos servidores do hub e conectar um subconjunto dos servidores spoke a cada servidor do hub.

Restrições:

- Um único servidor não pode ser tanto um servidor do hub quanto um servidor spoke.
- Cada servidor spoke pode ser designado a apenas um servidor do hub.
- Cada servidor do hub requer uma instância separada do Operations Center, cada uma da qual tem um endereço da web separado.

Dicas para Escolher um Servidor do Hub

Para o servidor do hub, deve-se escolher um servidor que possua recursos adequados e esteja localizado para o mínimo de latência de rede de roundtrip.

Atenção: Não use o mesmo servidor como o servidor do hub para diversos Centros de operações.

Use as diretrizes a seguir para decidir qual servidor designar como o servidor do hub:

Escolha um servidor pouco carregado

Considere um servidor que tenha uma carga leve para operações, como backup de cliente e archive. Um servidor com carga leve também é uma boa opção como o sistema host para o Operations Center.

Assegure-se de que o servidor tenha os recursos para manipular sua carga de trabalho do servidor típica e a carga de trabalho estimada para atuar como o servidor do hub.

Localize o servidor para latência mínima de rede de roundtrip

Localize o servidor do hub de modo que a conexão de rede entre o servidor do hub e os servidores spoke tenha uma latência roundtrip que não seja maior que 5 ms. Esta latência pode normalmente ser alcançada quando os servidores estão na mesma rede local (LAN).

As redes que são ajustadas de modo insuficiente, são muito usadas por outros aplicativos ou possuem latência de roundtrip muito mais alta do que 5 ms podem degradar as comunicações entre os servidores do hub e spoke. Por exemplo, latências roundtrip de 50 ms ou mais altas podem resultar em tempos limites de comunicação que fazem com que os servidores spoke se desconectem ou se reconectem ao Operations Center. Latências tão altas podem ser experimentadas em comunicações de redes de longa distância (WAN).

Se servidores spoke estão uma longa distância do servidor do hub e experimentam desconexões frequentes no Operations Center, é possível aumentar o valor da opção **ADMINCOMMTIMEOUT** em cada servidor para reduzir o problema.

Verifique se o servidor do hub atende aos requisitos de recurso para monitoramento de status

O monitoramento de status requer recursos extras em cada servidor no qual ele está ativado. Os recursos que são necessários dependem principalmente do número de clientes que são gerenciados pelos servidores do hub e spoke. Menos recursos são usados em um servidor do hub com um servidor spoke V7.1 ou posterior do que em um servidor do hub com um servidor spoke V6.3.4.

Verifique se o servidor do hub atende aos requisitos de recurso para uso do processador, espaço de banco de dados, espaço de log de archive e capacidade de operações de E/S por segundo (IOPS).

Um servidor do hub com capacidade de IOPS alta pode manipular uma quantidade maior de dados de status recebidos de servidores spoke. O uso dos dispositivos de armazenamento a seguir para o banco de dados do servidor do hub pode ajudar a atender esta capacidade:

- Uma unidade de estado sólido (SSD) de nível corporativo
- Um dispositivo de armazenamento em disco de SAN externo com diversos volumes ou diversos eixos sob cada volume

Em um ambiente com menos de 1000 clientes, considere estabelecer uma capacidade de linha de base de 1000 IOPS para o banco de dados do servidor do hub se o servidor do hub gerenciar quaisquer servidores spoke.

Determine se seu ambiente requer diversos servidores do hub

Se mais de 10.000 a 20.000 nós clientes e espaços no arquivo de máquina virtual forem gerenciados por um conjunto de servidores do hub e spoke, os requisitos de recurso poderão exceder o que o servidor do hub tem disponível, especialmente se os servidores spoke forem servidores V6.3.4. Considere designar um segundo servidor como um servidor do hub e mover os servidores spoke para o novo servidor do hub para balancear a carga.

Requisitos de Sistema Operacional

O Operations Center está disponível para sistemas AIX, Linux e Windows.

É possível executar o Operations Center nos sistemas a seguir.

O suporte do Operations Center para os sistemas AIX e Linux é limitado somente às versões Big Endian, a menos que seja indicado de outra forma.

- Sistemas AIX:
  - IBM AIX V7.1 Technology Level 5 e Service Pack 5 ou mais recente
  - IBM AIX V7.2 Technology Level 3 e Service Pack 3 ou mais recente

Para obter as informações de requisitos mais atualizadas, consulte Requisitos de software e de hardware.

Requisitos do Navegador da Web

O Operations Center pode ser executado em navegadores da web Apple, Google, Microsoft e Mozilla.

Para melhor visualização do Operations Center no navegador da web, assegure-se de que a resolução da tela para o sistema esteja configurada para um mínimo de 1024 X 768 pixels.

Para desempenho ideal, use um navegador da web que possua bom desempenho de JavaScript e ative o armazenamento em cache do navegador.

O Operations Center pode ser executado nos navegadores da web a seguir:

- Apple Safari no iPad

  Restrição: Se o Apple Safari estiver executando no iOS 8.x ou iOS 9.x, não será possível usar um certificado autoassinado para comunicação segura com o Operations Center sem configuração extra do certificado. Use um certificado de autoridade de certificação (CA) ou configure o certificado autoassinado conforme necessário. Para obter instruções, consulte a Nota técnica http://www.ibm.com/support/docview.wss?uid=swg21963153.
- Google Chrome 54 ou mais recente
- Microsoft Internet Explorer 11 ou mais recente
- Mozilla Firefox ESR 45 ou versão 48 ou mais recente

A comunicação entre o Operations Center e o navegador da web deve ser protegida usando o protocolo de Segurança da Camada de Transporte (TLS) 1.2. O navegador da web deve suportar o TLS 1.2 e o TLS 1.2 deve estar ativado. O navegador da web exibirá um erro de SSL se ele não atender a esses requisitos.

Para obter as informações de requisitos mais atualizadas, consulte Requisitos de software e de hardware.

Requisitos de Idioma

Por padrão, o Operations Center usa o idioma que o navegador da web usa. Entretanto, o processo de instalação usa o idioma que o sistema operacional usa. Verifique se o navegador da web e o sistema operacional estão configurados para o idioma necessário.

Tabela 23. Os valores do idioma Operations Center que você pode usar nos sistemas AIX

idioma	**Valor de opção de idioma**
Chinês, Simplificado	zh_CN
Chinês, Simplificado (UTF-8)	ZH_CN
Chinês, Tradicional (Big5)	Zh_TW
Chinês, Tradicional (UTF-8)	ZH_TW
Chinês, Tradicional (euc_tw)	zh_TW
Inglês	en_US
Inglês (UTF-8)	EN_US
Francês	fr_FR
Francês (UTF-8)	FR_FR
Alemão	de_DE
Alemão (UTF-8)	DE_DE
Italiano	it_IT
Italiano (UTF-8)	IT_IT
Japonês (EUC)	ja_JP

Tabela 23. Os valores do idioma Operations Center que você pode usar nos sistemas AIX (continuação)	
idioma	**Valor de opção de idioma**
Japonês (PC)	Ja_JP
Japonês (UTF-8)	JA_JP
Coreano	ko_KR
Coreano (UTF-8)	KO_KR
Português, Brasileiro	pt_BR
Português do Brasil (UTF-8)	PT_BR
Russo	ru_RU
Russo (UTF-8)	RU_RU
Espanhol	es_ES
Espanhol (UTF-8)	ES_ES

Requisitos e limitações do IBM Spectrum Protect

O IBM Spectrum Protect é um componente que você instala em clientes de backup-archive para coletar informações de diagnóstico como arquivos de log de cliente. Antes de instalar o serviço de gerenciamento de cliente no sistema, deve-se entender os requisitos e limitações.

Na documentação do serviço de gerenciamento de cliente, o *sistema do cliente* é o sistema no qual o cliente de backup-archive é instalado.

As informações de diagnóstico podem ser coletadas somente a partir de clientes Linux e Windows, mas os administradores podem visualizar as informações de diagnóstico no Operations Center nos sistemas operacionais AIX, Linux ou Windows.

Dica: Antes de instalar o serviço de gerenciamento de cliente, assegure-se de que uma conexão bem-sucedida tenha sido estabelecida entre o cliente de backup e archive e o servidor. O arquivo de armazenamento confiável do servidor usado pelo cliente não tem o certificado Secure Sockets Layer (SSL) do servidor até que o sistema do cliente tenha se conectado ao servidor.

Requisitos para o serviço de gerenciamento de cliente

Verifique os seguintes requisitos antes de instalar o serviço de gerenciamento de cliente:

- Para acessar remotamente o cliente, o administrador do Operations Center deve ter autoridade do sistema ou um dos níveis de autoridade do cliente a seguir:
  - Autoridade de política
  - Autoridade do proprietário cliente
  - Autoridade de acesso ao nó cliente
- Assegure-se de que o sistema do cliente atenda aos seguintes requisitos:
  - O serviço de gerenciamento de cliente pode ser instalado apenas em sistemas do cliente que sejam executados em sistemas operacionais Linux ou Windows:
    - Sistemas operacionais Linux x86 de 64 bits que sejam suportados para o cliente de backup-archive
    - Sistemas operacionais Windows de 32 e 64 bits que sejam suportados para o cliente de backup-archive
  - A Segurança da Camada de Transporte (TLS) versão 1.2 ou mais recente deve ser instalada para a transmissão de dados entre o serviço de gerenciamento de cliente e o Operations Center. A autenticação básica é fornecida e as informações sobre dados e autenticação são criptografadas por

meio do canal do Secure Sockets Layer (SSL). TLS é instalado automaticamente juntamente com os certificados SSL necessários quando você instala o serviço de gerenciamento de cliente.

Iniciando no IBM Spectrum Protect Versão 8.1.11, o protocolo TLS 1.3 é ativado por padrão para proteger as comunicações entre os servidores, os clientes e os agentes de armazenamento. Para usar o TLS 1.3, ambas as partes na sessão de comunicação devem usar o TLS 1.3. Se uma das partes usar o TLS 1.2, ambas usarão o TLS 1.2 por padrão.

- Em sistemas do cliente Linux, deve-se ter autoridade de usuário raiz para instalar oserviço de gerenciamento de cliente.
- Para sistemas do cliente que podem ter diversos nós cliente, como sistemas do cliente Linux, assegure-se de que cada nome do nó seja exclusivo no sistema do cliente.

Dica: Após instalar o serviço de gerenciamento de cliente, não é necessário instalá-lo novamente porque o serviço pode descobrir diversos arquivos de opções do cliente.

Limitações do serviço de gerenciamento de cliente

O serviço de gerenciamento de cliente fornece os serviços básicos para coletar informações de diagnóstico a partir de clientes de backup-archive. As limitações a seguir existem para o serviço de gerenciamento de cliente:

- É possível instalar o serviço de gerenciamento de cliente somente em sistemas com clientes de backup-archive, incluindo clientes de backup-archive que estão instalados em nós do movedor de dados do IBM Spectrum Protect for Virtual Environments: Proteção de Dados para VMware.
- Não é possível instalar o serviço de gerenciamento de cliente em outros produtos ou componentes do cliente IBM Spectrum Protect que não possuem clientes de backup-archive.
- Se os clientes de backup-archive estiverem protegidos por um firewall, assegure-se de que haja conectividade entre o Operations Center e os clientes de backup-archive por meio do firewall, usando a porta configurada para o serviço de gerenciamento de cliente. A porta padrão é 9028, mas pode ser alterada.
- O serviço de gerenciamento de cliente varre todos os arquivos de log do cliente para localizar entradas durante as últimas 72 horas.
- A página **Diagnóstico** no Operations Center fornece informações básicas de resolução de problemas para clientes de backup-archive. No entanto, para alguns problemas de backup, poderá ser necessário acessar o sistema cliente e obter informações de diagnóstico adicionais.
- Se o tamanho combinado dos arquivos do log de erros e dos arquivos de log de planejamento do cliente em um sistema do cliente for maior que 500 MB, poderão ocorrer atrasos no envio de registros de log para o Operations Center. É possível controlar o tamanho dos arquivos de log ao ativar a remoção ou o agrupamento de arquivo de log especificando a opção de cliente **`errorlogretention`** ou **`errorlogmax`**.
- Se você usar o mesmo nome do nó cliente para se conectar a vários servidores IBM Spectrum Protect que estão instalados no mesmo servidor, é possível visualizar arquivos de log apenas para um dos nós cliente.

Para conhecer as possíveis atualizações relacionadas ao serviço de gerenciamento de cliente, consulte a nota técnica 534165.

Tarefas relacionadas

“Coletando informações de diagnóstico com o IBM Spectrum Protect” na página 176
O serviço de gerenciamento de cliente coleta as informações de diagnóstico sobre os clientes de backup-archive e disponibiliza-as para o Operations Center para a capacidade de monitoramento básico.

IDs de Administrador que o Operations Center Requer

Um administrador deve ter um ID e senha válidos no servidor do hub para efetuar login no Operations Center. Um ID de administrador também está designado ao Operations Center para que o Operations Center possa monitorar servidores.

O Operations Center requer os IDs de administrador IBM Spectrum Protect a seguir:

Os IDs de administrador que são registrados no servidor do hub
Qualquer ID de administrador que estiver registrado no servidor do hub pode ser usado para efetuar login no Operations Center. O nível de autoridade do ID determina quais tarefas podem ser concluídas. É possível criar novos IDs de administradores usando o comando **REGISTER ADMIN**.

Restrição: Para usar um ID de administrador em uma configuração de multisservidor, o ID deve ser registrado nos servidores de hub e spoke com a mesma senha e nível de autoridade.

Para gerenciar a autenticação para esses servidores, considere usar um dos métodos a seguir:

- Um servidor Protocolo LDAP
- As funções de configuração corporativa para distribuir automaticamente as mudanças nas definições de administrador.

ID de administrador de monitoramento
Ao configurar inicialmente o servidor do hub, um ID de administrador chamado IBM-OC-*server_name* será registrado com autoridade do sistema no servidor do hub e será associado à senha inicial que especificar. Este ID, que, às vezes, é chamado de *administrador de monitoramento*, é destinado para uso somente pelo Operations Center.

Não exclua, bloqueie ou modifique esse ID. O mesmo ID de administrador com a mesma senha é registrado nos servidores spoke incluídos. A senha é automaticamente alterada nos servidores hub e spoke a cada 90 dias. Não é necessário usar ou gerenciar essa senha.

Restrição: O Operations Center mantém o ID de administrador e a senha de monitoramento em servidores spoke, a menos que seja usada uma configuração corporativa para gerenciar essas credenciais. Para obter informações adicionais sobre como usar uma configuração corporativa para gerenciar as credenciais, consulte "Dicas para Projetar a Configuração do Servidor do Hub e Spoke" na página 131.

IBM Installation Manager

O Operations Center usa o IBM Installation Manager, que é um programa de instalação que pode usar repositórios de software remotos ou locais para instalar ou atualizar muitos produtos IBM.

Se a versão necessária do IBM Installation Manager não estiver instalada ainda, ela será instalada ou atualizada automaticamente ao instalar o Operations Center. Ela deve permanecer instalada no sistema para que o Operations Center possa ser atualizado ou desinstalado posteriormente conforme necessário.

A lista a seguir contém explicações de alguns termos que são usados no IBM Installation Manager:

Oferta
Uma unidade instalável de um produto do software.

A oferta Operations Center contém toda a mídia requerida pelo IBM Installation Manager para instalar o Operations Center.

Pacote
O grupo de componentes de software que são necessários para instalar uma oferta.

O pacote Operations Center contém os componentes a seguir:

- Programa de Instalação do IBM Installation Manager
- Oferta Operations Center

Grupo de pacotes
Um conjunto de pacotes que compartilham um diretório-pai comum.

Repositório
Uma área de armazenamento remota ou local para dados e outros recursos do aplicativo.

O pacote do Operations Center está armazenado em um repositório no IBM Fix Central.

Diretório de recursos compartilhados
Um diretório que contém arquivos de software ou plug-ins que são compartilhados por pacotes.

O IBM Installation Manager armazena arquivos relacionados à instalação no diretório de recursos compartilhados, incluindo arquivos que são usados para retroceder para uma versão anterior do Operations Center.

Lista de Verificação da Instalação

Antes de instalar o Operations Center, você deve verificar certas informações, como as credenciais de instalação e deve determinar a entrada para fornecer ao IBM Installation Manager para a instalação.

A lista de verificação a seguir destaca as informações que você deve verificar ou determinar antes de instalar o Operations Center, e Tabela 24 na página 138 descreve os detalhes dessas informações:

__ Verifique o nome do host para o computador no qual o Operations Center deve ser instalado.
__ Verifique as credenciais de instalação.
__ Determine o diretório de instalação do Operations Center, se você não deseja aceitar o caminho padrão.
__ Determine o diretório de instalação IBM Installation Manager, se você não deseja aceitar o caminho padrão.
__ Determine o número da porta a ser usado pelo servidor da web Operations Center, se você não deseja aceitar o número da porta padrão.
__ Determine a senha para comunicações seguras.

Tabela 24. Informações a serem verificadas ou determinadas antes de instalar o Operations Center

Informações	Detalhes
Nome do host para o computador no qual o Operations Center deve ser instalado.	O nome do host deve atender aos critérios a seguir: • Ele não deve conter os caracteres do conjunto de caracteres de byte duplo (DBCS) ou o caractere de sublinhado (_). • Embora o nome do host possa conter o caractere de hífen (-), ele não pode ter um hífen como o último caractere no nome.
Credenciais de Instalação	Para instalar o Operations Center, você deve usar a conta do usuário a seguir: • O usuário raiz

Diretório de Instalação do Operations Center	O Operations Center é instalado no subdiretório `ui` do diretório de instalação.
	O caminho a seguir é o caminho padrão para o diretório de instalação do Operations Center:
	• `/opt/tivoli/tsm`
	Por exemplo, se você usar esse caminho padrão, o Operations Center será instalado no diretório a seguir:
	`/opt/tivoli/tsm/ui`
	O caminho do diretório de instalação deverá atender aos critérios a seguir:
	• O caminho deve conter menos que 128 caracteres.
	• O caminho deve incluir somente caracteres ASCII.
	• O caminho não pode incluir caracteres de controle não exibíveis.
	• O caminho não pode incluir nenhum dos caracteres a seguir:
	`% | < > ' " $ & ; *`

Tabela 24. Informações a serem verificadas ou determinadas antes de instalar o Operations Center (continuação)

Informações	Detalhes
Diretório de Instalação IBM Installation Manager	O caminho a seguir é o caminho padrão para o diretório de instalação IBM Installation Manager: • `/opt/IBM/InstallationManager`
O número da porta que é usado pelo servidor da web Operations Center.	O valor para o número da porta segura (https) deve atender aos critérios a seguir: • O número deve ser um número inteiro no intervalo de 1024 a 65535. • O número não pode estar em uso ou ser alocado para outros programas. Se você não especificar um número de porta, o valor padrão será 11090. **Dicas:** • Embora seja necessário especificar um número inteiro no intervalo de 1024 a 65535, é possível configurar posteriormente o Operations Center para usar a porta segura TCP/IP padrão (porta 443). Para obter informações adicionais, consulte "Configurando o servidor da web do Operations Center para usar a porta segura padrão do TCP/IP" na página 154. • Se posteriormente você não se lembrar do número da porta que especificou, consulte o arquivo a seguir, em que *installation_dir* representa o diretório no qual o Operations Center está instalado: – *installation_dir*`/ui/Liberty/usr/servers/guiServer/bootstrap.properties` O arquivo `bootstrap.properties` contém as informações de conexão do servidor IBM Spectrum Protect.

Tabela 24. Informações a serem verificadas ou determinadas antes de instalar o Operations Center (continuação)

Informações	**Detalhes**
Senha para Comunicações Seguras	O Operations Center usa o Hypertext Transfer Protocol Secure (HTTPS) para se comunicar com os navegadores da web. O Operations Center requer comunicação segura entre o servidor e o Operations Center. Para proteger a comunicação, você deve incluir o certificado Segurança da Camada de Transporte (TLS) do servidor do hub para o arquivo de armazenamento confiável do Operations Center. O arquivo de armazenamento confiável do Operations Center contém o certificado que o Operations Center usa para comunicação HTTPS com navegadores da web. Durante a instalação do Operations Center, você cria uma senha para o arquivo de armazenamento confiável. Ao configurar a comunicação segura entre o Operations Center e o servidor do hub, você deve usar a mesma senha para incluir o certificado do servidor do hub para o arquivo de armazenamento confiável. A senha para o arquivo de armazenamento confiável deve atender aos critérios a seguir: • A senha deve conter um mínimo de 6 caracteres e um máximo de 64 caracteres. • A senha deve conter pelo menos os caracteres a seguir: – Uma letra maiúscula (A – Z) – Uma letra minúscula (a – z) – Um dígito (0 – 9) – Dois dos caracteres não alfanuméricos que estão listados na série seguinte: `~ @ # $ % ^ & * _ - + = ` |` `( ) { } [ ] : ; < > , . ? /`

Capítulo 9. Instalando o Operations Center

É possível instalar o Operations Center usando alguns dos métodos a seguir: um assistente gráfico, a linha de comandos em modo do console ou modo silencioso.

Antes de Iniciar

Não é possível configurar o Operations Center até que instale, configure e inicie o servidor IBM Spectrum Protect. Portanto, antes de instalar o Operations Center, instale o pacote do servidor apropriado, de acordo com os requisitos de versão do servidor em "Requisitos de Servidor de Hub e Servidor Spoke" na página 130.

É possível instalar o Operations Center em um computador com o servidor do IBM Spectrum Protect ou em um computador separado.

Obtendo o Pacote de Instalação Operations Center

É possível obter o pacote de instalação a partir de um site de download da IBM, como o IBM Passport Advantage ou o IBM Fix Central.

Sobre Esta Tarefa

Após obter o pacote de um site de download da IBM, deve-se extrair os arquivos de instalação.

Procedimento

Conclua as etapas a seguir para extrair os arquivos de instalação do Operations Center. Nas etapas a seguir, substitua o *version_number* pela versão do Operations Center que você está instalando.

a. Faça download do arquivo de pacote a seguir para o diretório de sua opção:

```
version_number.000
-IBM-SPOC-AIX.bin
```

b. Assegure-se de ter a permissão executável para o arquivo de pacote.

   Se necessário, altere as permissões de arquivo, emitindo o comando a seguir:

```
chmod a+x version_number.000-IBM-SPOC-AIX.bin
```

c. Emita o seguinte comando para extrair os arquivos de instalação:

```
 ./version_number.000-IBM-SPOC-AIX.bin
```

   O arquivo de pacote autoextrator é extraído para o diretório.

Instalando o Operations Center Usando um Assistente Gráfico

É possível instalar ou atualizar o Operations Center usando o assistente gráfico do IBM Installation Manager.

Antes de Iniciar

Se os arquivos RPM a seguir não estiverem instalados no computador, instale-os. Para obter instruções, consulte "Instalando Arquivos RPM para o Assistente Gráfico" na página 142.

```
atk-1.12.3-2.aix5.2.ppc.rpm
cairo-1.8.8-1.aix5.2.ppc.rpm
expat-2.0.1-1.aix5.2.ppc.rpm
```

```
fontconfig-2.4.2-1.aix5.2.ppc.rpm
freetype2-2.3.9-1.aix5.2.ppc.rpm
gettext-0.10.40-6.aix5.1.ppc.rpm
glib2-2.12.4-2.aix5.2.ppc.rpm
gtk2-2.10.6-4.aix5.2.ppc.rpm
libjpeg-6b-6.aix5.1.ppc.rpm
libpng-1.2.32-2.aix5.2.ppc.rpm
libtiff-3.8.2-1.aix5.2.ppc.rpm
pango-1.14.5-4.aix5.2.ppc.rpm
pixman-0.12.0-3.aix5.2.ppc.rpm
xcursor-1.1.7-3.aix5.2.ppc.rpm
xft-2.1.6-5.aix5.1.ppc.rpm
xrender-0.9.1-3.aix5.2.ppc.rpm
zlib-1.2.3-3.aix5.1.ppc.rpm
```

Procedimento

1. A partir do diretório no qual o arquivo do pacote de instalação do Operations Center foi extraído, emita o seguinte comando:

   ```
   ./install.sh
   ```
2. Siga as instruções do assistente para instalar o IBM Installation Manager e os pacotes do Operations Center.

   A seguinte mensagem pode ser exibida e o assistente de instalação pode ficar lento, se seu código de idioma usar a codificação UTF-8:

   ```
   Não é possível criar conjunto de fonte
   ```

   Se a mensagem for exibida, execute uma das seguintes ações:

   - Altere para um código de idioma que não usa a codificação UTF-8. Para valores de opção de idioma que não usam a codificação UTF-8, consulte “Requisitos de Idioma” na página 134.
   - Instale o Operations Center usando a linha de comandos no modo do console.
   - Instale o Operations Center no modo silencioso.

O que Fazer Depois

Consulte “Configurando o Operations Center” na página 149.

Instalando Arquivos RPM para o Assistente Gráfico

Antes seja possa usar o assistente gráfico do IBM Installation Manager para instalar o Operations Center, certos arquivos RPM devem estar instalados.

Sobre Esta Tarefa

Se os arquivos RPM listados em “Instalando o Operations Center Usando um Assistente Gráfico” na página 141 não estiverem instalados, você deve fazer download e instalar os arquivos.

Procedimento

1. Assegure-se de que haja pelo menos 150 MB de espaço livre no sistema de arquivos `/opt`.
2. No diretório em que o arquivo do pacote de instalação Operations Center é extraído, vá para o diretório `gtk`.
3. Para fazer o download automaticamente dos arquivos RPM para o diretório atual a partir do website do IBM AIX Toolbox for Linux Applications, emita o comando a seguir:

```
download-prerequisites.sh
```

4. Instale os arquivos emitindo o seguinte comando a partir do diretório que contém os arquivos:

```
rpm -Uvh *.rpm
```

Se uma mensagem indicar que um dos arquivos já está instalado no sistema, execute uma das seguintes ações:

- Emita o seguinte comando:

```
rpm -Uvh --force *.rpm
```

- Mova as versões anteriores dos arquivos para um diretório diferente e emita o comando **rpm** novamente, conforme mostrado no exemplo a seguir:

```
mkdir already-installed
mv gettext*.rpm already-installed
rpm -Uvh *.rpm
```

Instalando o Operations Center no Modo do Console

É possível instalar ou atualizar o Operations Center usando a linha de comandos no modo do console.

Procedimento

1. No diretório em que o arquivo de pacote de instalação é extraído, execute o programa a seguir:

```
./install.sh -c
```

2. Siga as instruções do console para instalar o Installation Manager e os pacotes do Operations Center.

O que Fazer Depois

Consulte “Configurando o Operations Center” na página 149.

Instalando o Operations Center no Modo Silencioso

É possível instalar ou fazer upgrade do Operations Center no modo silencioso. No modo silencioso, a instalação não envia as mensagens para um console, mas, em vez disso, armazena as mensagens e os erros nos arquivos de log.

Antes de Iniciar

Para fornecer entrada de dados ao usar o método de instalação silenciosa, é possível usar um arquivo de resposta. Os arquivos de resposta de amostra a seguir são fornecidos no diretório `input` em que o pacote de instalação é extraído:

`install_response_sample.xml`
Use este arquivo para instalar o Operations Center.

`update_response_sample.xml`
Use este arquivo para fazer upgrade do Operations Center.

Esses arquivos contêm valores padrão que podem ajudar a evitar quaisquer avisos desnecessários. Para usar esses arquivos, siga as instruções fornecidas nos arquivos.

Se você quiser customizar um arquivo de resposta, é possível modificar as opções que estão no arquivo. Para obter informações sobre arquivos de resposta, acesse Arquivos de respostas.

Procedimento

1. Crie um arquivo de resposta.

   É possível modificar o arquivo de resposta de amostra ou criar seu próprio arquivo.

   Dica: Para gerar um arquivo de resposta como parte de uma instalação de modo do console, conclua a seleção das opções de instalação de modo do console. Em seguida, no painel **Resumo**, insira `G` para gerar o arquivo de resposta de acordo com as opções selecionadas anteriormente.
2. Crie uma senha para o armazenamento confiável do Operations Center no arquivo de resposta.

   Se você está usando o arquivo `install_response_sample.xml`, inclua a senha na linha a seguir do arquivo, em que *mypassword* representa a senha:

   ```
   <variable name='ssl.password' value='mypassword'/>
   ```

   Para obter mais informações sobre esta senha, consulte "Lista de Verificação da Instalação" na página 138.

   Para criptografar a senha, siga as instruções em "Criptografando senhas em arquivos de resposta de instalação silenciosa" na página 144.

   Dica: Para fazer upgrade do Operations Center, a senha do armazenamento confiável não será necessária se você estiver usando o arquivo `update_response_sample.xml`.
3. Inicie a instalação silenciosa emitindo o comando a seguir a partir do diretório em que o pacote de instalação é extraído. O valor *response_file* representa o caminho do arquivo e o nome do arquivo:

   - ```
     ./install.sh -s -input response_file -acceptLicense
     ```

O que Fazer Depois

Consulte "Configurando o Operations Center" na página 149.

Criptografando senhas em arquivos de resposta de instalação silenciosa

Para aumentar a segurança durante uma instalação silenciosa do Operations Center, é possível criptografar a senha no arquivo de resposta. Somente uma senha (criptografada ou não criptografada) pode ser listada no campo de chave de dados no arquivo de resposta.

Antes de Iniciar

Abra o IBM Installation Manager. No diretório em que o IBM Installation Manager está instalado, acesse o subdiretório `eclipse`. Por padrão, o subdiretório está no local a seguir:

`/opt/IBM/InstallationManager/eclipse`

Procedimento

Para criptografar a senha no arquivo de resposta que é usado para instalar silenciosamente o Operations Center e assegurar que apenas uma senha seja usada no campo de chave de dados, conclua as etapas a seguir:

1. Se você estiver instalando o Operations Center como o usuário raiz, acesse o subdiretório de ferramentas. Por padrão, o subdiretório de ferramentas está no local a seguir:

   `/opt/IBM/InstallationManager/eclipse/tools`

   Se você estiver instalando o Operations Center como um usuário não raiz, acesse este subdiretório:

   `/home/non_root_user/IBM/InstallationManager/eclipse/tools`

   em que *non_root_user* é o ID do usuário da instância.
2. Emita o seguinte comando em uma única linha:
     ```

```
./IBMIM -silent -noSplash encryptString string_to_encrypt
>encrypted_pwd
```

em que *string_to_encrypt* é o valor que é criptografado e *encrypted_pwd* é o arquivo que contém o valor criptografado.

3. Abra o arquivo de senha criptografada e copie o valor para o campo de chave de dados do arquivo de resposta. Em seguida, remova o arquivo de senha criptografada, comentando-o.
4. Para remover a senha não criptografada do campo de chave de dados, conclua as etapas a seguir:
   a. Comente a senha não criptografada (`user.SSL_PASSWORD`) para que a linha de senha fique semelhante ao exemplo a seguir:

      ```
      <!-- <data key='user.SSL_PASSWORD' value='${ssl.password}'/> -->
      ```

   b. Remova as tags de comentário da senha criptografada (`user.SSL_PASSWORD_ENCRYPTED`) para que as linhas de senha fiquem semelhantes ao exemplo a seguir:

      ```
      <data key='user.enableSP800_131' value='${enable.SP800131a}'/>
       <data key='user.SSL_PASSWORD_ENCRYPTED' value='${ssl.password.encrypted}'/>
      ```

Restrição: Use somente um valor no campo de chave de dados no arquivo de resposta, seja a senha `user.SSL_PASSWORD` ou `user.SSL_PASSWORD_ENCRYPTED`. Deve-se comentar aquela que você não está usando, caso contrário, você receberá uma mensagem de erro e a instalação falhará.

Exemplo

Usando a ferramenta de linha de comandos do Installation Manager, criptografe a senha passw0rd. Salve o valor criptografado no arquivo `my_pwd.txt`. Emita o comando a seguir:

```
./IBMIM -silent -noSplash encryptString passw0rd > my_pwd.txt
```

em que o arquivo `my_pwd.txt` contém o valor criptografado, *rbN1IaMAWYYtQxLf6KdNyA==*:

```
<variable name='ssl.password.encrypted' value=' rbN1IaMAWYYtQxLf6KdNyA==' />
```

Capítulo 10. Atualizando o Operations Center

É possível fazer upgrade do Operations Center usando qualquer um dos métodos a seguir: um assistente gráfico, a linha de comandos no modo do console ou modo silencioso.

Antes de Iniciar

Antes de fazer upgrade do Operations Center, revise os requisitos do sistema e a lista de verificação de instalação. A nova versão do Operations Center pode ter requisitos e considerações adicionais ou diferentes da versão que está sendo usada atualmente.

Sobre Esta Tarefa

As instruções para upgrade do Operations Center são as mesmas que as instruções para instalar o Operations Center, com as exceções a seguir:

- Use a função **Atualizar** de IBM Installation Manager em vez da função **Instalar**.

  Dica: No IBM Installation Manager, o termo *atualizar* significa descobrir e instalar as atualizações e correções para os pacotes de software instalados. Nesse contexto, *atualizar* e *fazer upgrade* são sinônimos.
- Se você fizer upgrade do Operations Center no modo silencioso, será possível ignorar a etapa para criar uma senha para o arquivo de armazenamento confiável.

Capítulo 11. Introdução ao Operations Center

Antes que possa usar o Operations Center para gerenciar seu ambiente de armazenamento, deve configurá-lo.

Sobre Esta Tarefa

Após instalar o Operations Center, conclua as etapas de configuração básicas a seguir:

1. Designe o servidor do hub.
2. Inclua quaisquer servidores spoke.
3. Opcionalmente, configure alertas de email nos servidores do hub e spoke.

Figura 1 na página 149 ilustra uma configuração do Centro de Operações.

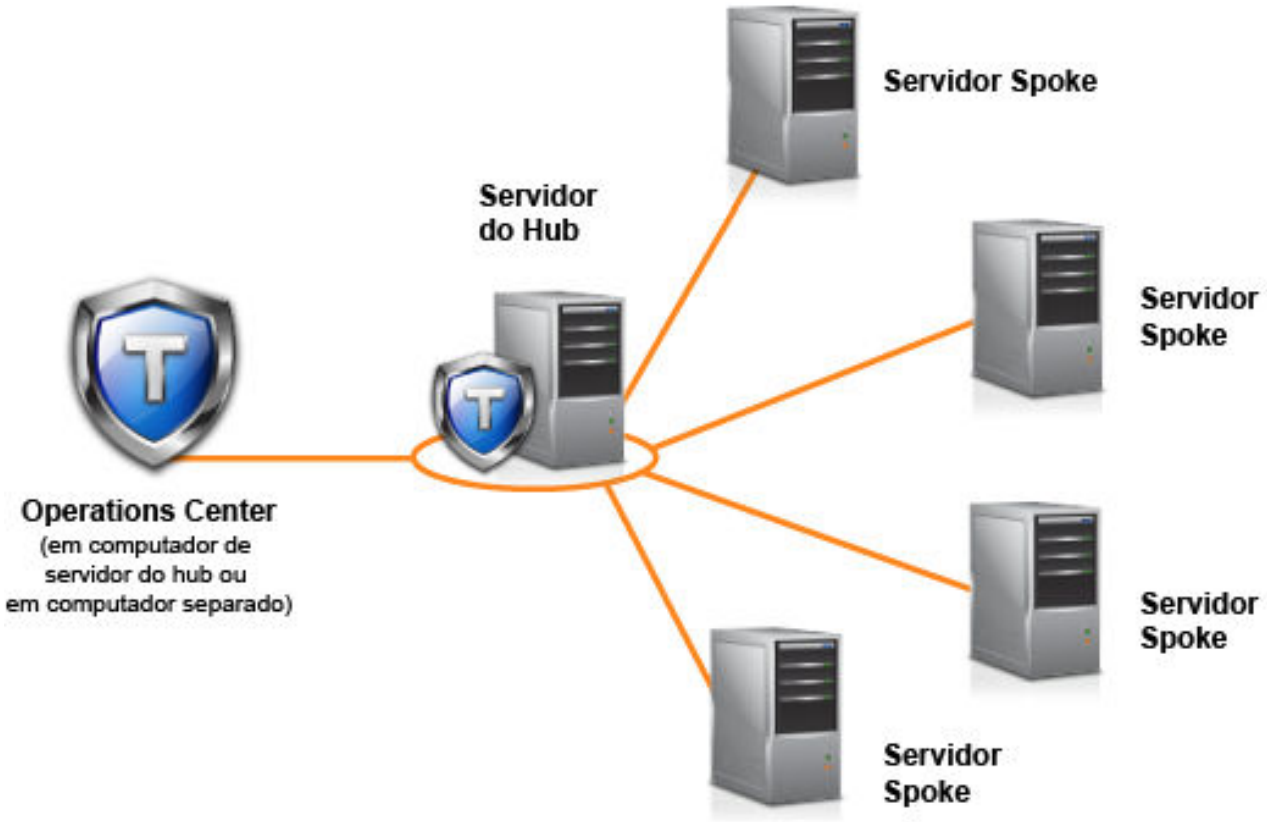


Figura 1. Exemplo de uma Configuração do Centro de Operações com os Servidores do Hub e Spoke

Configurando o Operations Center

Quando você abrir o Operations Center pela primeira vez, você deve configurá-lo para gerenciar seu ambiente de armazenamento. Deve-se associar o Operations Center ao servidor do IBM Spectrum Protect que está designado como o servidor do hub. É possível então conectar servidores IBM Spectrum Protect adicionais como servidores spoke.

Designando o Servidor do Hub

Ao conectar-se ao Operations Center pela primeira vez, você deve designar qual servidor IBM Spectrum Protect é o servidor do hub.

Antes de Iniciar

O Operations Center requer comunicação segura entre o servidor do hub e o Operations Center. Para proteger a comunicação, você deve incluir o certificado Segurança da Camada de Transporte (TLS) do servidor do hub para o arquivo de armazenamento confiável do Operations Center. Para obter informações adicionais, consulte “Protegendo as comunicações entre o Operations Center e o servidor do hub usando certificados autoassinados” na página 156.

Procedimento

Em um navegador da web, insira o endereço a seguir, em que *hostname* representa o nome do computador em que o Operations Center está instalado, e *secure_port* representa o número da porta que o Operations Center usa para comunicação HTTPS nesse computador:

```
https://hostname:secure_port/oc
```

Dicas:

- A URL faz distinção entre maiúsculas e minúsculas. Por exemplo, certifique-se de digitar "oc" em minúsculas, conforme indicado.
- Para obter mais informações sobre o número da porta, consulte a Lista de verificação de instalação.
- Se estiver se conectando ao Operations Center pela primeira vez, é necessário fornecer as seguintes informações:
  - Informações de conexão para o servidor que deseja designar como um servidor do hub
  - Credenciais de login para um ID de administrador que está definido para esse servidor
- Se o período de retenção de registro de eventos do servidor for menos que 14 dias, o período será automaticamente reconfigurado para 14 dias se você configurar o servidor como um servidor de hub.

O que Fazer Depois

Se você tem diversos servidores do IBM Spectrum Protect em seu ambiente, inclua os outros servidores como servidores spoke no servidor do hub.

Atenção: Não mude o nome de um servidor após ele ser configurado como um servidor de hub ou spoke.

Incluindo um Servidor spoke

Depois de configurar o servidor do hub para o Operations Center, é possível incluir um ou mais servidores spoke no servidor do hub.

Antes de Iniciar

A comunicação entre o servidor spoke e o servidor do hub deve ser protegida usando o protocolo de Segurança da Camada de Transporte (TLS). Para proteger a comunicação, inclua o certificado do servidor spoke no arquivo de armazenamento confiável do servidor do hub.

Procedimento

1. Na barra de menus Operations Center, clique em **Servidores**.

   A página **Servidores** se abre.

   Na tabela na página **Servidores**, um servidor pode ter um status de "Não monitorado". Este status significa que embora um administrador tenha definido esse servidor para o servidor do hub usando o comando **DEFINE SERVER**, o servidor ainda não está configurado como um servidor spoke.
2. Conclua uma das seguintes etapas:
   - Clique no servidor para destacá-lo e na barra de menus da tabela, clique em **Monitorar Spoke**.

- Se o servidor que você deseja incluir não for mostrado na tabela e a comunicação segura do SSL/TLS não for necessária, clique em **+ Spoke** na barra de menus da tabela.

3. Forneça as informações necessárias e conclua as etapas no assistente de configuração do spoke.

   Dica: Se o período de retenção de registro de eventos do servidor for menor que 14 dias, o período será automaticamente reconfigurado para 14 dias se você configurar o servidor como um servidor spoke.

Enviando Alertas de Email para Administradores

Um alerta é uma notificação de um problema relevante no servidor do IBM Spectrum Protect e é acionado por uma mensagem do servidor. Os alertas podem ser mostrados no Operations Center e podem ser enviados do servidor para administradores por email.

Antes de Iniciar

Antes de configurar a notificação por email para os administradores sobre os alertas, assegure que os requisitos a seguir sejam atendidos:

- Um servidor SMTP é necessário para enviar e receber alertas por e-mail e o servidor que envia os alertas por e-mail deve ter acesso ao servidor SMTP.

  Dica: Se o Operations Center for instalado em um computador separado, esse computador não precisará acessar o servidor SMTP.
- Um administrador deve ter privilégio no sistema para configurar a notificação por email.

Sobre Esta Tarefa

Uma notificação por email é enviada apenas para a primeira ocorrência de um alerta. Além disso, se for gerado um alerta antes de você configurar a notificação por email, nenhuma notificação por email será enviada para esse alerta.

É possível configurar a notificação por email das maneiras a seguir:

- Enviar notificação para alertas individuais
- Enviar resumos de alerta

Um resumo de alerta contém informações sobre os alertas atuais. O resumo inclui o número total de alertas, o número total de alertas ativos e inativos, o alerta mais antigo, o alerta mais recente e o alerta de ocorrência mais frequente.

É possível especificar um máximo de três administradores para receber resumos de alerta por email. Os resumos de alerta são enviados aproximadamente a cada hora.

Procedimento

Para configurar a notificação por email para administradores sobre alertas, conclua as etapas a seguir em cada hub e servidor spoke a partir dos quais deseja receber alertas de email:

1. Para verificar se o monitoramento de alerta está ativo, emita o comando a seguir:

   ```
   QUERY MONITORSETTINGS
   ```

2. Se a saída de comando indicar que o monitoramento de alerta está desligado, emita o comando a seguir. Caso contrário, continue na próxima etapa.

   ```
   SET ALERTMONITOR ON
   ```

3. Para ativar o envio de notificação por email, emita o comando a seguir:

   ```
   SET ALERTEMAIL ON
   ```

4. Para definir o servidor SMTP usado para enviar a notificação por email, emita o comando a seguir:

```
SET ALERTEMAILSMTPHOST host_name
```

5. Para especificar o número da porta para o servidor SMTP, emita o comando a seguir:

```
SET ALERTEMAILSMTPPORT port_number
```

   O número da porta padrão é 25.
6. Para especificar o endereço de email do emissor dos alertas, emita o comando a seguir:

```
SET ALERTEMAILFROMADDR email_address
```

7. Para cada ID de administrador que deve receber a notificação por email, emita um dos comandos a seguir para ativar a notificação por email e para especificar o endereço de email:

```
REGISTER ADMIN admin_name ALERT=YES EMAILADDRESS=email_address
```

```
UPDATE ADMIN admin_name ALERT=YES EMAILADDRESS=email_address
```

8. Escolhe uma das opções a seguir, ou ambas, e especifique os IDs de administrador para receber notificação por email:
   - Enviar notificação para alertas individuais

     Para especificar ou atualizar os IDs de administrador para receber a notificação por email para um alerta individual, emita um dos comandos a seguir:

     ```
     DEFINE ALERTTRIGGER message_number
     ADmin=admin_name1,admin_name2
     ```

     ```
     UPDATE ALERTTRIGGER message_number
     ADDadmin=admin_name3 DELadmin=admin_name1
     ```

     Dica: Na página **Configurar alertas** do Operations Center, é possível selecionar os administradores que receberão notificação por email.
   - Enviar resumos de alerta

     Para especificar ou atualizar os IDs de administrador para receber os resumos de alerta por email, emita o comando a seguir:

     ```
     SET ALERTSUMMARYTOADMINS admin_name1,admin_name2,admin_name3
     ```

   Se você deseja receber os resumos de alerta, mas não deseja receber notificação sobre os alertas individuais, conclua as etapas a seguir:

   a. Suspenda a notificação sobre alertas individuais, conforme descrito em "Suspendendo os Alertas de Email Temporariamente" na página 153.
   b. Assegure-se de que o respectivo ID de administrador esteja listado no comando a seguir:

      ```
      SET ALERTSUMMARYTOADMINS admin_name1,admin_name2,admin_name3
      ```

Enviando os alertas de email a vários administradores

O exemplo a seguir ilustra os comandos que fazem alertas para a mensagem ANR1075E serem enviados em um email para os administradores `myadmin`, `djadmin` e `csadmin`:

```
SET ALERTMONITOR ON
SET ALERTEMAIL ON
SET ALERTEMAILSMTPHOST mymailserver.domain.com
SET ALERTEMAILSMTPPORT 450
SET ALERTEMAILFROMADDR srvadmin@mydomain.com
UPDATE ADMIN myadmin ALERT=YES EMAILADDRESS=myaddr@anycompany.com
UPDATE ADMIN djadmin ALERT=YES EMAILADDRESS=djaddr@anycompany.com
```

```
UPDATE ADMIN csadmin ALERT=YES EMAILADDRESS=csaddr@anycompany.com
DEFINE ALERTTRIGGER anr0175e ADMIN=myadmin,djadmin,csadmin
```

Suspendendo os Alertas de Email Temporariamente

Em certas situações, talvez queira suspender os email alertas de email temporariamente. Por exemplo, talvez queira receber os resumos de alerta, mas suspender a notificação sobre os alertas individuais ou talvez queira suspender os alertas de email quando um administrador estiver em férias.

Antes de Iniciar

Configure a notificação por email para os administradores, conforme descrito em "Enviando Alertas de Email para Administradores" na página 151.

Procedimento

Suspenda a notificação por email para os alertas individuais ou para os resumos de alerta.

- Suspenda a notificação sobre os alertas individuais

  Use um dos métodos a seguir:

  Comando UPDATE ADMIN
  Para desligar a notificação por email para o administrador, emita o comando a seguir:

  ```
  UPDATE ADMIN admin_name ALERT=NO
  ```

  Para ativar a notificação por email novamente mais tarde, emita o comando a seguir:

  ```
  UPDATE ADMIN admin_name ALERT=YES
  ```

  Comando UPDATE ALERTTRIGGER
  Para evitar que um alerta específico seja enviado a um administrador, emita o comando a seguir:

  ```
  UPDATE ALERTTRIGGER message_number DELADMIN=admin_name
  ```

  Para iniciar o envio desse alerta ao administrador novamente, emita o comando a seguir:

  ```
  UPDATE ALERTTRIGGER message_number ADDADMIN=admin_name
  ```

- Suspenda a notificação sobre os resumos de alerta

  Para evitar que os resumos de alerta sejam enviados a um administrador, remova o ID do administrador da lista no comando a seguir:

  ```
  SET ALERTSUMMARYTOADMINS admin_name1,admin_name2,admin_name3
  ```

  Se um ID de administrador for listado no comando anterior, o administrador receberá os resumos de alerta por email, mesmo se a notificação sobre os alertas individuais for suspensa para o respectivo ID do administrador.

Incluindo texto customizado na tela de login

É possível incluir texto customizado, como Termos de uso do software de sua organização, na tela de login do Operations Center para que os usuários do Operations Center vejam o texto antes de inserirem seu nome de usuário e senha.

Procedimento

Para incluir texto customizado na tela de login, conclua as seguintes etapas:

1. No computador em que o Operations Center está instalado, acesse o seguinte diretório, em que *installation_dir* representa o diretório no qual o Operations Center está instalado:

installation_dir/ui/Liberty/usr/servers/guiServer

2. No diretório, crie um arquivo chamado `loginText.html` que contenha o texto que você deseja incluir na tela de login.

   Qualquer texto especial não ASCII deve ser codificado com UTF-8.

3. Revise o texto incluído na tela de login do Operations Center.

   Para abrir o Operations Center, insira o seguinte endereço em um navegador da web, em que *hostname* representa o nome do computador em que o Operations Center está instalado e *secure_port* representa o número da porta que o Operations Center usa para comunicação HTTPS nesse computador:

   ```
   https://hostname:secure_port/oc
   ```

Configurando o servidor da web do Operations Center para usar a porta segura padrão do TCP/IP

A porta 443 é a porta padrão para a comunicação segura do navegador da web. Se os usuários precisam acessar o Operations Center por meio de um firewall, é possível configurar o Operations Center para comunicar-se por meio dessa porta padrão. Dessa forma, é possível evitar a abertura de outra porta no firewall.

Sobre Esta Tarefa

Na instalação do Operations Center, o número da porta padrão para a comunicação segura entre o servidor da web do Operations Center e os navegadores da web é 11090. É possível aceitar essa porta padrão no momento da instalação ou especificar um número de porta diferente no intervalo de 1024 a 65535. Não é possível especificar um número de porta que seja inferior a 1024 no momento da instalação porque essas portas são reservadas para serviços de rede específicos.

Depois que o Operations Center é instalado, o servidor da web passa a atender na porta especificada para solicitações de navegadores da web. Se os usuários não conseguirem abrir o Operations Center porque a porta está bloqueada por um firewall, um administrador deverá abrir a porta para permitir que os navegadores se conectem. Em alguns ambientes de produção, pode ser mais eficiente usar a porta do sistema 443. Como essa porta do sistema é reservada para navegação na web segura, provavelmente ela já é uma porta aberta no firewall. Embora não seja possível especificar a porta 443 no momento da instalação, é possível especificar essa porta após a instalação.

Procedimento

Para configurar o servidor da web do Operations Center para usar a porta 443, conclua as etapas a seguir após a instalação do Operations Center:

1. Pare o servidor da web Operations Center.

   Para obter instruções sobre como parar o servidor da web, consulte “Iniciando e parando o servidor da web” na página 175.

2. Acesse o seguinte diretório, em que *installation_dir* representa o diretório no qual o Operations Center está instalado:

   installation_dir/ui/Liberty/usr/servers/guiServer

3. Abra o arquivo `bootstrap.properties` , que contém uma propriedade que especifica a porta que o servidor da web Operations Center usa para comunicação segura.

4. Atualize a propriedade `tsm.https.port` para especificar a porta 443:

   ```
   tsm.https.port=443
   ```

5. Salve e feche o arquivo `bootstrap.properties` .

6. Inicie o servidor da web Operations Center.

Deve-se iniciar o Operations Center como o usuário raiz. Se você não iniciar o Operations Center como o usuário raiz, o Operations Center não poderá se comunicar pela porta 443.

Para obter instruções de como iniciar o servidor da web Operations Center , consulte "Iniciando e parando o servidor da web" na página 175.

O que Fazer Depois

Notifique os usuários de que o Operations Center está usando a porta segura TCP/IP padrão. Geralmente, o usuário abre o Operations Center no navegador incluindo o número da porta na URL. Como a porta 443 é o padrão para a comunicação segura do navegador da web, os usuários não precisam especificar o número da porta na URL. Nesse caso, a URL a seguir pode ser usada, em que *hostname* especifica o nome do computador no qual o Operations Center está instalado:

```
https:hostname/oc/
```

Para obter instruções de como abrir o Operations Center, consulte "Abrindo o Operations Center" na página 175.

Ativando os serviços REST

Os aplicativos que usam serviços Representational State Transfer (REST) podem consultar e gerenciar o ambiente de armazenamento conectando-se ao Operations Center.

Sobre Esta Tarefa

Ative esse recurso para permitir que serviços REST interajam com servidores hub e spoke enviando chamadas para o endereço a seguir:

```
https://oc_host_name:port/oc/api
```

em que *oc_host_name* é o nome da rede ou endereço IP do sistema host do Operations Center e *port* é o número da porta do Operations Center. O número da porta padrão é 11090.

Para obter informações sobre os serviços REST que estão disponíveis para o Operations Center, consulte a Nota técnica http://www-01.ibm.com/support/docview.wss?uid=swg21997347 ou emita a chamada REST a seguir:

```
https://oc_host_name:port/oc/api/help
```

Procedimento

1. Na barra de menus do Operations Center, passe o mouse sobre o ícone de configurações  e clique em **Configurações**.
2. Na página Geral, selecione a caixa de seleção **Ativar API REST administrativa**.
3. Clique em **Salvar**.

Configurando para comunicação segura

O Operations Center usa o Hypertext Transfer Protocol Secure (HTTPS) para se comunicar com os navegadores da web. O protocolo de Segurança da Camada de Transporte (TLS) protege comunicações entre o Operations Center e o servidor do hub, e entre o servidor do hub e os servidores spoke associados.

Sobre Esta Tarefa

O TLS Versão 1.2 ou mais recente é necessário para a comunicação segura entre o servidor IBM Spectrum Protect e o Operations Center e entre o servidor do hub e os servidores spoke.

Protegendo as comunicações entre o Operations Center e o servidor do hub usando certificados autoassinados

Para proteger as comunicações entre o Operations Center e o servidor do hub, você deve incluir o certificado Segurança da Camada de Transporte (TLS) do servidor do hub para o arquivo de armazenamento confiável do Operations Center.

Antes de Iniciar

O arquivo de armazenamento confiável do Operations Center é um contêiner para certificados que o Operations Center pode acessar. Durante a instalação do Operations Center, deve-se criar uma senha para o arquivo de armazenamento confiável. Para comunicações seguras entre o Operations Center e o servidor do hub, deve-se usar a mesma senha para incluir o certificado do servidor do hub no arquivo de armazenamento confiável. Se você não se lembrar desta senha, agora deverá recriar e configurar o arquivo de armazenamento confiável. Para obter instruções, consulte Excluindo e redesignando a senha para o arquivo de armazenamento confiável do Operations Center.

A figura a seguir ilustra os componentes para configurar uma conexão Secure Sockets Layer (SSL) entre o servidor do hub e o Operations Center.

Sobre Esta Tarefa

Este procedimento fornece etapas para implementar comunicações seguras usando certificados autoassinados. Se você usar certificados assinados por uma autoridade de certificação (CA), consulte Protegendo as comunicações entre o Operations Center e o servidor do hub usando certificados assinados por CA.

Procedimento

1. Pare o servidor da web Operations Center.
2. Acesse a linha de comandos do sistema operacional no qual o Operations Center está instalado.
3. Inclua o certificado no arquivo de armazenamento confiável do Operations Center usando o utilitário **iKeycmd** ou o utilitário **iKeyman**.

   O utilitário **iKeycmd** é uma interface da linha de comandos e o utilitário **iKeyman** é a interface gráfica com o usuário do IBM Key Management.

   Os utilitários **iKeycmd** e **iKeyman** devem ser executados como o usuário raiz.

   Para incluir o certificado TLS usando a interface da linha de comandos, conclua as etapas a seguir:

   a) Acesse o seguinte diretório, em que *installation_dir* representa o diretório no qual o Operations Center está instalado:

   - *installation_dir*/ui/jre/bin

   b) Emita o comando **iKeycmd** para incluir o certificado `cert256.arm` do servidor no armazenamento confiável do Operations Center.

```
ikeycmd -cert -add
-db /installation_dir/ui/Liberty/usr/servers/guiServer/gui-truststore.jks
-file /server_instance_dir/cert256.arm
```

```
-label 'label_description'
-pw 'password' -type jks -format ascii -trust enable
```

onde:

installation_dir
O diretório no qual o Operations Center está instalado.

server_instance_dir
O diretório de instância do servidor IBM Spectrum Protect.

label description
A descrição que você designa ao rótulo.

senha
A senha que você criou quando instalou o Operations Center. Para reconfigurar a senha, desinstale o Operations Center, exclua o arquivo `.jks` e reinstale o Operations Center.

Para incluir o certificado usando a janela **IBM Key Management**, conclua as etapas a seguir:

a) Acesse o seguinte diretório, em que *installation_dir* representa o diretório no qual o Operations Center está instalado:

- *installation_dir*/ui/jre/bin

b) Abra a janela **IBM Key Management** emitindo o comando a seguir:

```
ikeyman
```

c) Clique em **Arquivo do Banco de Dados de Chave** > **Abrir**.

d) Na janela **Abrir**, clique em **Procurar** e acesse o diretório a seguir, em que *installation_dir* representa o diretório no qual o Operations Center está instalado:

- *installation_dir*/ui/Liberty/usr/servers/guiServer

e) No diretório `guiServer`, selecione o arquivo `gui-truststore.jks`.

f) Clique em **Abrir** e clique em **OK**.

g) Insira a senha para o arquivo de armazenamento confiável e clique em **OK**.

h) Na área **Conteúdo do Banco de Dados de Chaves** da janela **IBM Key Management**, clique na seta e selecione **Certificados de Assinante** na lista.

i) Clique em **Incluir**.

j) Na janela **Abrir**, clique em **Procurar** e acesse o diretório de instância do servidor do hub. Esse diretório contém o certificado `cert256.arm`.

Se você não puder acessar o diretório de instâncias do servidor do hub a partir da janela **Abrir**, conclua as etapas a seguir:

i) Use o FTP ou outro método de transferência de arquivos para copiar os arquivos `cert256.arm` do diretório de instância do servidor do hub para o diretório a seguir no computador no qual o Operations Center está instalado:

- *installation_dir*/ui/Liberty/usr/servers/guiServer

ii) Na janela **Abrir**, acesse o diretório `guiServer`.

k) Selecione o certificado `cert256.arm`.

Dica: O certificado selecionado deve ser configurado como o certificado padrão no arquivo do banco de dados de chaves do servidor do hub.

l) Clique em **Abrir** e clique em **OK**.

m) Insira um rótulo para o certificado.
Por exemplo, insira o nome do servidor do hub.

n) Clique em **OK**.

O certificado SSL do servidor do hub é incluído no arquivo de armazenamento confiável e o rótulo é exibido na área **Conteúdo do Banco de Dados de Chaves** da janela **IBM Key Management**.

o) Feche a janela **IBM Key Management**.

4. Inicie o servidor da web Operations Center.
5. Ao conectar-se ao Operations Center pela primeira vez, você será solicitado a identificar o endereço IP ou o nome da rede do servidor do hub, além do número da porta para comunicação com o servidor do hub. Insira o número da porta que é especificado pela opção do servidor TCPADMINPORT ou SSLTCPADMINPORT.

   Se o Operations Center foi configurado anteriormente, é possível revisar o conteúdo do arquivo `serverConnection.properties` para verificar as informações de conexão. O arquivo `serverConnection.properties` está no diretório a seguir no computador em que o Operations Center está instalado:

   - *`installation_dir`*`/ui/Liberty/usr/servers/guiServer`

O que Fazer Depois

Para configurar as comunicações TLS entre o servidor do hub e um servidor spoke, consulte "Protegendo a comunicação entre o servidor do hub e um servidor spoke" na página 159.

Tarefas relacionadas

"Excluindo e redesignando a senha para o arquivo de armazenamento confiável do Operations Center" na página 173

Para configurar a comunicação segura entre o Operations Center e o servidor do hub, você deve saber a senha para o arquivo de armazenamento confiável do Operations Center. Crie esta senha durante a instalação do Operations Center. Se você não souber a senha, é possível excluí-la e designar uma nova.

Protegendo as comunicações entre o Operations Center e o servidor do hub usando certificados assinados por CA

Se você usar os certificados assinados por CA para proteger o servidor do hub, os arquivos de certificado de autoridade de certificação raiz e intermediários enviados pela autoridade de certificação (CA) para uso no servidor do hub deverão ser incluídos ao arquivo de armazenamento confiável do Operations Center.

Antes de Iniciar

Certifique-se de que os seguintes pré-requisitos sejam atendidos:

- O arquivo de armazenamento confiável do Operations Center é um contêiner para certificados que o Operations Center pode acessar. Durante a instalação do Operations Center, deve-se criar uma senha para o arquivo de armazenamento confiável. Para proteger as comunicações entre o Operations Center e o servidor do hub, deve-se usar a mesma senha para incluir o certificado do servidor do hub no arquivo de armazenamento confiável. Se você não se lembrar dessa senha, o arquivo de armazenamento confiável deverá ser recriado e configurado. Para obter instruções, consulte "Excluindo e redesignando a senha para o arquivo de armazenamento confiável do Operations Center" na página 173.
- Você recebeu os certificados assinados por CA necessários para se conectar ao servidor por meio da autoridade de certificação e instalou-os no servidor. Consulte Configurando o servidor para aceitar conexões SSL.

A figura a seguir ilustra os componentes para configurar uma conexão do Secure Sockets Layer (SSL) entre o servidor do hub e o Operations Center.

Sobre Esta Tarefa

Para importar os certificados de autoridade de certificação raiz e intermediários de cada servidor IBM Spectrum Protect do servidor do hub para o Operations Center, conclua as etapas a seguir.

Dica: Se você usar os certificados autoassinados, instalados por padrão, consulte "Protegendo as comunicações entre o Operations Center e o servidor do hub usando certificados autoassinados" na página 156.

Procedimento

1. Navegue até a linha de comandos do sistema operacional no qual o Operations Center está instalado.
2. Na linha de comandos, altere o diretório para o local do keystore:

   installation_dir`/ui/Liberty/usr/servers/guiServer`

   em que *installation_dir* representa o diretório no qual o Operations Center está instalado.
3. Copie o certificado de autoridade de certificação raiz e os arquivos de certificado de autoridade de certificação intermediários para este local.

   Dica: Os arquivos de certificado foram copiados anteriormente para o local do servidor do hub.
4. Pare o servidor da web do Operations Center conforme descrito em "Iniciando e parando o servidor da web" na página 175.
5. Faça uma cópia de backup do arquivo de armazenamento confiável do Operations Center, se você tiver que reverter para a versão original. O arquivo de armazenamento confiável do Operations Center é denominado `gui-truststore.jks`.
6. Para concluir as etapas para receber o certificado assinado por CA, use um dos comandos a seguir:
   - Comando **ikeyman**: consulte "Recebendo o certificado assinado usando o IBM Key Management" na página 165 e acesse as etapas para receber o certificado assinado.
   - Comando **ikeycmd**: consulte "Recebendo o certificado assinado usando ikeycmd" na página 172 e acesse as etapas para receber o certificado assinado.
7. Inicie o servidor da web Operations Center.

O que Fazer Depois

Para configurar as comunicações TLS entre o servidor do hub e um servidor spoke, sigas as instruções em "Protegendo a comunicação entre o servidor do hub e um servidor spoke" na página 159.

Tarefas relacionadas

"Recebendo o certificado assinado" na página 165
A CA deve enviar a você o arquivo de certificado para inclusão no arquivo de armazenamento confiável.

Protegendo a comunicação entre o servidor do hub e um servidor spoke

Para proteger as comunicações entre o servidor do hub e um servidor spoke usando o protocolo de Segurança da Camada de Transporte (TLS), deve-se definir o certificado do servidor spoke para o servidor do hub e o certificado do servidor do hub para o servidor spoke. Você deve também configurar o Operations Center para monitorar o servidor spoke.

Sobre Esta Tarefa

O servidor hub recebe informações de status e alerta do servidor spoke e mostra essas informações no Operations Center. Para receber as informações de status e alerta do servidor spoke, o certificado do servidor spoke deve ser incluído no arquivo de armazenamento confiável do servidor do hub. Você deve também configurar o Operations Center para monitorar o servidor spoke.

Para ativar outras funções do Operations Center, como a implementação automática de atualizações de cliente, o certificado do servidor do hub deve ser incluído no arquivo de armazenamento confiável do servidor spoke.

Procedimento

1. Conclua as seguintes etapas para definir o certificado do servidor spoke para o servidor do hub:
   a) No servidor spoke, vá para o diretório da instância do servidor spoke.
   b) Verifique os certificados no arquivo do banco de dados de chave do servidor spoke. Emita o seguinte comando:

   ```
   gsk8capicmd_64 -cert -list -db cert.kdb -stashed
   ```

   c) Transfira com segurança o arquivo `cert256.arm` do servidor spoke para o servidor do hub.
   d) No servidor do hub, vá para o diretório da instância do servidor do hub.
   e) Defina o certificado do servidor spoke para o servidor do hub. Emita o comando a seguir a partir do diretório de instância do servidor do hub, em que *spoke_servername* é o nome do servidor spoke e *spoke_cert256.arm* é o nome do arquivo do certificado do servidor spoke:

   ```
   gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii -trust enable
    -label spoke_servername -file spoke_cert256.arm
   ```

2. Conclua as seguintes etapas para definir o certificado do servidor do hub para o servidor spoke:
   a) No servidor do hub, vá para o diretório da instância do servidor do hub.
   b) Verifique os certificados no arquivo do banco de dados de chave do servidor spoke. Emita o seguinte comando:

   ```
   gsk8capicmd_64 -cert -list -db cert.kdb -stashed
   ```

   c) Transfira o arquivo `cert256.arm` de maneira segura do servidor do hub para o servidor spoke.
   d) No servidor spoke, vá para o diretório da instância do servidor spoke.
   e) Defina o certificado do servidor do hub para o servidor spoke. Emita o comando a seguir a partir do diretório de instância do servidor spoke, em que *hub_servername* é o nome do servidor do hub e *hub_cert256.arm* é o nome do arquivo do certificado do servidor do hub:

   ```
   gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii -trust enable
    -label hub_servername -file hub_cert256.arm
   ```

3. Reinicie o servidor do hub e o servidor spoke.
4. Conclua as etapas a seguir para definir o servidor spoke para o servidor do hub e o servidor do hub para o servidor spoke.
   a) Emita os seguintes comandos no servidor do hub e no servidor spoke:

   ```
   SET SERVERPASSWORD server_password
   SET SERVERHLADDRESS ip_address
   SET SERVERLLADDRESS tcp_port
   ```

   b) No servidor do hub, emita o comando **DEFINE SERVER**, de acordo com o exemplo a seguir:

   ```
   DEFINE SERVER spoke_servername HLA=spoke_address
    LLA=spoke_SSLTCPADMINPort SERVERPA=spoke_serverpassword
   ```

   c) No servidor spoke, emita o comando **DEFINE SERVER**, de acordo com o exemplo a seguir:

```
DEFINE SERVER hub_servername HLA=hub_address
 LLA=hub_SSLTCPADMINPort SERVERPA=hub_serverpassword
```

Dica: Por padrão, a comunicação do servidor é criptografada, exceto quaando o servidor envia ou recebe dados do objeto. Dados do objeto são enviados e recebidos usando TCP/IP. Escolhendo não criptografar os dados do objeto, o desempenho do servidor é semelhante à comunicação sobre uma sessão TCP/IP e a sessão é segura. Para criptografar toda a comunicação com o servidor especificado, mesmo quando o servidor estiver enviando ou recebendo dados do objeto, especifique o parâmetro SSL=YES no comando **DEFINE SERVER**.

5. Conclua as seguintes etapas para configurar o Operations Center para monitorar o servidor spoke:
   a) Na barra de menus do Operations Center, clique em **Servidores**.

      O servidor spoke possui um status de "Não monitorado." Esse status significa que, embora este servidor tenha sido definido para o servidor do hub usando o comando **DEFINE SERVER**, o servidor ainda não está configurado como spoke.

   b) Clique no servidor spoke para destacar o item e, em seguida, clique em **Monitorar Spoke**.

Configurando a comunicação de SSL entre o Operations Center e navegadores da web

Durante a instalação do Operations Center, um certificado digital autoassinado é gerado e é então usado para sessões do navegador da web. É possível opcionalmente usar um certificado que seja assinado por um certificado de empresa terceirizada em vez do certificado autoassinado.

Sobre Esta Tarefa

O Operations Center sempre usa o protocolo HTTPS para se comunicar com navegadores da web. Toda a comunicação entre o navegador e o Operations Center é criptografada usando a versão 1.2 ou mais recente do protocolo TLS.

Por padrão, o certificado autoassinado é usado para criar a conexão segura entre o navegador e o Operations Center. Como o certificado é um certificado autoassinado, o navegador da web não consegue verificar a identidade do servidor e exibe um aviso. Os certificados autoassinados são normalmente usados para websites de intranet, em que o perigo de uma conexão interceptada e um servidor personificado pode não ser considerado uma ameaça séria. É possível efetuar bypass do aviso de segurança do navegador e usar o certificado autoassinado ou substituir o certificado autoassinado por um certificado de uma autoridade de certificação (CA) confiável.

Para usar o certificado autoassinado, nenhuma configuração adicional é necessária.

Para usar um certificado que é assinado por uma CA, deve-se concluir múltiplas etapas.

Procedimento

1. Crie uma solicitação de assinatura de certificado.
2. Envie a solicitação de assinatura de certificado para a autoridade de certificação para assinatura.
3. Inclua o certificado no arquivo de armazenamento confiável do Operations Center.

Criando um Certificate Signing Request

Para obter um certificado que seja assinado por terceiros, deve-se criar uma solicitação de assinatura de certificado (CSR) para enviar à CA.

Antes de Iniciar

O arquivo de armazenamento confiável do Operations Center é um contêiner para certificados SSL/TLS que o Operations Center pode acessar. O arquivo de armazenamento confiável contém o certificado que o Operations Center usa para comunicação HTTPS com navegadores da web.

Durante a instalação do Operations Center, crie uma senha para o arquivo de armazenamento confiável. Para trabalhar com o arquivo de armazenamento confiável, deve-se saber a senha do armazenamento confiável. Se você não se lembrar dessa senha, siga as instruções em "Excluindo e redesignando a senha para o arquivo de armazenamento confiável do Operations Center" na página 173.

Procedimento

Para criar uma CSR, conclua as etapas a seguir:

1. Na linha de comandos, altere o diretório para o local do keystore:

   installation_dir/ui/Liberty/usr/servers/guiServer

2. Crie uma solicitação de certificado usando o comando **ikeyman** ou o comando **ikeycmd**. O comando **ikeyman** abre a interface gráfica com o usuário do IBM Key Management e o **ikeycmd** é uma interface da linha de comandos.

   Dica: Talvez você precise especificar o caminho completo para o comando **ikeyman** ou **ikeycmd**. Os comandos estão localizados no diretório a seguir, em que *installation_dir* representa o diretório no qual o Operations Center está instalado:

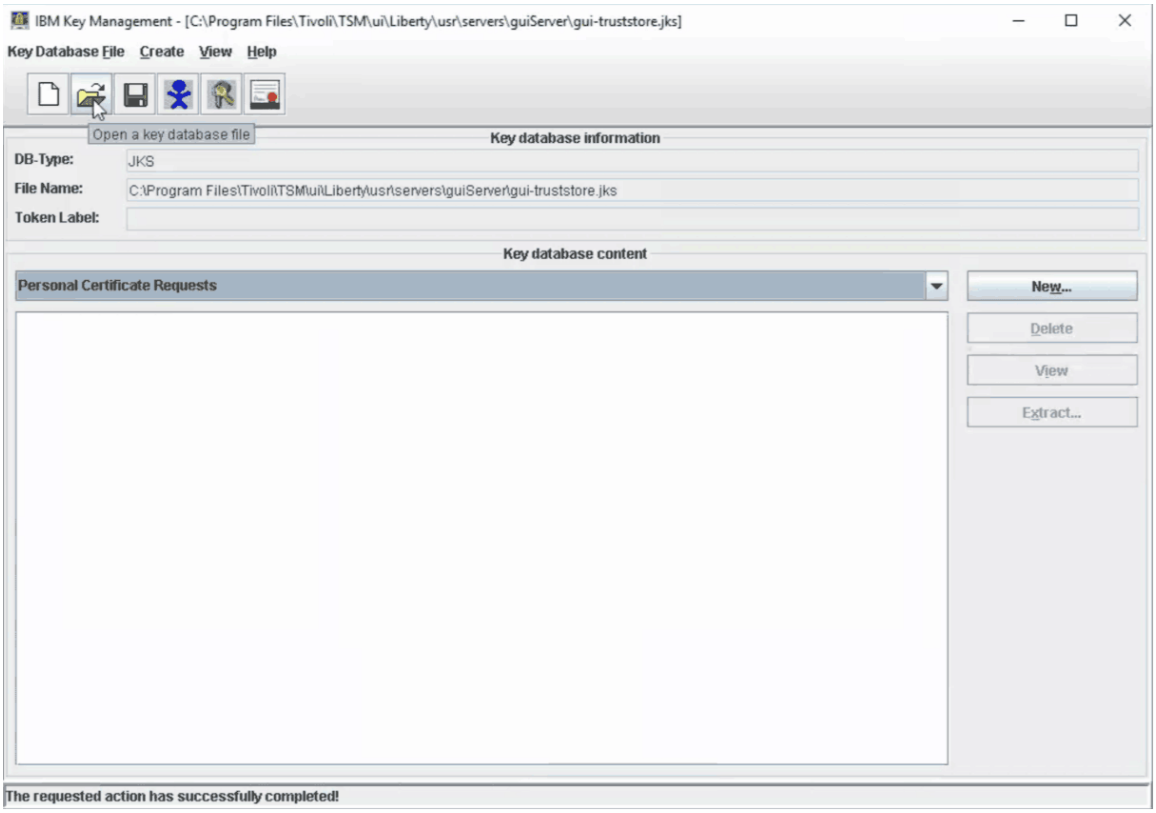
   installation_dir/ui/jre/bin

   - Para criar uma solicitação de certificado usando a interface gráfica com o usuário **ikeyman**, conclua as seguintes etapas:

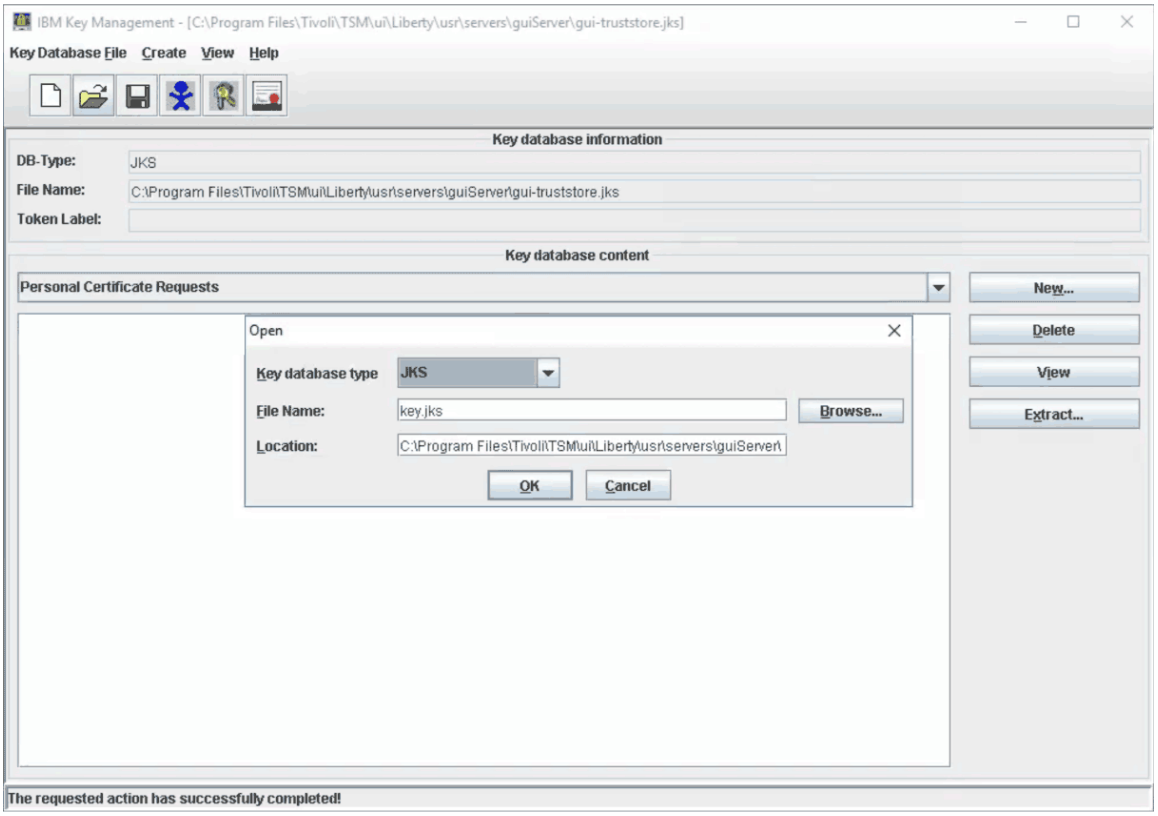
     a. Abra a ferramenta IBM Key Management emitindo o comando a seguir:

     ```
     ikeyman
     ```

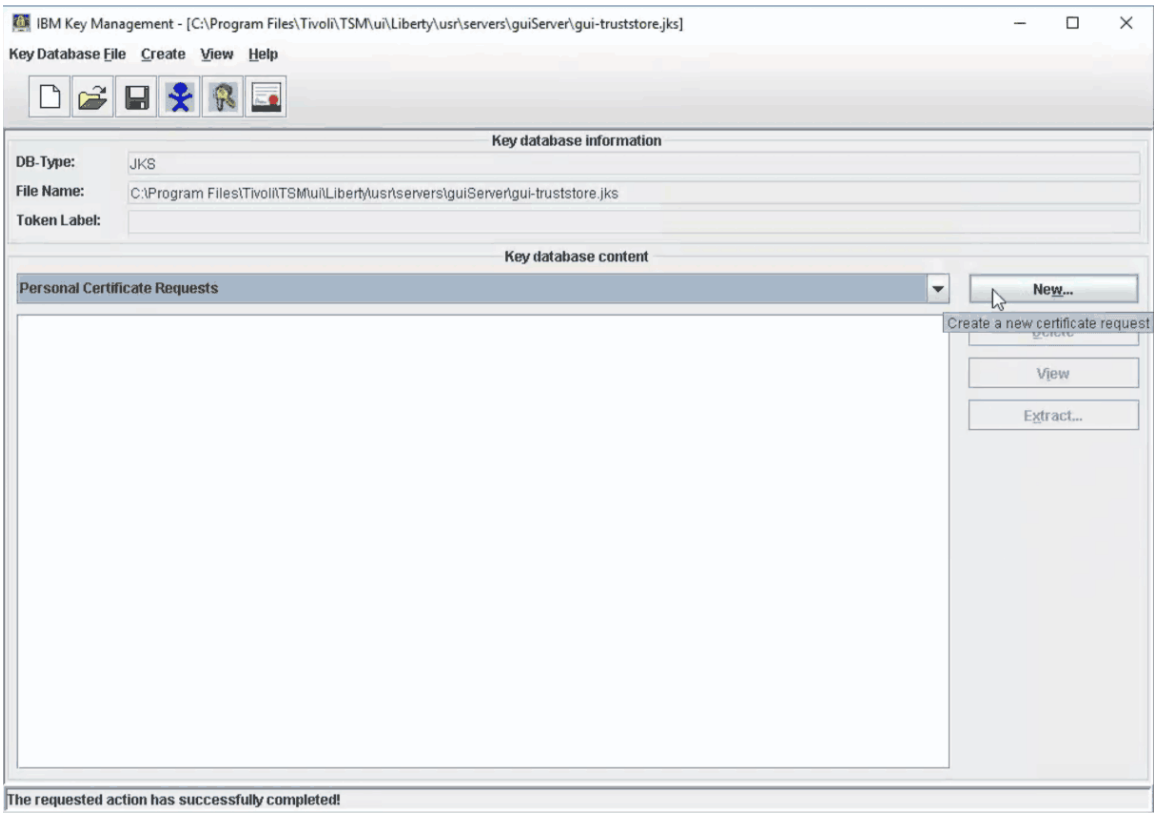
     b. Clique em **Arquivo do Banco de Dados de Chave** > **Abrir**.

     Na janela **Abrir**, clique em **Procurar** para abrir o diretório e selecione o arquivo `gui-truststore.jks`. Clique em **OK**.



c. Criar uma solicitação de certificado. Na área **Conteúdo do Banco de Dados de Chaves**, clique em **Novo**.



d. Na caixa de diálogo Criar Nova Chave e Solicitação de Certificado, complete os campos conforme necessário por CA e organização. Especifique as informações a seguir:

Rótulo Chave
Especifique um rótulo exclusivo para o certificado no armazenamento confiável. O nome do rótulo, por exemplo, *usr-cert-name*, identifica o certificado no armazenamento confiável.

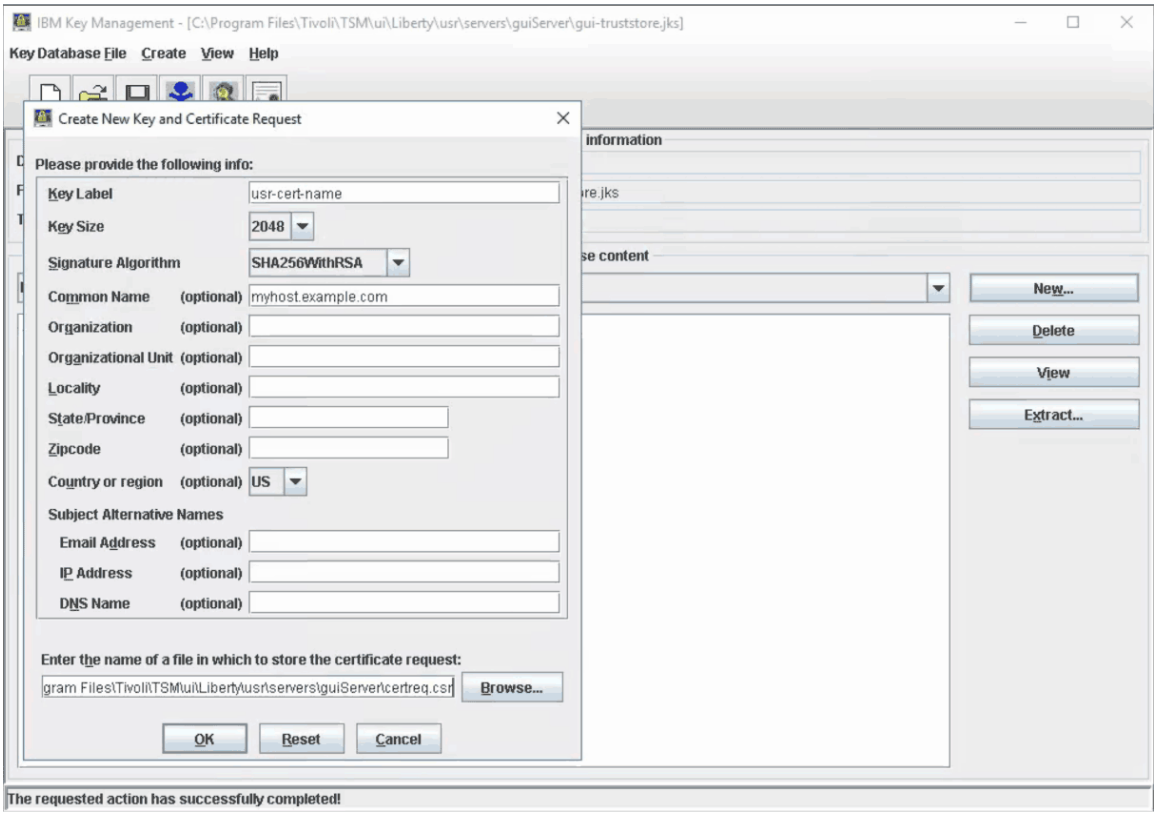
Tamanho de chave
Selecione um tamanho de chave de pelo menos 2048 bits.

Algoritmo de Assinatura
Selecione **SHA256WithRSA**.

Nome comum
Especifique o nome completo do domínio (FQDN) do sistema na rede em que o Operations Center está instalado.

Lembre-se: O FQDN para o sistema em sua rede é usado na URL para o Operations Center em seu sistema. A URL é usada por um navegador da web para acessar o Operations Center.

Insira o nome de um arquivo no qual armazenar a solicitação de certificado
Especifique um arquivo denominado `certreq.csr` no diretório `guiServer`.



e. Feche a janela **Abrir**.

- Para criar uma solicitação de certificado usando o comando **ikeycmd**, emita o seguinte comando:

```
ikeycmd -certreq -create -db gui-truststore.jks -size 2048
-sig_alg SHA256WithRSA -dn "CN=myhost.example.com" -file certreq.csr -label usr-cert-name
-san_dnsname myhost.example.com,myhost
-san_ipaddr 192.0.2.1,192.0.2.2
```

onde:

-dn "CN=*myhost.example.com*"
Especifica o nome distinto. Entrada como uma sequência de caracteres entre aspas contendo a especificação CN=*myhost.example.com*, em que *myhost.example.com* especifica o FQDN do sistema na rede em que o Operations Center está instalado.

Lembre-se: O FQDN para o sistema em sua rede é usado na URL para o Operations Center em seu sistema. A URL é usada por um navegador da web para acessar o Operations Center.

-label *usr-cert-name*
Especifica um rótulo exclusivo, *usr-cert-name*, para o certificado no arquivo de armazenamento confiável.

-san_dnsname *myhost.example.com,myhost* (Opcional)
Especifica os nomes de servidor de nomes de domínio (DNS) do sistema em que o Operations Center está instalado. O `CN` e o `dnsname` são geralmente o mesmo valor.

-san_ipaddr *192.0.2.1,192.0.2.2* (Optional)
Especifica o endereço IP do sistema no qual o Operations Center está instalado.

Enviando o Certificate Signing Request para a autoridade de certificação

Após criar o arquivo de solicitação de certificado (`certreq.csr`), você deve enviá-lo para a CA para assinatura. Siga as instruções da CA.

Recebendo o certificado assinado

A CA deve enviar a você o arquivo de certificado para inclusão no arquivo de armazenamento confiável.

Procedimento

Para receber o certificado assinado, conclua as etapas a seguir:

1. Na linha de comandos, altere o diretório para o local do keystore:
   installation_dir`/ui/Liberty/usr/servers/guiServer`
2. Copie os arquivos que você recebeu da autoridade de certificação (CA) nesse local. Esses arquivos incluem o certificado raiz da CA, certificados de CA intermediários (se houver) e o certificado assinado para Operations Center.
3. Pare o servidor da web do Operations Center conforme descrito em "Iniciando e parando o servidor da web" na página 175.
4. Faça uma cópia de backup do armazenamento confiável do Operations Center, caso você deva reverter para o armazenamento confiável original. O armazenamento confiável do Operations Center é chamado `gui-truststore.jks`.
5. Para concluir as etapas para receber o certificado assinado, use um dos comandos a seguir:
   - Comando **`ikeyman`**: conclua as etapas em "Recebendo o certificado assinado usando o IBM Key Management" na página 165.
   - Comando **`ikeycmd`**: conclua as etapas em "Recebendo o certificado assinado usando ikeycmd" na página 172.

Recebendo o certificado assinado usando o IBM Key Management

É possível usar uma interface gráfica com o usuário, a ferramenta IBM Key Management, para gerenciar as chaves de certificado e receber o certificado assinado.

Procedimento

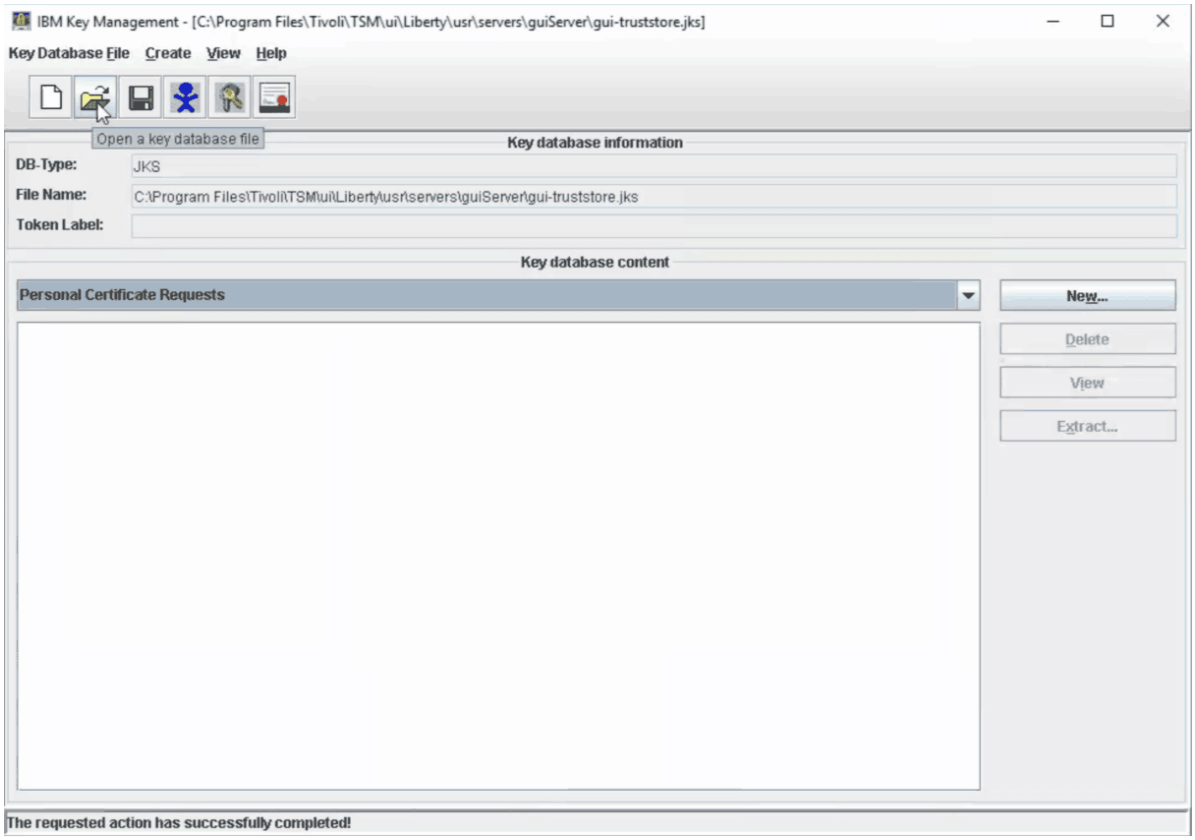
1. Verifique se o Certificado Assinado Pessoal está no diretório adequado usando o comando **`ikeyman`**. Execute as etapas a seguir:
   a) Abra a ferramenta IBM Key Management emitindo o comando a seguir:

   ```
   ikeyman
   ```

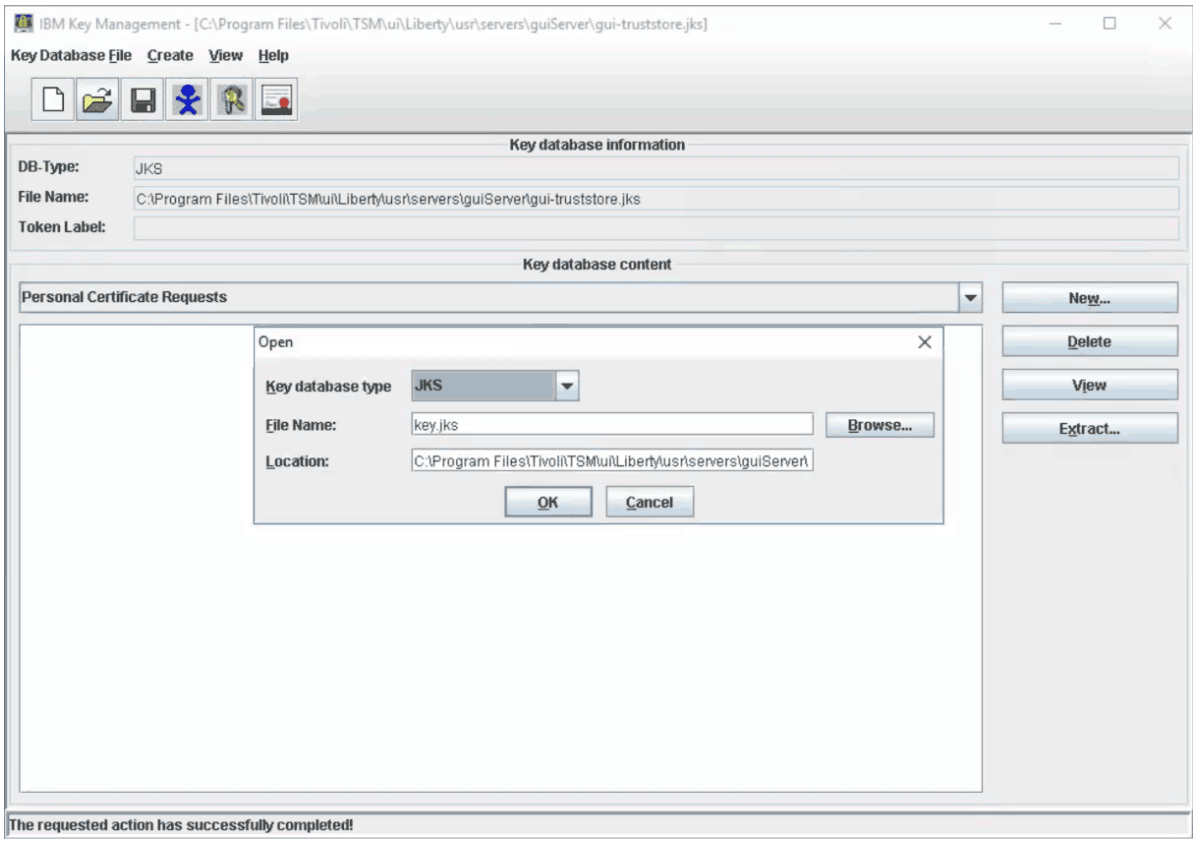
   Dica: Talvez você tenha que especificar o caminho completo para o comando **`ikeyman`**. Os comandos estão localizados no diretório a seguir, em que *installation_dir* representa o diretório no qual o Operations Center está instalado:

   installation_dir`/ui/jre/bin`

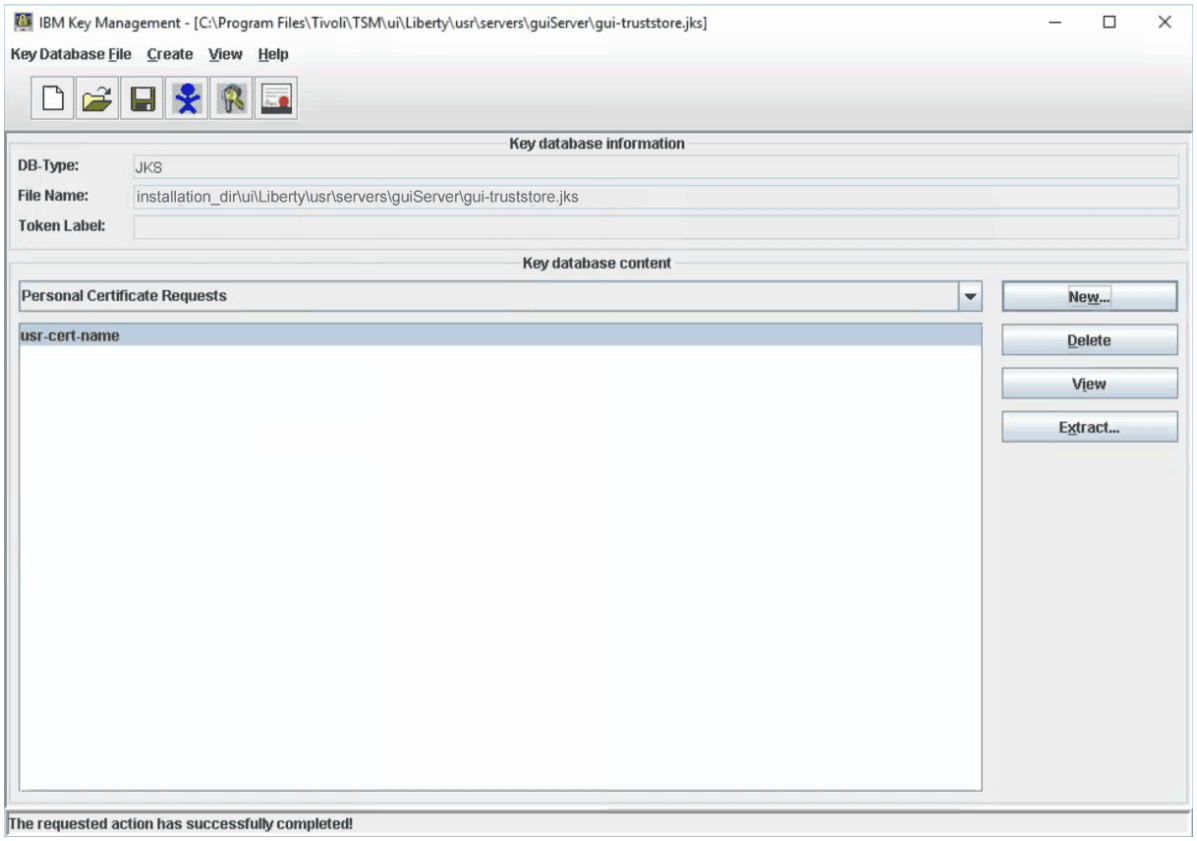
   b) Clique em **Arquivo do Banco de Dados de Chave** > **Abrir**.



Na caixa de diálogo **Abrir**, clique em **Procurar** para abrir o diretório e selecione o arquivo `gui-truststore.jks`. Clique em **OK**.



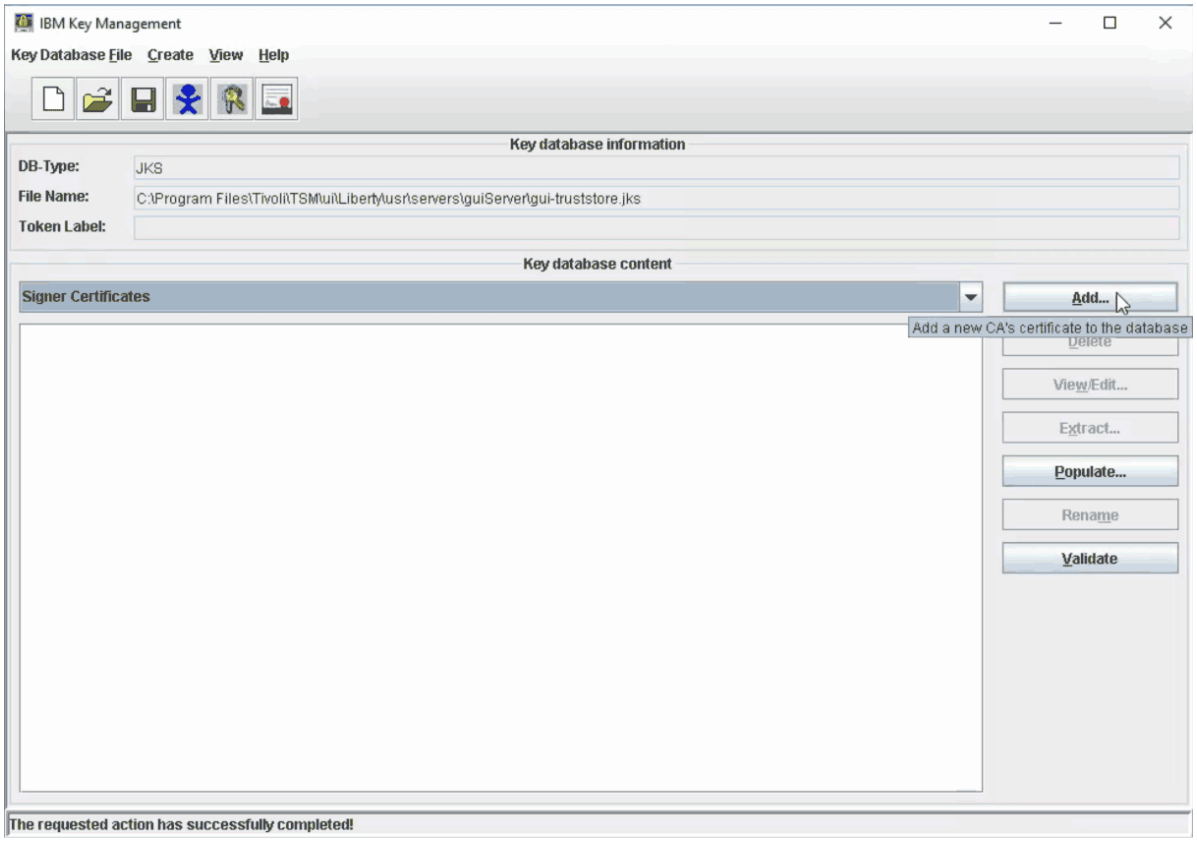
c) Na área **Conteúdo do banco de dados de chaves**, selecione **Solicitações de Certificado Pessoal** e confirme se o rótulo **usr-cert-name** é exibido.



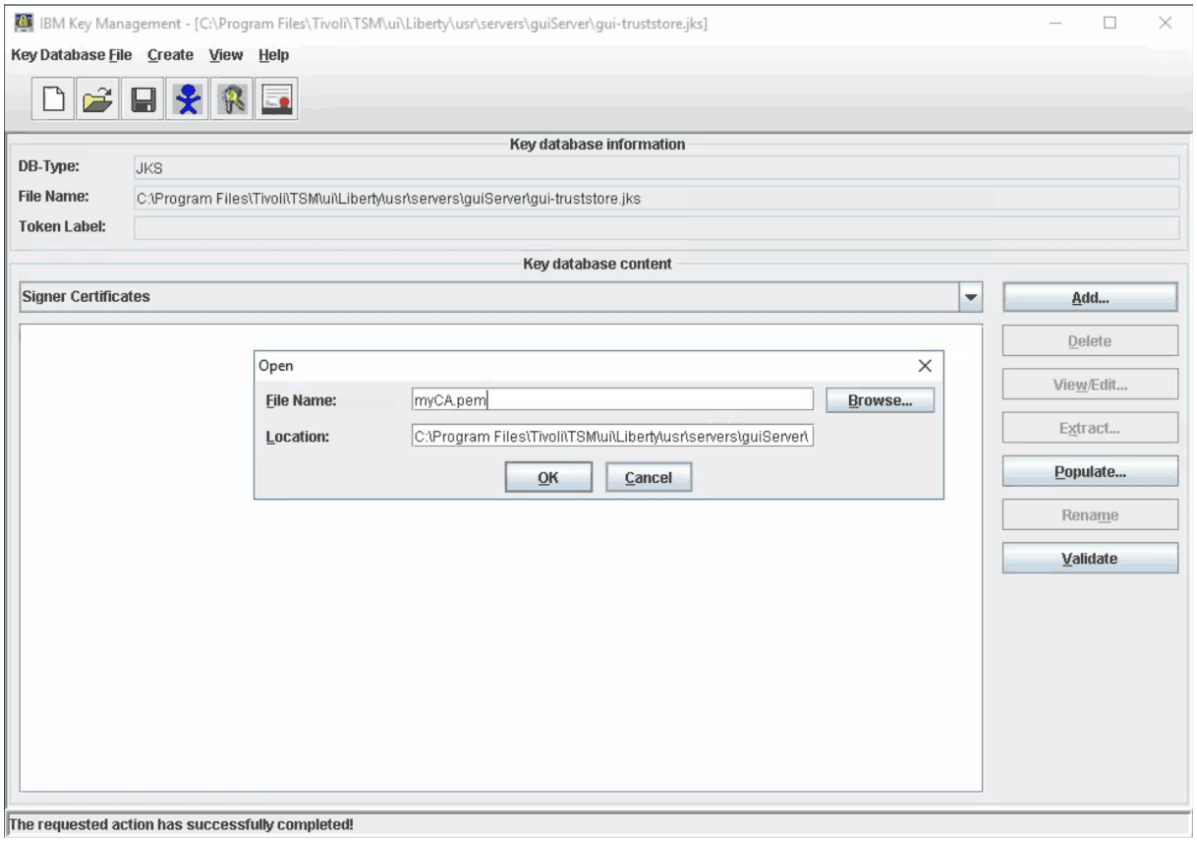
2. Inclua o certificado raiz da CA e quaisquer certificados intermediários no arquivo de armazenamento confiável. Se você recebeu certificados intermediários da CA, deve-se incluir cada um no arquivo de armazenamento confiável antes de incluir o certificado raiz da CA. Conclua as etapas a seguir para cada certificado intermediário e o certificado raiz da CA.

   Importante: A CA envia um certificado raiz, o certificado assinado e possivelmente um ou mais certificados intermediários. Dependendo da CA, o arquivo de certificado pode ser um arquivo ou vários arquivos. Se você receber o arquivo de certificado como um arquivo, será necessário extrair os certificados como arquivos separados. Entre em contato com a CA se não tiver certeza de como extrair os certificados.

   a) Na área **Conteúdo do banco de dados de chaves**, selecione **Certificados de assinante** e clique em **Incluir**.

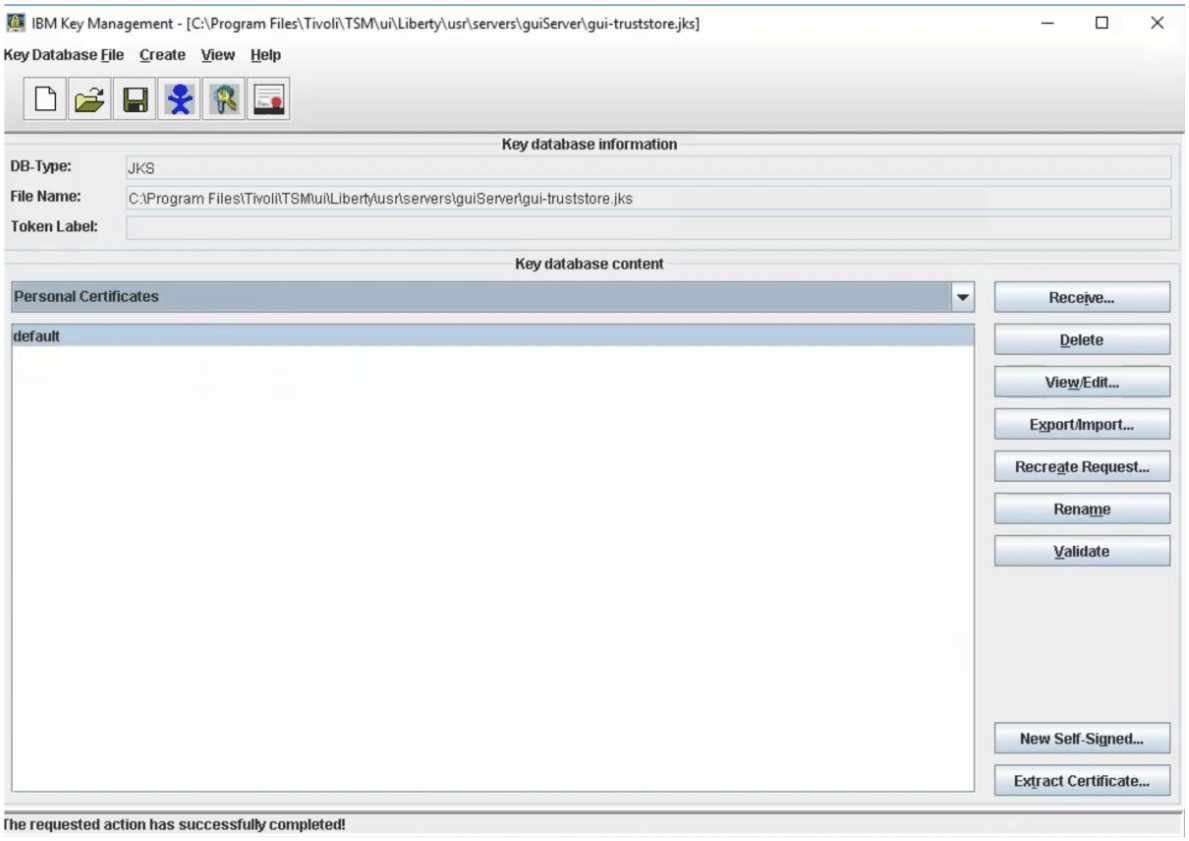


b) Na caixa de diálogo Abrir, especifique o certificado raiz da CA ou o certificado intermediário e clique em **OK**.

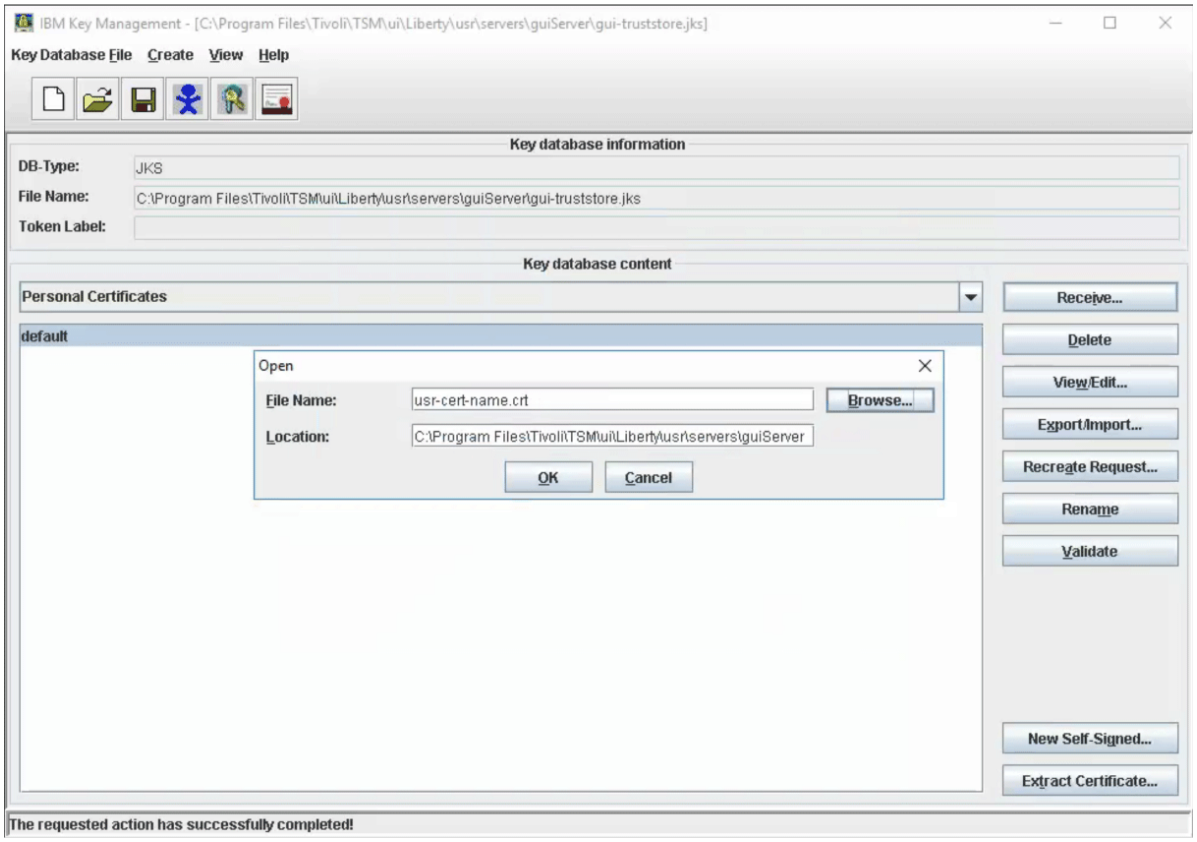


3. Receba o certificado assinado concluindo as seguintes etapas:

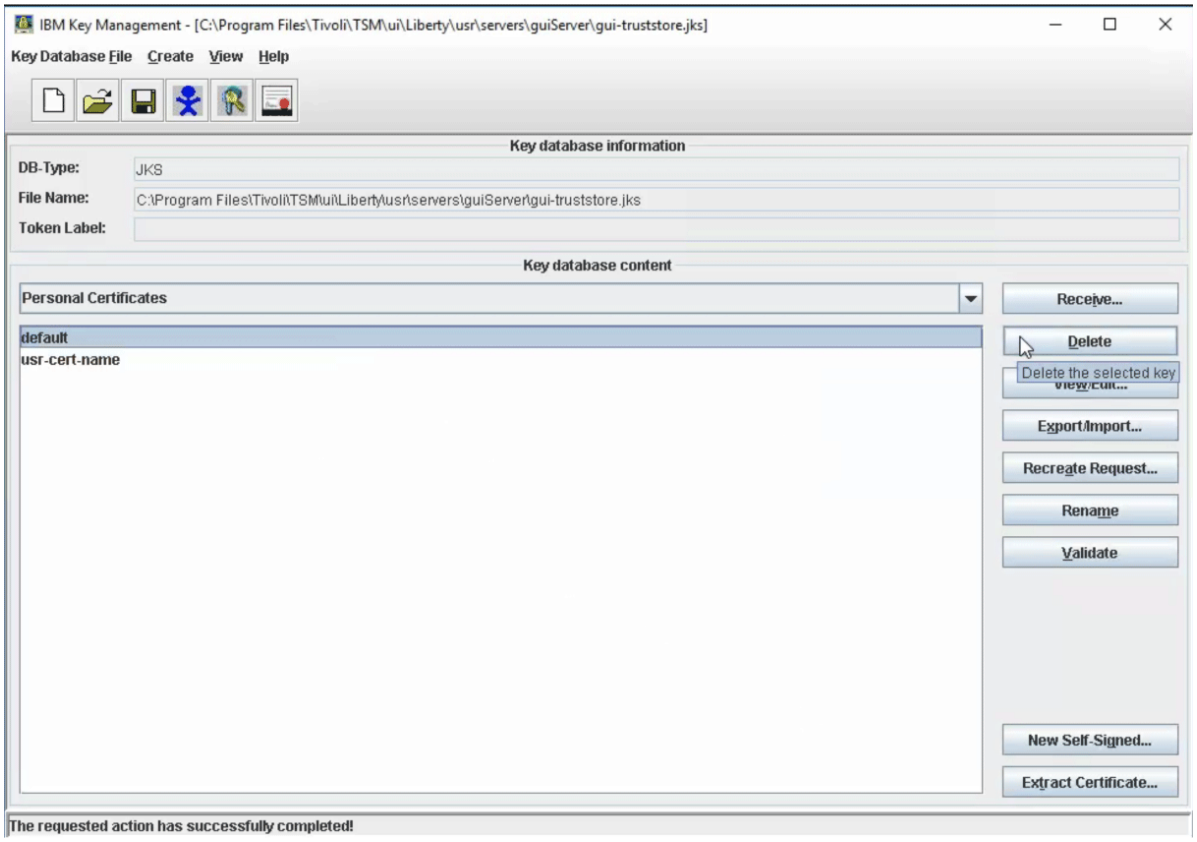
a) Na área **Conteúdo do banco de dados de chaves**, selecione **Certificados pessoais** e clique em **Receber**.



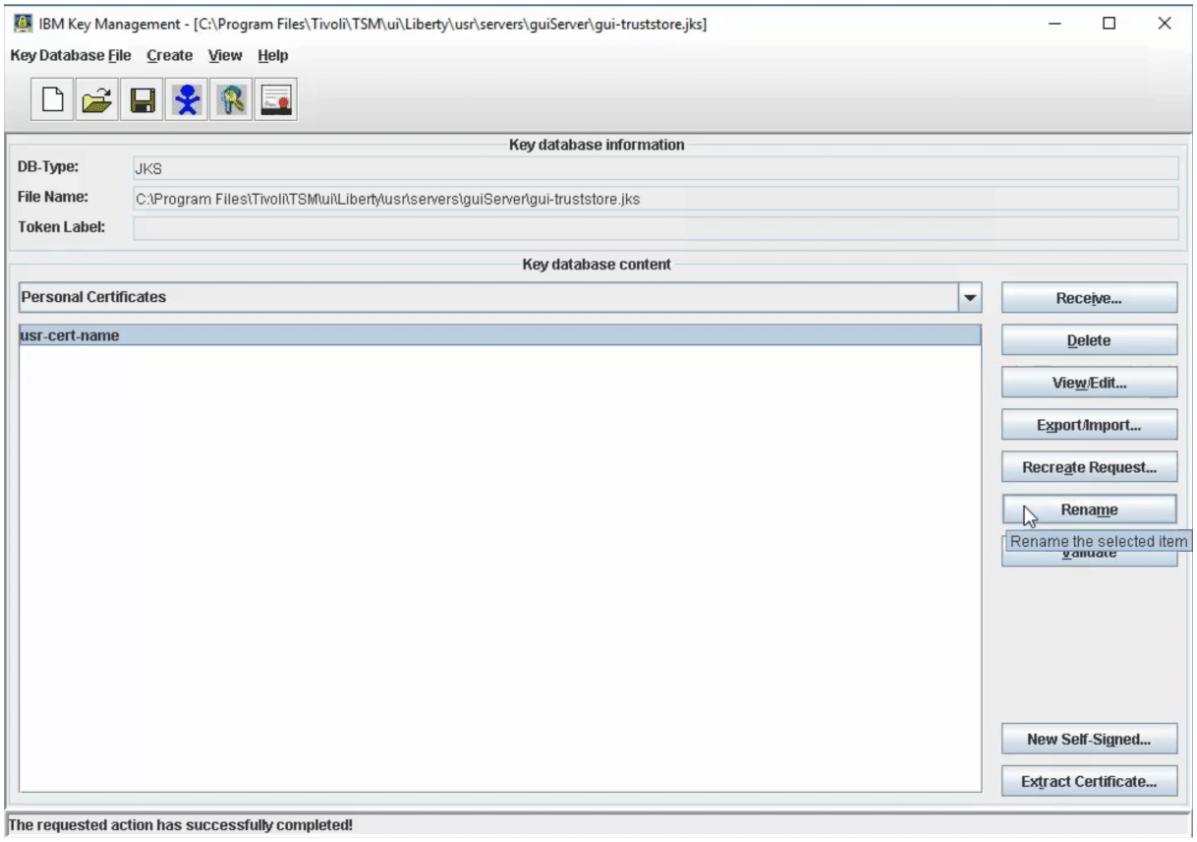
b) Na caixa de diálogo Abrir, especifique o certificado assinado e clique em **OK**.



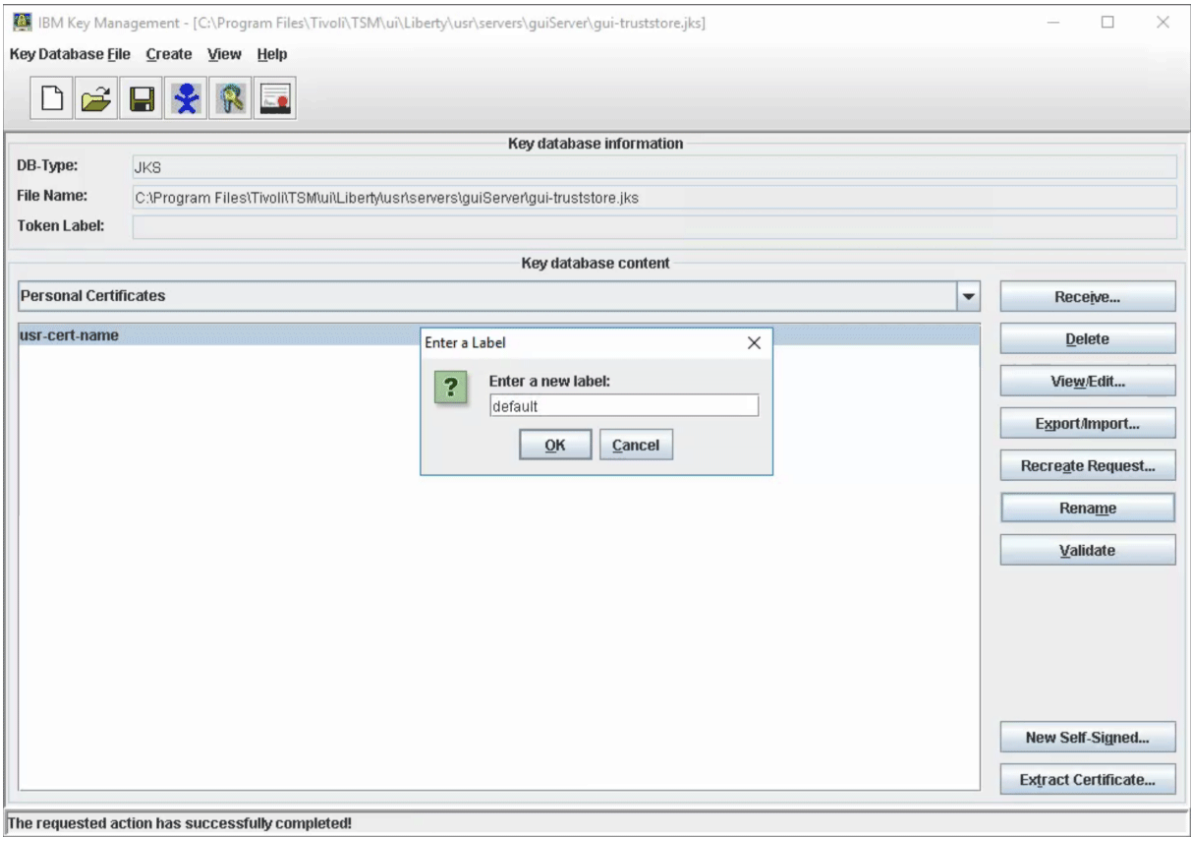
4. Exclua o certificado autoassinado atualmente usado pelo Operations Center e substitua-o pelo certificado assinado por CA concluindo as seguintes etapas:
   a) Na área **Conteúdo do banco de dados de chaves**, selecione **Certificados pessoais**.
   b) Selecione o certificado rotulado **default** e clique em **Excluir**. Clique em **Sim** na caixa de diálogo de confirmação.



   c) Selecione o certificado assinado por CA, **usr-cert-name**, e clique em **Renomear**.



d) Na caixa de diálogo Renomear, renomeie o certificado assinado (`usr-cert-name`) para `default` e clique em **OK**.



5. Valide o certificado `default` concluindo as seguintes etapas:
   a) Na área **Conteúdo do banco de dados de chaves**, selecione **Certificados pessoais**.

b) Selecione o certificado rotulado como **default** e clique em **Validar**. Clique **OK** na caixa de diálogo de confirmação.

6. Inicie o servidor da web do Operations Center conforme descrito em "Iniciando e parando o servidor da web" na página 175.

Recebendo o certificado assinado usando `ikeycmd`

É possível usar o comando **ikeycmd**, que abre uma linha de comandos, para gerenciar chaves do certificado e receber certificados assinados.

Procedimento

1. Verifique se o Certificado Assinado Pessoal está no diretório adequado usando o comando **ikeycmd**. Execute as etapas a seguir:
   a) Emita o seguinte comando:

   ```
   ikeycmd -certreq -list -db gui-truststore.jks
   ```

   Dica: Talvez você tenha que especificar o caminho completo para o comando **ikeycmd**. Os comandos estão localizados no diretório a seguir, em que *installation_dir* representa o diretório no qual o Operations Center está instalado:

   installation_dir/ui/jre/bin

   b) Uma mensagem exibe o nome do Certificado Assinado Pessoal, `usr-cert-name`, que está no arquivo de armazenamento confiável.
2. Inclua o certificado raiz da CA e quaisquer certificados intermediários no arquivo de armazenamento confiável emitindo os seguintes comandos. Se você recebeu certificados intermediários da CA, deve-se incluí-los no arquivo de armazenamento confiável antes de incluir o certificado raiz da CA.

   ```
   ikeycmd -cert -add -db gui-truststore.jks
       -file intermediate_certificate_file
   ```

   ```
   ikeycmd -cert -add -db gui-truststore.jks
       -file root_certificate_file
   ```

   onde:

   -file *certificate_file*
   Especifica o nome do arquivo que contém o certificado.
3. Receba o certificado assinado emitindo o seguinte comando:

   ```
   ikeycmd -cert -receive -db gui-truststore.jks
   -file signer_certificate_file
   ```

   onde:

   -file *signer_certificate_file*
   Especifica o nome do arquivo que contém o certificado assinado.
4. Exclua o certificado autoassinado atualmente usado pelo Operations Center e substitua-o pelo certificado assinado por CA concluindo as seguintes etapas:
   a) Para excluir o certificado autoassinado existente, emita o comando a seguir:

   ```
   ikeycmd -cert -delete -db gui-truststore.jks -label default
   ```

   b) Para renomear o certificado assinado por CA, *usr-cert-name*, para `default`, emita o seguinte comando:

   ```
   ikeycmd -cert -rename -db gui-truststore.jks -label usr-cert-name
   -new_label default
   ```

   onde:

-label *usr-cert-name*
Identifica o certificado assinado por CA por seu rótulo.

5. Valide o certificado `default` emitindo o seguinte comando:

```
ikeycmd -cert -validate -db gui-truststore.jks -label default
```

6. Inicie o servidor da web Operations Center seguindo as instruções em "Iniciando e parando o servidor da web" na página 175.

Excluindo e redesignando a senha para o arquivo de armazenamento confiável do Operations Center

Para configurar a comunicação segura entre o Operations Center e o servidor do hub, você deve saber a senha para o arquivo de armazenamento confiável do Operations Center. Crie esta senha durante a instalação do Operations Center. Se você não souber a senha, é possível excluí-la e designar uma nova.

Sobre Esta Tarefa

Para designar uma nova senha, deve-se criar uma senha, excluir o arquivo de armazenamento confiável do Operations Center e reiniciar o servidor da web Operations Center.

Atenção:

Se você esqueceu a senha do armazenamento confiável, será necessário obter um novo certificado assinado da CA. Para obter informações adicionais, consulte "Recebendo o certificado assinado" na página 165.

Conclua essas etapas apenas se você não souber a senha do armazenamento confiável. Não conclua essas etapas se você souber a senha do armazenamento confiável e quiser alterá-la. Para excluir e redesignar uma senha, deve-se excluir o arquivo de armazenamento confiável, que exclui todos os certificados armazenados no arquivo de armazenamento confiável. Se você souber a senha do armazenamento confiável, é possível alterá-la usando o utilitário **ikeycmd** ou **ikeyman**.

Procedimento

1. Pare o servidor da web Operations Center.
2. Acesse o seguinte diretório, em que *installation_dir* representa o diretório no qual o Operations Center está instalado:

   installation_dir/ui/Liberty/usr/servers/guiServer
3. Abra o arquivo `bootstrap.properties`, que contém a senha para o arquivo de armazenamento confiável.

   Se a senha não estiver criptografada, é possível usá-la para abrir o arquivo de armazenamento confiável sem precisar redesignar a senha.

   Os exemplos a seguir indicam a diferença entre uma senha criptografada e não criptografada:

   Exemplo de senha criptografada
   As senhas criptografadas começam com a sequência de texto `{xor}`.

   O exemplo a seguir mostra uma senha criptografada como o valor do parâmetro **tsm.truststore.pswd**:

   ```
   tsm.truststore.pswd={xor}MiYPPiwsKDAtOw==
   ```

   Exemplo de senha não criptografada
   O exemplo a seguir mostra uma senha não criptografada como o valor do parâmetro **tsm.truststore.pswd**:

   ```
   tsm.truststore.pswd=J8b%^B
   ```
4. Substitua a senha no arquivo `bootstrap.properties` por uma nova.

É possível substituir a senha com uma senha criptografada ou não criptografada. Lembre-se da senha não criptografada para uso futuro.

Para criar uma senha criptografada, conclua as seguintes etapas:

a. Crie uma senha não criptografada.

A senha para o arquivo de armazenamento confiável deve atender aos critérios a seguir:

- A senha deve conter um mínimo de 6 caracteres e um máximo de 64 caracteres.
- A senha deve conter pelo menos os caracteres a seguir:
  - Uma letra maiúscula (A – Z)
  - Uma letra minúscula (a – z)
  - Um dígito (0 – 9)
  - Dois dos caracteres não alfanuméricos que estão listados na série seguinte:

```
~ @ # $ % ^ & * _ - + = ` |
```

```
( ) { } [ ] : ; < > , . ? /
```

b. Na linha de comandos do sistema operacional, acesse o diretório a seguir:

installation_dir/ui/Liberty/bin

c. Para criptografar a senha, emita o comando a seguir, em que *myPassword* representa a senha não criptografada:

securityUtility encode *myPassword* --encoding=aes

5. Salve o arquivo `bootstrap.properties`.
6. Acesse o diretório a seguir:

installation_dir/ui/Liberty/usr/servers/guiServer

7. Exclua o arquivo `gui-truststore.jks`, que é o arquivo de armazenamento confiável do Operations Center.
8. Inicie o servidor da web Operations Center.

Conclua as etapas a seguir para iniciar o servidor da web Operations Center:

a. Emita o comando a seguir para iniciar o servidor da web Operations Center:

```
/opt/tivoli/tsm/ui/Liberty/bin/server start guiServer
```

Um novo arquivo de armazenamento confiável é criado automaticamente para o Operations Center, e o certificado TLS do Operations Center é incluído automaticamente no arquivo de armazenamento confiável. No entanto, o Operations Center não está disponível.

b. Emita o comando a seguir para parar o servidor da web Operations Center:

```
/opt/tivoli/tsm/ui/Liberty/server stop guiServer
```

c. Emita o comando a seguir para reiniciar o servidor da web Operations Center:

```
/opt/tivoli/tsm/ui/utils/startServer.sh
```

Resultados

Um novo arquivo de armazenamento confiável é criado automaticamente para o Operations Center, e o certificado TLS do Operations Center é incluído automaticamente no arquivo de armazenamento confiável.

Iniciando e parando o servidor da web

O servidor da web do Operations Center é executado como um serviço e é iniciado automaticamente. Talvez seja necessário parar e iniciar o servidor da web, por exemplo, para fazer mudanças na configuração.

Procedimento

Pare e inicie o servidor da web.

- No diretório /*installation_dir*/ui/utils, em que *installation_dir* representa o diretório em que o Operations Center está instalado, emita o comando a seguir:
  - Para parar o servidor:

    ```
    ./stopserver.sh
    ```

  - Para iniciar o servidor:

    ```
    ./startserver.sh
    ```

Abrindo o Operations Center

A página **Visão geral** é a visualização inicial padrão no Operations Center. No entanto, em seu navegador da web você pode marcar a página que deseja abrir ao efetuar login no Operations Center.

Procedimento

1. Em um navegador da web, insira o endereço a seguir, em que *hostname* representa o nome do computador em que o Operations Center está instalado, e *secure_port* representa o número da porta que o Operations Center usa para comunicação HTTPS nesse computador:

   ```
   https://hostname:secure_port/oc
   ```

   Dicas:

   - A URL faz distinção entre maiúsculas e minúsculas. Por exemplo, certifique-se de digitar "oc" em minúsculas, conforme indicado.
   - O número da porta padrão para a comunicação HTTPS é 11090, mas um número de porta diferente no intervalo de 1024 a 65535 pode ser especificado durante a instalação do Operations Center. Após a instalação, um administrador pode configurar o Operations Center para usar a porta segura TCP/IP padrão (porta 443) para a comunicação HTTPS. Se o Operations Center estiver configurado para usar a porta 443, não será necessário incluir o número da porta segura ao abrir o Operations Center. Nesse caso, é possível inserir o seguinte endereço, em que *hostname* representa o nome do computador no qual o Operations Center está instalado:

     ```
     https:hostname/oc/
     ```

     Para obter mais informações sobre como configurar o Operations Center para usar a porta 443, consulte “Configurando o servidor da web do Operations Center para usar a porta segura padrão do TCP/IP” na página 154.
2. Efetue login usando um ID de administrador que está registrado no servidor do hub.

   Na página **Visão geral**, é possível visualizar informações de resumo para clientes serviços, servidores, conjuntos de armazenamentos e dispositivos de armazenamento. É possível visualizar mais detalhes clicando em itens ou usando a barra de menus do Operations Center.

   Monitorando a partir de um dispositivo móvel: Para monitorar remotamente o ambiente de armazenamento, é possível visualizar a página **Visão geral** do Operations Center no navegador da web de um dispositivo móvel. O Operations Center suporta o navegador da web Apple Safari no iPad. Outros dispositivos móveis também podem ser usados.

Coletando informações de diagnóstico com o IBM Spectrum Protect

O serviço de gerenciamento de cliente coleta as informações de diagnóstico sobre os clientes de backup-archive e disponibiliza-as para o Operations Center para a capacidade de monitoramento básico.

Sobre Esta Tarefa

Após instalar o serviço de gerenciamento de cliente, será possível visualizar a página **Diagnóstico** no Operations Center para obter informações sobre resolução de problemas para clientes de backup-archive.

Dica: Antes de instalar o serviço de gerenciamento de cliente, assegure-se de que uma conexão bem-sucedida tenha sido estabelecida entre o cliente de backup e archive e o servidor. O arquivo de armazenamento confiável do servidor usado pelo cliente não tem o certificado Secure Sockets Layer (SSL) do servidor até que o sistema do cliente tenha se conectado ao servidor.

As informações de diagnóstico podem ser coletadas somente a partir de clientes Linux e Windows, mas os administradores podem visualizar as informações de diagnóstico no Operations Center nos sistemas operacionais AIX, Linux ou Windows.

Também é possível instalar o serviço de gerenciamento de cliente nos nós do movedor de dados para o IBM Spectrum Protect for Virtual Environments: Proteção de Dados para VMware para coletar informações de diagnóstico sobre os movedores de dados.

Dica: Na documentação do serviço de gerenciamento de cliente, o *sistema do cliente* é o sistema no qual o cliente de backup-archive é instalado.

Instalando o serviço de gerenciamento de cliente Usando um Assistente Gráfico

Para coletar informações de diagnóstico sobre clientes de backup-archive, como arquivos de log do cliente, deve-se instalar o serviço de gerenciamento de cliente em sistemas do cliente que você gerenciar.

Antes de Iniciar

Revise o “Requisitos e limitações do IBM Spectrum Protect” na página 135.

Sobre Esta Tarefa

Deve-se instalar o serviço de gerenciamento de cliente no mesmo computador que o cliente de backup-archive.

Procedimento

1. Faça download do pacote de instalação para o serviço de gerenciamento de cliente a partir de um site de download da IBM, como IBM Passport Advantage ou IBM Fix Central. Procure um nome de arquivo que seja semelhante a `<version>-IBM-SPCMS-<operating system>.bin`.

   A tabela a seguir mostra os nomes dos pacotes de instalação.

Sistema operacional do cliente	Nome do pacote de instalação
Linux x86 de 64 bits	`8.1.x.000-IBM-SPCMS-Linuxx64.bin`
Windows de 32 bits	`8.1.x.000-IBM-SPCMS-Windows32.exe`
Windows de 64 bits	`8.1.x.000-IBM-SPCMS-Windows64.exe`

2. Crie um diretório no sistema do cliente que deseja gerenciar e copie o pacote de instalação nesse diretório.

3. Extraia o conteúdo do arquivo do pacote de instalação.
   - Nos sistemas do cliente Linux, conclua as seguintes etapas:
     a. Altere o arquivo para um arquivo executável ao emitir o seguinte comando:

     ```
     chmod +x 8.1.x.000-IBM-SPCMS-Linuxx64.bin
     ```

     b. Emita o seguinte comando:

     ```
     ./8.1.x.000-IBM-SPCMS-Linuxx64.bin
     ```

   - Em sistemas do cliente Windows, clique duas vezes no nome do pacote de instalação no Windows Explorer.

   Dica: Se o pacote foi instalado e desinstalado anteriormente, selecione **Tudo** quando perguntado se deseja substituir os arquivos de instalação existentes.

4. Execute o arquivo em lote de instalação no diretório no qual os arquivos de instalação e arquivos associados foram extraídos. Esse é o diretório que foi criado na etapa “2” na página 176.
   - Nos sistemas do cliente Linux, emita o seguinte comando:

   ```
   ./install.sh
   ```

   - Nos sistemas do cliente Windows, clique duas vezes em **install.bat**.
5. Para instalar o serviço de gerenciamento de cliente, siga as instruções no assistente IBM Installation Manager.

   Se o IBM Installation Manager ainda não estiver instalado no sistema do cliente, deve-se selecionar o **IBM Installation Manager** e o **IBM Spectrum Protect Client Management Services**.

   Dica: É possível aceitar os locais padrão do diretório de recursos compartilhados e do diretório de instalação do IBM Installation Manager.

O que Fazer Depois

Verifique a instalação.

Instalando o serviço de gerenciamento de cliente no Modo Silencioso

É possível instalar o serviço de gerenciamento de cliente no modo silencioso. Ao usar o modo silencioso, forneça os valores de instalação em um arquivo de resposta e, em seguida, execute um comando de instalação.

Antes de Iniciar

Revise o “Requisitos e limitações do IBM Spectrum Protect” na página 135.

Extraia o pacote de instalação seguindo as instruções em “Instalando o serviço de gerenciamento de cliente Usando um Assistente Gráfico” na página 176.

Sobre Esta Tarefa

Deve-se instalar o serviço de gerenciamento de cliente no mesmo computador que o cliente de backup-archive.

O diretório `input`, que está no diretório onde o pacote de instalação foi extraído, contém o arquivo de resposta de amostra a seguir:

`install_response_sample.xml`

É possível usar o arquivo de amostra com os valores padrão ou é possível customizá-lo.

Dica: Se desejar customizar o arquivo de amostra, crie uma cópia do arquivo de amostra, renomeie-o e edite a cópia.

Procedimento

1. Crie um arquivo de resposta baseado no arquivo de amostra ou use o arquivo de amostra `install_response_sample.xml`.

   Em qualquer caso, assegure-se de que o arquivo de resposta especifique o número da porta para o serviço de gerenciamento de cliente. A porta padrão é 9028. Exemplo:

   ```
   <variable name='port' value='9028'/>
   ```

2. Execute o comando para instalar o serviço de gerenciamento de cliente e aceite a licença. No diretório em que o arquivo do pacote de instalação é extraído, emita o comando a seguir, em que *response_file* representa o caminho do arquivo de resposta, incluindo o nome do arquivo:

   Em um sistema do cliente Linux:

   ```
   ./install.sh -s -input response_file -acceptLicense
   ```

   Exemplo:

   ```
   ./install.sh -s -input /cms_install/input/install_response.xml
   -acceptLicense
   ```

   Em um sistema do cliente Windows:

   ```
   install.bat -s -input response_file -acceptLicense
   ```

   Exemplo:

   ```
   install.bat -s -input c:\cms_install\input\install_response.xml -acceptLicense
   ```

O que Fazer Depois

Verifique a instalação.

Verificando se o serviço de gerenciamento de cliente está instalado corretamente

Antes de usar o serviço de gerenciamento de cliente para coletar informações de diagnóstico sobre um cliente de backup-archive, será possível verificar se o serviço de gerenciamento de cliente foi instalado e configurado corretamente.

Procedimento

Na linha de comandos do sistema do cliente, execute os seguintes comandos para visualizar a configuração do serviço de gerenciamento de cliente:

- Nos sistemas do cliente Linux, emita o seguinte comando:

  ```
  client_install_dir/cms/bin/CmsConfig.sh list
  ```

  em que *client_install_dir* é o diretório no qual o cliente de backup-archive está instalado. Por exemplo, com a instalação do cliente padrão, emita o comando a seguir:

  ```
  /opt/tivoli/tsm/cms/bin/CmsConfig.sh list
  ```

  A saída é semelhante ao seguinte texto:

  ```
  Listando a configuração do CMS
  ```

```
server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
    Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

    Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252

    Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

- Nos sistemas do cliente Windows, emita o seguinte comando:

  ```
  client_install_dir\cms\bin\CmsConfig.bat list
  ```

  em que *client_install_dir* é o diretório no qual o cliente de backup-archive está instalado. Por exemplo, com a instalação do cliente padrão, emita o comando a seguir:

  ```
  C:\"Program Files"\Tivoli\TSM\cms\bin\CmsConfig.bat list
  ```

  A saída é semelhante ao seguinte texto:

  ```
  Listando a configuração do CMS

  server1.example.com:1500 NO_SSL HOSTNAME
  Capabilities: [LOG_QUERY]
      Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

      Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

Se o serviço de gerenciamento de cliente estiver instalado e configurado corretamente, a saída exibirá o local do arquivo de log de erro.

O texto de saída é extraído do arquivo de configuração a seguir:

- Nos sistemas do cliente Linux:

  ```
  client_install_dir/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
  ```

- Nos sistemas do cliente Windows:

  ```
  client_install_dir\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
  ```

Se a saída não contiver nenhuma entrada, deve-se configurar o arquivo `client-configuration.xml`. Para obter instruções sobre como configurar esse arquivo, consulte Configurar o serviço de gerenciamento de cliente para configurações customizadas. É possível usar o comando **CmsConfig verify** para verificar se uma definição de nó está corretamente criada no arquivo `client-configuration.xml`.

Configurando o Operations Center para usar o serviço de gerenciamento de cliente

Se você não usou a configuração padrão do serviço de gerenciamento de cliente, deve-se configurar o Operations Center para acessar o serviço de gerenciamento de cliente.

Antes de Iniciar

Certifique-se de que o serviço de gerenciamento de cliente esteja instalado e iniciado no sistema do cliente. Revise o “Requisitos e limitações do IBM Spectrum Protect” na página 135.

Verifique se a configuração padrão é usada. A configuração padrão não será usada se uma das condições a seguir for atendida:

- O serviço de gerenciamento de cliente não usa o número da porta padrão 9028.

- O cliente de backup-archive não é acessado pelo mesmo endereço IP do sistema do cliente no qual o cliente de backup-archive está instalado. Por exemplo, um endereço IP diferente pode ser usado nas situações a seguir:
  - O sistema de computador possui duas placas de rede. O cliente de backup-archive está configurado para comunicação em uma rede, enquanto que o serviço de gerenciamento de cliente se comunica na outra rede.
  - O sistema do cliente está configurado com o Protocolo de Configuração de Host Dinâmico (DHCP). Como resultado, o sistema do cliente é designado dinamicamente a um endereço IP, que é salvo no servidor IBM Spectrum Protect durante a operação do cliente de backup-archive anterior. Quando o sistema do cliente é reiniciado, esse sistema poderá ser designado a um endereço IP diferente. Para assegurar que o Operations Center sempre possa localizar o sistema do cliente, especifique um nome de domínio completo.

Procedimento

Para configurar o Operations Center para usar o serviço de gerenciamento de cliente, execute as seguintes etapas:

1. Na página **Clientes** do Operations Center, selecione o cliente.
2. Clique em **Detalhes**.
3. Clique na guia **Propriedades**.
4. No campo **URL de diagnósticos remota** da seção **Geral**, especifique a URL para o serviço de gerenciamento de cliente no sistema do cliente.

   O endereço deve iniciar com `https`. A tabela a seguir mostra exemplos da URL de diagnósticos remota.

Tipo de URL	Exemplo
Com o nome do host DNS e porta padrão 9028	`https://server.example.com`
Com o nome do host DNS e porta não padrão	`https://server.example.com:1599`
Com o endereço IP e porta não padrão	`https://192.0.2.0:1599`

5. Clique em **Salvar**.

O que Fazer Depois

É possível acessar informações de diagnóstico do cliente, como arquivos de log do cliente, a partir da guia **Diagnósticos** no Operations Center.

Iniciando e parando o serviço de gerenciamento de cliente

O serviço de gerenciamento de cliente é iniciado automaticamente após ter sido instalado no sistema do cliente. Poderá ser necessário parar e iniciar o serviço em determinadas situações.

Procedimento

- Para parar, iniciar ou reiniciar o serviço de gerenciamento de cliente em sistemas do cliente Linux, emita os comandos a seguir:
  - Se **systemctl** estiver instalado no sistema, emita os comandos a seguir:
    - Para parar o servidor:

      ```
      systemctl stop cms.service
      ```

    - Para iniciar o servidor:

      ```
      systemctl start cms.service
      ```

- Para reiniciar o servidor:

```
systemctl restart cms.service
```

- Para determinar se o servidor está em execução, emita o comando a seguir:

```
systemctl status cms.service
```

- Se **systemctl** não estiver instalado no sistema, emita os comandos a seguir:
  - Para parar o servidor:

```
service cms.rc stop
```

  - Para iniciar o servidor:

```
service cms.rc start
```

  - Para reiniciar o servidor:

```
service cms.rc restart
```

  - Para determinar se o servidor está em execução, emita o comando a seguir:

```
service cms.rc status
```

- Em sistemas do cliente Windows, abra a janela **Serviços** e pare, inicie ou reinicie o serviço do IBM Spectrum Protect Client Management Services.

Desinstalando o serviço de gerenciamento de cliente

Se não precisar mais coletar informações de diagnóstico do cliente, será possível desinstalar o serviço de gerenciamento de cliente a partir do sistema do cliente.

Sobre Esta Tarefa

Deve-se usar o IBM Installation Manager para desinstalar o serviço de gerenciamento de cliente. Se não desejar mais usar o IBM Installation Manager, ele também poderá ser desinstalado.

Procedimento

1. Desinstale o serviço de gerenciamento de cliente a partir do sistema do cliente:
   a) Abra o IBM Installation Manager:
      - No sistema do cliente Linux, no diretório em que o IBM Installation Manager está instalado, acesse o subdiretório `eclipse` (por exemplo, `/opt/IBM/InstallationManager/eclipse`) e emita o comando a seguir:

```
./IBMIM
```

      - No sistema do cliente do Windows, abra o IBM Installation Manager a partir do menu **Iniciar**.

   b) Clique em **Desinstalar**.
   c) Selecione o **IBM Spectrum Protect Client Management Services** e clique em **Avançar**.
   d) Clique em **Desinstalar** e depois em **Concluir**.
   e) Feche a janela **IBM Installation Manager**.
2. Se não precisar mais do IBM Installation Manager, desinstale-o do sistema do cliente:
   a) Abra o assistente de desinstalação do IBM Installation Manager:

- No sistema do cliente Linux, mude para o diretório de desinstalação do IBM Installation Manager, (por exemplo, `/var/ibm/InstallationManager/uninstall`), e emita o seguinte comando:

```
./uninstall
```

- No sistema do cliente do Windows, clique em **Iniciar** > **Painel de Controle** . Em seguida, clique em **Desinstalar um programa** > **IBM Installation Manager** > **Desinstalar**.

b) Na janela do **IBM Installation Manager**, selecione **IBM Installation Manager** se ainda não tiver selecionado e clique em **Avançar**.

c) Clique em **Desinstalar** e depois em **Concluir**.

Configurando o serviço de gerenciamento de cliente para instalações do cliente customizadas

O serviço de gerenciamento de cliente usa as informações no arquivo de configuração do cliente (`client-configuration.xml`) para descobrir informações de diagnóstico. Se o serviço de gerenciamento de cliente não conseguir descobrir o local dos arquivos de log, deve-se executar o utilitário **CmsConfig** e incluir o local dos arquivos de log no arquivo `client-configuration.xml`.

Sobre Esta Tarefa

Antes de instalar o serviço de gerenciamento de cliente, assegure-se de que uma conexão bem-sucedida tenha sido estabelecida entre o cliente e o servidor de backup e archive. O arquivo de armazenamento confiável do servidor usado pelo cliente não tem o certificado Secure Sockets Layer (SSL) do servidor até que o sistema do cliente tenha se conectado ao servidor.

Utilitário CmsConfig

Se você não estiver usando a configuração do cliente padrão, é possível executar o utilitário **CmsConfig** no sistema do cliente para descobrir e incluir o local dos arquivos de log do cliente no arquivo `client-configuration.xml`. Depois de concluir a configuração, o serviço de gerenciamento de cliente pode acessar os arquivos de log do cliente e disponibilizá-los para funções de diagnósticos básicos no Operations Center.

Também pode-se usar o utilitário **CmsConfig** para mostrar a configuração do serviço de gerenciamento de cliente e remover um nome do nó do arquivo `client-configuration.xml`.

O arquivo de configuração `client-configuration.xml` está no diretório a seguir:

- Nos sistemas do cliente Linux:

```
client_install_dir/cms/Liberty/usr/servers/cmsServer
```

- Nos sistemas do cliente Windows:

```
client_install_dir\cms\Liberty\usr\servers\cmsServer
```

em que *client_install_dir* é o diretório no qual o cliente de backup-archive está instalado.

O utilitário **CmsConfig** está disponível nos seguintes locais.

Sistema operacional do cliente	Local e nome do utilitário
Linux	*client_install_dir*/cms/bin/CmsConfig.sh
Windows	*client_install_dir*\cms\bin\CmsConfig.bat

Para usar o utilitário **CmsConfig**, emita qualquer comando que é incluído no utilitário. Assegure-se de inserir cada comando em uma única linha.

Comando CmsConfig discover

É possível usar o comando **CmsConfig discover** para descobrir automaticamente os arquivos de opções e os arquivos de log e incluí-los no arquivo de configuração do cliente, `client-configuration.xml`. Dessa forma, é possível ajudar a assegurar que o serviço de gerenciamento de cliente possa acessar os arquivos de log do cliente e disponibilizá-los para diagnóstico no Operations Center.

Normalmente, o instalador do serviço de gerenciamento de cliente executa o comando **CmsConfig discover** automaticamente. No entanto, esse comando deverá ser executado manualmente se você alterou o cliente de backup-archive, como incluído um cliente ou alterado a configuração do servidor ou o local dos arquivos de log.

Para o serviço de gerenciamento de cliente criar uma definição de log no arquivo `client-configuration.xml`, o endereço do servidor, a porta do servidor e o nome do nó cliente do IBM Spectrum Protect deverão ser obtidos. Se o nome do nó não estiver definido no arquivo de opções do cliente (normalmente, `dsm.sys` em sistemas do cliente Linux e `dsm.opt` em sistemas do cliente Windows), o nome do host do sistema do cliente será utilizado.

Para atualizar o arquivo de configuração do cliente, o serviço de gerenciamento de cliente deverá acessar um ou mais arquivos de log, como `dsmerror.log` e `dsmsched.log`. Para obter melhores resultados, execute o comando **CmsConfig discover** no mesmo diretório e usando as mesmas variáveis de ambiente usadas para o comando do cliente de backup-archive, **dsmc**. Dessa forma, poder-se melhorar as chances de localizar os arquivos de log corretos.

Se o arquivo de opções do cliente estiver em um local customizado ou não tiver um nome típico de arquivo de opções, também é possível especificar o caminho para o arquivo de opções do cliente para limitar o escopo da descoberta.

Sintaxe

Parâmetros

configPath

O caminho do arquivo de opções do cliente (geralmente `dsm.opt`). Especifique o caminho de configuração quando o arquivo de opções do cliente não estiver em um local padrão ou não tiver o nome padrão. O serviço de gerenciamento de cliente carrega o arquivo de opções do cliente e descobre os nós clientes e registra a partir desse local. Esse parâmetro é opcional.

Em um sistema do cliente Linux, o serviço de gerenciamento de cliente sempre carrega o arquivo de opções de usuário do cliente (`dsm.opt`) primeiro e, em seguida, procura pelo arquivo de opções do sistema do cliente (geralmente `dsm.sys`). O valor do parâmetro *configPath*, no entanto, é sempre o arquivo de opções de usuário do cliente.

Exemplos para um sistema do cliente Linux

- Descubra os arquivos de log do cliente e inclua automaticamente as definições de log no arquivo `client-configuration.xml`.

  Emita o comando a seguir a partir do diretório `/opt/tivoli/tsm/cms/bin`.

  Comando:

  ```
  ./CmsConfig.sh discover
  ```

  Saída:

  ```
  Discovering client configuration and logs.

  server.example.com:1500 SUSAN
      /opt/tivoli/tsm/client/ba/bin/dsmerror.log
  ```

```
Finished discovering client configuration and logs.
```

- Descubra os arquivos de configuração e os arquivos de log que estão especificados no arquivo `/opt/tivoli/tsm/client/ba/bin/daily.opt` e inclua automaticamente as definições de log no arquivo `client-configuration.xml`.

  Emita o comando a seguir a partir do diretório `/opt/tivoli/tsm/cms/bin`.

  Comando:
  ```
  ./CmsConfig.sh discover /opt/tivoli/tsm/client/ba/bin/daily.opt
  ```

  Saída:

  ```
  Descobrindo logs e configurações do cliente

  server.example.com:1500 NO_SSL SUSAN
  Capabilities: [LOG_QUERY]
      Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

      Log File:  /opt/tivoli/tsm/client/ba/bin/dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

  Finished discovering client configuration and logs.
  ```

Exemplos para um sistema do cliente Windows

- Descubra os arquivos de log do cliente e inclua automaticamente as definições de log no arquivo `client-configuration.xml`.

  Emita o comando a seguir a partir do diretório `C:\Program Files\Tivoli\TSM\cms\bin`.

  Comando:
  ```
  cmsconfig discover
  ```

  Saída:

  ```
  Discovering client configuration and logs.

  server.example.com:1500 SUSAN
      C:\Program Files\Tivoli\TSM\baclient\dsmerror.log

  Finished discovering client configuration and logs.
  ```

- Descubra os arquivos de configuração e os arquivos de log que estão especificados no arquivo `c:\program files\tivoli\tsm\baclient\daily.opt` e inclua automaticamente as definições de log no arquivo `client-configuration.xml`.

  Emita o comando a seguir a partir do diretório `C:\Program Files\Tivoli\TSM\cms\bin`.

  Comando:
  ```
  cmsconfig discover "c:\program files\tivoli\tsm\baclient\daily.opt"
  ```

  Saída:

  ```
  Descobrindo logs e configurações do cliente

  server.example.com:1500 NO_SSL SUSAN
  Capabilities: [LOG_QUERY]
      Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

      Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

  Finished discovering client configuration and logs.
  ```

Comando CmsConfig addnode

Use o comando **CmsConfig addnode** para incluir manualmente uma definição de nó cliente para o arquivo de configuração `client-configuration.xml`. A definição de nó contém informações necessárias pelo serviço de gerenciamento de cliente para comunicar-se com o servidor IBM Spectrum Protect.

Use esse comando somente se o arquivo de opções do cliente ou os arquivos de log do cliente estiverem armazenados em um local não padrão no sistema do cliente.

Sintaxe

Parâmetros

nodeName

O nome de nó cliente que está associado aos arquivos de log. Para a maioria dos sistemas do cliente, somente um nome do nó é registrado no servidor IBM Spectrum Protect. No entanto, em sistemas com diversos usuários, como sistemas do cliente Linux, pode haver mais de um nome do nó cliente. Esse parâmetro é necessário.

serverIP

O endereço TCP/IP do servidor IBM Spectrum Protect com o qual o serviço de gerenciamento de cliente é autenticado. Esse parâmetro é necessário.

É possível especificar um endereço TCP/IP contendo de 1 a 64 caracteres para o servidor. O endereço do servidor pode ser um nome de domínio TCP/IP ou um endereço IP numérico. O endereço IP numérico pode ser um endereço TCP/IP v4 ou TCP/IP v6. É possível usar endereços IPv6 somente se a opção **commmethod V6Tcpip** estiver especificada para o sistema do cliente.

Exemplos:

- `server.example.com`
- `192.0.2.0`
- `2001:0DB8:0:0:0:0:0:0`

serverPort

O número da porta TCP/IP que é usado para comunicação com o servidor IBM Spectrum Protect. É possível especificar um valor no intervalo 1 a 32767. Esse parâmetro é necessário.

Exemplo: `1500`

serverProtocol

O protocolo que é usado para comunicação entre o serviço de gerenciamento de cliente e o servidor IBM Spectrum Protect. Esse parâmetro é necessário.

É possível especificar um dos seguintes valores.

Valor	Significado
NO_SSL	O protocolo de segurança SSL não é utilizado.
SSL	O protocolo de segurança SSL é utilizado.
FIPS	O protocolo TLS 1.2 é usado no modo Federal Information Processing Standard (FIPS). **Dica:** Como alternativa, é possível inserir `TLS_1.2` para especificar que o protocolo TLS 1.2 é usado no modo FIPS.

optPath

O caminho completo do arquivo de opções do cliente. Esse parâmetro é necessário.

Exemplo (cliente Linux): `/opt/backup_tools/tivoli/tsm/baclient/dsm.sys`

Exemplo (cliente Windows): `C:\backup tools\Tivoli\TSM\baclient\dsm.opt`

Exemplo de um sistema do cliente Linux

Inclua a definição de nó para o nó cliente SUSAN para o arquivo `client-configuration.xml`. O servidor IBM Spectrum Protect com o qual o nó se comunica é `server.example.com` na porta do servidor `1500`. O protocolo de segurança SSL não é utilizado. O caminho para o arquivo de opções do sistema do cliente é `/opt/tivoli/tsm/client/ba/bin/custom_opt.sys`.

Emita o comando a seguir a partir do diretório `/opt/tivoli/tsm/cms/bin`.

Comando:

```
./CmsConfig.sh addnode SUSAN server.example.com 1500 NO_SSL /opt/tivoli/tsm/
client/ba/bin/custom_opt.sys
```

Saída:

```
Adding node.

Finished adding client configuration.
```

Exemplo de um sistema do cliente Windows

Inclua a definição de nó para o nó cliente SUSAN para o arquivo `client-configuration.xml`. O servidor IBM Spectrum Protect com o qual o nó se comunica é `server.example.com` na porta do servidor `1500`. O protocolo de segurança SSL não é utilizado. O caminho para o arquivo de opções do cliente é `c:\program files\tivoli\tsm\baclient\custom.opt`.

Emita o comando a seguir a partir do diretório `C:\Program Files\Tivoli\TSM\cms\bin`.

Comando:

```
cmsconfig addnode SUSAN server.example.com 1500 NO_SSL "c:\program files
\tivoli\tsm\baclient\custom.opt"
```

Saída:

```
Adding node.

Finished adding client configuration.
```

Comando CmsConfig setopt

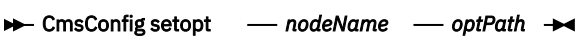
Use o comando **CmsConfig setopt** para configurar o caminho do arquivo de opções do cliente (geralmente `dsm.opt`) para uma definição de nó existente sem primeiro ler o conteúdo do arquivo de opções do cliente.

Esse comando poderá ser útil se o arquivo de opções do cliente não tiver um nome típico ou estiver em um local não padrão.

Requisito: Se a definição de nó não existir, deve-se primeiro emitir o comando **CmsConfig addnode** para criar a definição de nó.

Diferente do comando **CmsConfig discover**, o comando **CmsConfig setopt** não cria definições de log associadas no arquivo `client-configuration.xml`. Deve-se usar o comando **CmsComfog addlog** para criar as definições de log.

Sintaxe



Parâmetros

nodeName
O nome de nó cliente que está associado aos arquivos de log. Para a maioria dos sistemas do cliente, somente um nome do nó é registrado no servidor IBM Spectrum Protect. No entanto, em sistemas com diversos usuários, como sistemas do cliente Linux, pode haver mais de um nome do nó cliente. Esse parâmetro é necessário.

optPath
O caminho completo do arquivo de opções do cliente. Esse parâmetro é necessário.

Exemplo (cliente Linux): `/opt/backup_tools/tivoli/tsm/baclient/dsm.opt`

Exemplo (cliente Windows): `C:\backup tools\Tivoli\TSM\baclient\dsm.opt`

Exemplo de um sistema do cliente Linux

Configure o caminho do arquivo de opções do cliente para o nó SUSAN. O caminho para o arquivo de opções do cliente é `/opt/tivoli/tsm/client/ba/bin/dsm.opt`.

Emita o comando a seguir a partir do diretório `/opt/tivoli/tsm/cms/bin`.

Comando:

```
./CmsConfig.sh setopt SUSAN /opt/tivoli/tsm/client/ba/bin/dsm.opt
```

Saída:

```
Adding node configuration file.
Finished adding client configuration file.
```

Exemplo de um sistema do cliente Windows

Configure o caminho do arquivo de opções do cliente para o nó SUSAN. O caminho para o arquivo de opções do cliente é `c:\program files\tivoli\tsm\baclient\dsm.opt`.

Emita o comando a seguir a partir do diretório `C:\Program Files\Tivoli\TSM\cms\bin`.

Comando:

```
cmsconfig setopt SUSAN "c:\program files\tivoli\tsm\baclient\dsm.opt"
```

Saída:

```
Adding node configuration file.
Finished adding client configuration file.
```

Comando CmsConfig setsys

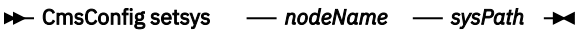
Em um sistema do cliente Linux, use o comando **CmsConfig setsys** para configurar o caminho do arquivo de opções do sistema do cliente (normalmente `dsm.sys`) para uma definição de nó existente sem primeiro ler o conteúdo do arquivo de opções do sistema do cliente.

Esse comando poderá ser útil se o arquivo de opções do sistema do cliente não tiver um nome típico ou estiver em um local não padrão.

Requisito: Se a definição de nó não existir, deve-se primeiro emitir o comando **CmsConfig addnode** para criar a definição de nó.

Diferente do comando **CmsConfig discover**, o comando **CmsConfig setsys** não cria as definições de log associadas no arquivo `client-configuration.xml`. Deve-se usar o comando **CmsComfog addlog** para criar as definições de log.

Sintaxe



Parâmetros

nodeName
O nome de nó cliente que está associado aos arquivos de log. Para a maioria dos sistemas do cliente, somente um nome do nó é registrado no servidor IBM Spectrum Protect. No entanto, em sistemas com diversos usuários, como sistemas do cliente Linux, pode haver mais de um nome do nó cliente. Esse parâmetro é necessário.

sysPath
O caminho completo do arquivo de opções do sistema do cliente. Esse parâmetro é necessário.

Exemplo: `/opt/backup_tools/tivoli/tsm/baclient/dsm.sys`

Exemplo

Configure o caminho do arquivo de opções do sistema do cliente para o nó SUSAN. O caminho para o arquivo de opções do sistema do cliente é `/opt/tivoli/tsm/client/ba/bin/dsm.sys`.

Emita o comando a seguir a partir do diretório `/opt/tivoli/tsm/cms/bin`.

Comando:

```
./CmsConfig.sh setopt SUSAN /opt/tivoli/tsm/client/ba/bin/dsm.sys
```

Saída:

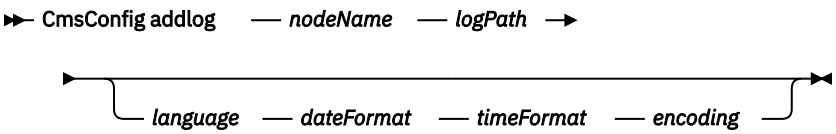
```
Adding node configuration file.
Finished adding client configuration file.
```

Comando CmsConfig addlog

Use o comando **CmsConfig addlog** para incluir manualmente o local dos arquivos de log do cliente em uma definição de nó existente no arquivo de configuração `client-configuration.xml`. Use esse comando apenas se os arquivos de log do cliente estiverem armazenados em um local não padrão no sistema do cliente.

Requisito: Se a definição de nó não existir, deve-se primeiro emitir o comando **CmsConfig addnode** para criar a definição de nó.

Sintaxe



Parâmetros

nodeName
O nome de nó cliente que está associado aos arquivos de log. Para a maioria dos sistemas do cliente, somente um nome do nó é registrado no servidor IBM Spectrum Protect. No entanto, em sistemas com diversos usuários, como sistemas do cliente Linux, pode haver mais de um nome do nó cliente. Esse parâmetro é necessário.

logPath
O caminho completo dos arquivos de log. Esse parâmetro é necessário.

Exemplo (cliente Linux): `/opt/backup_tools/tivoli/tsm/baclient/dsmerror.log`

Exemplo (cliente Windows): `C:\backup tools\Tivoli\TSM\baclient\dsmerror.log`

language
O código de idioma do arquivo de log. Esse parâmetro é opcional. No entanto, se você especificar este parâmetro, também deverá especificar os parâmetros **dateFormat**, **timeFormat** e **encoding**. É necessário especificar o código de idioma para os seguintes idiomas.

idioma	Código de idioma
Português do Brasil	pt_BR
Chinês, Simplificado	zh_CN
Chinês, Tradicional	zh_TW
Tcheco	cs_CZ
Inglês	en_US
Francês	fr_FR
Alemão	de_DE
Húngaro	hu_HU
Italiano	it_IT
Japonês	ja_JP
Coreano	ko_KR
Polonês	pl_PL
Russo	ru_RU
Espanhol	es_ES

dateFormat
O formato de data das entradas de registro de data e hora no arquivo de log do cliente. Esse parâmetro é opcional. No entanto, se você especificar este parâmetro, também deverá especificar os parâmetros **language**, **timeFormat** e **encoding**.

A tabela a seguir mostra os formatos de data para os idiomas.

Dica: Ao invés de usar um dos formatos de data listados na tabela, é possível especificar um formato de data usando a opção **dateformat** do cliente de backup-archive.

idioma	Formato de data
Chinês, Simplificado	yyyy-MM-dd
Chinês, Tradicional	yyyy/MM/dd
Tcheco	dd.MM.yyyy
Inglês	MM/dd/yyyy
Francês	dd/MM/yyyy
Alemão	dd.MM.yyyy
Húngaro	yyyy.MM.dd
Italiano	dd/MM/yyyy
Japonês	yyyy-MM-dd
Coreano	yyyy/MM/dd

idioma	Formato de data
Polonês	yyyy-MM-dd
Português, Brasileiro	dd/MM/yyyy
Russo	dd.MM.yyyy
Espanhol	dd.MM.yyyy

timeFormat

O formato de hora das entradas de registro de data e hora no arquivo de log do cliente. Esse parâmetro é opcional. No entanto, se você especificar este parâmetro, também deverá especificar os parâmetros **language**, **dateFormat** e **encoding**.

A tabela a seguir mostra exemplos dos formatos de hora padrão que podem ser especificados e os sistemas operacionais do cliente.

Dica: Ao invés de usar um dos formatos de hora listados na tabela, é possível especificar um formato de hora usando a opção **timeformat** do cliente de backup-archive.

idioma	Formato de hora para sistemas do cliente Linux	Formato de hora para sistemas do cliente Windows
Chinês, Simplificado	HH:mm:ss	HH:mm:ss
Chinês, Tradicional	HH:mm:ss	ahh:mm:ss
Tcheco	HH:mm:ss	HH:mm:ss
Inglês	HH:mm:ss	HH:mm:ss
Francês	HH:mm:ss	HH:mm:ss
Alemão	HH:mm:ss	HH:mm:ss
Húngaro	HH.mm.ss	HH:mm:ss
Italiano	HH:mm:ss	HH:mm:ss
Japonês	HH:mm:ss	HH:mm:ss
Coreano	HH:mm:ss	HH:mm:ss
Polonês	HH:mm:ss	HH:mm:ss
Português, Brasileiro	HH:mm:ss	HH:mm:ss
Russo	HH:mm:ss	HH:mm:ss
Espanhol	HH:mm:ss	HH:mm:ss

encoding

A codificação de caracteres das entradas nos arquivos de log do cliente. Esse parâmetro é opcional. No entanto, se você especificar este parâmetro, também deverá especificar os parâmetros **language**, **dateFormat** e **timeFormat**.

Para sistemas do cliente Linux, a codificação de caracteres típica é UTF-8. Para sistemas do cliente Windows, os valores de codificação padrão são mostrados na tabela a seguir. Se seu sistema do cliente for customizado de modo diferente, use o parâmetro **encoding** para especificar um valor diferente do padrão.

idioma	Codificação
Chinês, Simplificado	CP936
Chinês, Tradicional	CP950

idioma	Codificação
Tcheco	Windows-1250
Inglês	Windows-1252
Francês	Windows-1252
Alemão	Windows-1252
Húngaro	Windows-1250
Italiano	Windows-1252
Japonês	CP932
Coreano	CP949
Polonês	Windows-1250
Português, Brasileiro	Windows-1252
Russo	Windows-1251
Espanhol	Windows-1252

Exemplo de um sistema do cliente Linux

Inclua a localização do arquivo de log do cliente na definição existente para o nó cliente SUSAN no arquivo `client-configuration.xml`. O caminho para o arquivo de log do cliente é `/usr/work/logs/dsmerror.log`. Inclua a especificação de idioma, o formato de hora e o formato de data para o código de idioma francês.

Emita o comando a seguir a partir do diretório `/opt/tivoli/tsm/cms/bin`.

Comando:

```
./CmsConfig.sh addlog SUSAN /usr/work/logs/dsmerror.log fr_FR yyyy/MM/dd
HH:MM:ss UTF-8
```

Saída:

```
Adding log.

Finished adding log.
```

Exemplo de um sistema do cliente Windows

Inclua a localização do arquivo de log do cliente na definição existente para o nó cliente SUSAN no `client-configuration.xml`. O caminho para o arquivo de log do cliente é `c:\work\logs\dsmerror.log`. Inclua a especificação de idioma, o formato de hora e o formato de data para o código de idioma francês.

Emita o comando a seguir a partir do diretório `C:\Program Files\Tivoli\TSM\cms\bin`.

Comando:

```
cmsconfig addlog SUSAN c:\work\logs\dsmerror.log fr_FR yyyy/MM/dd HH:MM:ss
UTF-8
```

Saída:

```
Adding log.

Finished adding log.
```

Comando CmsConfig remove

Use o comando **CmsConfig remove** para remover uma definição de nó cliente do arquivo de configuração do cliente, `client-configuration.xml`. Todas as entradas do arquivo de log que são associadas ao nome do nó cliente também são removidas.

Sintaxe

Parâmetros

nodeName

O nome de nó cliente que está associado aos arquivos de log. Para a maioria dos sistemas do cliente, somente um nome do nó é registrado no servidor IBM Spectrum Protect. No entanto, em sistemas com diversos usuários, como sistemas do cliente Linux, pode haver mais de um nome do nó cliente. Esse parâmetro é necessário.

Exemplo de um sistema do cliente Linux

Remova a definição de nó do SUSAN do arquivo `client-configuration.xml`.

Emita o comando a seguir a partir do diretório `/opt/tivoli/tsm/cms/bin`.

Comando:

```
./CmsConfig.sh remove SUSAN
```

Saída:

```
Removing node.

Finished removing node.
```

Exemplo de um sistema do cliente Windows

Remova a definição de nó do SUSAN do arquivo `client-configuration.xml`.

Emita o comando a seguir a partir do diretório `C:\Program Files\Tivoli\TSM\cms\bin`.

Comando:

```
cmsconfig remove SUSAN
```

Saída:

```
Removing node.

Finished removing node.
```

Comando CmsConfig verify

Use o comando **CmsConfig verify** para verificar se uma definição de nó está corretamente criada no arquivo `client-configuration.xml`. Se houver erros na definição de nó ou o nó não estiver corretamente definido, você deverá corrigir a definição de nó usando os comandos **CmsConfig** adequados.

Sintaxe

Parâmetros

nodeName
O nome de nó cliente que está associado aos arquivos de log. Para a maioria dos sistemas do cliente, somente um nome do nó é registrado no servidor IBM Spectrum Protect. No entanto, em sistemas com diversos usuários, como sistemas do cliente Linux, pode haver mais de um nome do nó cliente. Esse parâmetro é necessário.

cmsPort
O número da porta TCP/IP que é usado para comunicação com o serviço de gerenciamento de cliente. Especifique o número da porta, se você não usou o número da porta padrão quando instalou o serviço de gerenciamento de cliente. O número da porta padrão é 9028. Esse parâmetro é opcional.

Exemplo de um sistema do cliente Linux

Verifique se a definição de nó para o nó SUSAN foi criada corretamente no arquivo `client-configuration.xml`.

Emita o comando a seguir a partir do diretório `/opt/tivoli/tsm/cms/bin`.

Comando:

```
./CmsConfig.sh verify SUSAN
```

Durante o processo de verificação, é solicitado que insira o nome do nó cliente ou ID do usuário administrativo e senha.

Saída:

```
Verifying node.


Verifying the CMS service configuration for node SUSAN.
The CMS configuration looks correct.

Verifying the CMS service works correctly on port 9028.

Enter your user id: admin
Enter your password:

Connecting to CMS service and verifying resources.
The CMS service is working correctly.
Finished verifying node.
```

Exemplo de um sistema do cliente Windows

Verifique se a definição de nó para o nó SUSAN foi criada corretamente no arquivo `client-configuration.xml`.

Emita o comando a seguir a partir do diretório `C:\Program Files\Tivoli\TSM\cms\bin`.

Comandos:

```
cmsconfig verify SUSAN
```

Durante o processo de verificação, é solicitado que insira o nome do nó cliente ou ID do usuário administrativo e senha.

Saída:

```
Verifying node.


Verifying the CMS service configuration for node SUSAN.
The CMS configuration looks correct.

Verifying the CMS service works correctly on port 9028.

Enter your user id: admin
Enter your password:
```

```
Connecting to CMS service and verifying resources.
The CMS service is working correctly.
Finished verifying node.
```

Comando CmsConfig list

Use o comando **CmsConfig list** para mostrar a configuração do serviço de gerenciamento de cliente.

Sintaxe

Exemplo de um sistema do cliente Linux

Mostre a configuração do serviço de gerenciamento de cliente. Em seguida, visualize a saída para assegurar-se de ter inserido o comando corretamente.

Emita o comando a seguir a partir do diretório `/opt/tivoli/tsm/cms/bin`.

Comando:

```
./CmsConfig.sh list
```

Saída:

```
Listando a configuração do CMS

server.example.com:1500 NO_SSL SUSAN
Capabilities: [LOG_QUERY]
    Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

    Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252

    Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

Exemplo de um sistema do cliente Windows

Mostre a configuração do serviço de gerenciamento de cliente. Em seguida, visualize a saída para assegurar-se de ter inserido o comando corretamente.

Emita o comando a seguir a partir do diretório `C:\Program Files\Tivoli\TSM\cms\bin`.

Comando:

```
cmsconfig list
```

Saída:

```
Listando a configuração do CMS

server.example.com:1500 NO_SSL SUSAN
Capabilities: [LOG_QUERY]
    Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

    Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252

    Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

Comando CmsConfig help

Use o comando **CmsConfig help** para mostrar a sintaxe dos comandos do utilitário **CmsConfig**.

Sintaxe

Exemplo de um sistema do cliente Linux

Emita o comando a seguir a partir do diretório `/opt/tivoli/tsm/cms/bin`:

```
./CmsConfig help
```

Exemplo de um sistema do cliente Windows

Emita o comando a seguir a partir do diretório `C:\Program Files\Tivoli\TSM\cms\bin`:

```
CmsConfig
help
```

Recursos avançados do serviço de gerenciamento de cliente

Por padrão, o IBM Spectrum Protect serviço de gerenciamento de cliente coleta informações somente dos arquivos de log do cliente. Para iniciar outras ações do cliente, é possível acessar a API Representational State Transfer (REST) que está incluída com o serviço de gerenciamento de cliente.

Desenvolvedores de API podem criar aplicativos REST para iniciar as ações do cliente a seguir:

- Consultar e atualizar arquivos de opções do cliente (por exemplo, o arquivo `dsm.sys` nos clientes Linux e o arquivo `dsm.opt` nos clientes Linux e Windows).
- Consulte o status do client acceptor do IBM Spectrum Protect e do planejador.
- Fazer backup e restaurar arquivos para um nó cliente.
- Estender os recursos do serviço de gerenciamento de cliente com scripts.

Para obter informações detalhadas sobre a API REST do serviço de gerenciamento de cliente, consulte Guia da API REST do Client Management Services.

Capítulo 12. Resolvendo Problemas de Instalação do Operations Center

Se ocorrer um problema com a instalação do Operations Center e você não puder resolvê-lo, é possível consultar as descrições de problemas conhecidos para uma possível solução.

O assistente de instalação gráfico não pode ser iniciado em um sistema AIX

Você está instalando o Operations Center em um sistema AIX usando o assistente gráfico e o programa de instalação não é iniciado.

Solução

Os arquivos RPM que são listados no “Instalando o Operations Center Usando um Assistente Gráfico” na página 141 devem ser instalados no computador. Verifique se os arquivos RPM estão instalados.

Capítulo 13. Desinstalando o Operations Center

É possível desinstalar o Operations Center usando alguns dos métodos a seguir: um assistente gráfico, a linha de comandos no modo do console ou modo silencioso.

Desinstalando o Operations Center Usando um Assistente Gráfico

É possível desinstalar o Operations Center usando o assistente gráfico do IBM Installation Manager.

Procedimento

1. Abra o IBM Installation Manager.

   No diretório em que IBM Installation Manager está instalado, acesse o subdiretório `eclipse` (por exmeplo, `/opt/IBM/InstallationManager/eclipse`), e emita o comando a seguir:

   ```
   ./IBMIM
   ```

2. Clique em **Desinstalar**.
3. Selecione a opção para o Operations Center e clique em **Avançar**.
4. Clique em **Desinstalar**.
5. Clique em **Concluir**.

Desinstalando o Operations Center no Modo do Console

Para desinstalar o Operations Center usando a linha de comandos, você deve executar o programa de desinstalação do IBM Installation Manager a partir da linha de comandos com o parâmetro para o modo de console.

Procedimento

1. No diretório onde o IBM Installation Manager está instalado, acesse o seguinte subdiretório:

   `eclipse/tools`

   Por exemplo:

   `/opt/IBM/InstallationManager/eclipse/tools`
2. No diretório `tools`, emita o comando a seguir:

   `./imcl -c`
3. Para desinstalar, insira 5.
4. Escolha desinstalar do grupo de pacotes do IBM Spectrum Protect.
5. Insira N para Avançar.
6. Escolha desinstalar o pacote do Operations Center.
7. Insira N para Avançar.
8. Insira U para Desinstalar.
9. Insira F para Concluir.

Desinstalando o Operations Center no Modo Silencioso

Para desinstalar o Operations Center no modo silencioso, você deve executar o programa de desinstalação de IBM Installation Manager a partir da linha de comandos com os parâmetros para o modo silencioso.

Antes de Iniciar

Você pode utilizar um arquivo de resposta para fornecer entrada de dados para instalar silenciosamente o Operations Center servidor. IBM Spectrum Protect inclui um arquivo de resposta como amostra, `uninstall_response_sample.xml`, no diretório de `entrada` onde o pacote de instalação está extraído. Esses arquivos contém valores padrão para ajudar você a evitar quaisquer avisos desnecessários.

Para desinstalar os Operations Center, deixe `modify="false"` configurado para a entrada Operations Center no arquivo de resposta.

Se você quiser customizar um arquivo de resposta, é possível modificar as opções que estão no arquivo. Para obter informações sobre arquivos de resposta, acesse Arquivos de respostas.

Procedimento

1. No diretório onde o IBM Installation Manager está instalado, acesse o seguinte subdiretório:

   ```
   eclipse/tools
   ```

   Por exemplo:

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```

2. No diretório `tools`, emita o comando a seguir, em que *response_file* representa o caminho do arquivo de resposta, incluindo o nome do arquivo:

   ```
   ./imcl -input response_file -silent
   ```

   O comando a seguir é um exemplo:

   ```
   ./imcl -input /tmp/input/uninstall_response.xml -silent
   ```

Capítulo 14. Retrocedendo para uma Versão Anterior do Operations Center

Por padrão, o IBM Installation Manager salva versões anteriores de um pacote para o qual retroceder se você encontrar um problema em versões mais recentes de atualizações, correções ou pacotes.

Antes de Iniciar

A função de retrocesso está disponível somente após o Operations Center ser atualizado.

Sobre Esta Tarefa

Quando o IBM Installation Manager retrocede um pacote para uma versão anterior, a versão atual dos arquivos do pacote é desinstalada e uma versão anterior é reinstalada.

Para retroceder para uma versão anterior, o IBM Installation Manager deve acessar arquivos para essa versão. Por padrão, esses arquivos são salvos durante cada instalação sucessiva. Como o número de arquivos salvos aumenta com cada versão instalada, talvez você queira excluir esses arquivos do seu sistema em um planejamento regular. No entanto, se você excluir os arquivos, não poderá retroceder para uma versão anterior.

Para excluir os arquivos salvos ou atualizar sua preferência para salvar esses arquivos em instalações futuras, conclua as etapas a seguir:

1. No IBM Installation Manager, clique em **Arquivo** > **Preferências**.
2. Na página **Preferências**, clique em **Arquivos para Retrocesso** e especifique sua preferência.

Procedimento

- Para retroceder para uma versão anterior do Operations Center, use a função **Retroceder** do IBM Installation Manager.

Apêndice A. Arquivos de Log de Instalação

Se ocorrerem erros durante a instalação, estes erros serão registrados em arquivos de log que estão armazenados no diretório de logs do IBM Installation Manager.

É possível visualizar arquivos de log de instalação clicando em **Arquivo** > **Visualizar Log** na ferramenta Installation Manager. Para coletar estes arquivos de log, clique em **Ajuda** > **Exportar Dados para Análise de Problemas** na ferramenta Installation Manager.

Apêndice B. Recursos de Acessibilidade para a Família de Produtos IBM Spectrum Protect

Os recursos de acessibilidade ajudam os usuários que possuem uma deficiência, como mobilidade restrita ou visão limitada, a usar o conteúdo de tecnologia da informação com êxito.

Visão Geral

A família de produtos IBM Spectrum Protect inclui os principais recursos de acessibilidade a seguir:

- Operação apenas do teclado
- Operações que usam um leitor de tela

A família de produtos IBM Spectrum Protect usa o padrão W3C mais recente, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), para assegurar conformidade com o US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) e Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). Para aproveitar os recursos de acessibilidade, use a liberação mais recente do seu leitor de tela e o último navegador da web que seja suportado pelo produto.

A documentação do produto no IBM Knowledge Center é ativada para acessibilidade. Os recursos de acessibilidade do IBM Knowledge Center estão descritos na Seção Acessibilidade da ajuda do IBM Knowledge Center (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

Navegação pelo Teclado

Esse produto usa as chaves de navegação padrão

Informações sobre a Interface

As interfaces com o usuário não têm conteúdo que pisca 2-55 vezes por segundo.

Interfaces com o usuário da web dependem de folhas de estilo em cascata para renderizar o conteúdo corretamente e para fornecer uma experiência utilizável. O aplicativo fornece uma maneira equivalente para os usuários com visão reduzida usarem as configurações de exibição do sistema, incluindo o modo de alto contraste. É possível controlar o tamanho da fonte usando as configurações do dispositivo ou do navegador da web.

As interfaces com o usuário da web incluem referências de navegação WAI-ARIA que podem ser usadas para navegar rapidamente para áreas funcionais no aplicativo.

Software do Fornecedor

A família de produtos do IBM Spectrum Protect inclui determinado software de fornecedor que não é coberto pelo contrato de licença da IBM. A IBM não representa nenhum recurso de acessibilidade desses produtos. Entre em contato com o fornecedor para obter informações de acessibilidade sobre estes produtos.

Informações sobre acessibilidade relacionadas

Além dos websites padrão do IBM help desk e do suporte, a IBM tem um serviço telefônico TTY para ser usado por clientes com deficiência auditiva para acessar os serviços de suporte e vendas:

Serviço de TTY
800-IBM-3383 (800-426-3383)
(na América do Norte)

Para obter informações adicionais sobre o compromisso que a IBM tem com a acessibilidade, consulte Acessibilidade IBM (www.ibm.com/able).

Aviso

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos. Este material pode estar disponível na IBM em outros idiomas. No entanto, pode ser necessário possuir uma cópia do produto ou da versão de produto no mesmo idioma para acessá-lo.

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 sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a um produto, programa ou serviço IBM não afirma ou significa que apenas que o produto, programa ou serviço IBM pode ser usado. 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 concede ao Cliente nenhum direito sobre tais patentes. Pedidos de licenças 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:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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.

Esta publicação pode 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 fazer aperfeiçoamentos e/ou alterações nos produtos ou programas descritos nesta publicação a qualquer momento sem aviso prévio.

As referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites 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) o uso mútuo 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 neste documento e todo o material licenciado disponível para ele são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato de Licença de Programa Internacional IBM ou de qualquer outro contrato equivalente entre as partes.

Os dados de desempenho discutidos aqui são apresentados como derivados sob as condições de operação específicas. Os resultados reais podem variar.

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 aos fornecedores desses produtos.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos incluem nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com os 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. Os programas de amostra são fornecidos "NO ESTADO EM QUE SE ENCONTRAM", sem garantia de qualquer tipo. A IBM não poderá ser responsabilizada por quaisquer danos decorrentes ao uso dos programas de amostra.

Qualquer cópia, parte desses programas de amostra ou trabalho derivado deve incluir um aviso de copyright da seguinte forma: © (o nome de sua empresa) (ano). Partes deste código são derivadas dos Programas de Amostra da IBM Corp. © Copyright IBM Corp. _digite o ano ou anos_.

Marcas

IBM, o logotipo IBM e ibm.com são marcas registradas ou comerciais da International Business Machines Corp., registradas em vários países no mundo todo. Outros nomes de produtos e serviços podem ser marcas registradas da IBM ou de outras empresas. Uma lista atual de marcas comerciais IBM está disponível na web em "Copyright and trademark information" em www.ibm.com/legal/copytrade.shtml.

Adobe é uma marca registrada da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

Linear Tape-Open, LTO e Ultrium são marcas comerciais da HP, IBM Corp. e Quantum nos Estados Unidos e em outros países.

Intel e Itanium são marcas comerciais ou marcas registradas da Intel Corporation ou de suas subsidiárias nos Estados Unidos e em outros países.

A marca registrada Linux é usada conforme uma sublicença da Linux Foundation, a licenciada exclusiva de Linus Torvalds, proprietário da marca em nível mundial.

Microsoft, Windows e Windows NT são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países.

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

Red Hat®, OpenShift®, Ansible® e Ceph® são marcas comerciais ou marcas registradas da Red Hat, Inc. ou de suas subsidiárias nos Estados Unidos e em outros países.

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.

VMware, VMware vCenter Server e VMware vSphere são marcas registradas ou marcas comerciais da VMware, Inc. ou de suas subsidiárias nos Estados Unidos e/ou em outras jurisdições.

Termos e Condições para a Documentação do Produto

As permissões para uso dessas publicações são concedidas sujeitas aos termos e condições a seguir.

Aplicabilidade
Esses termos e condições são adicionais a quaisquer termos de uso para o website da IBM.

utilizar o Personal
Você pode reproduzir estas publicações para seu uso pessoal não comercial desde que todos os avisos do proprietário sejam preservados. O Cliente não pode distribuir, exibir ou fazer trabalho derivado destas publicações, ou de parte delas, sem o consentimento expresso da IBM.

Uso comercial
É possível reproduzir, distribuir e exibir estas publicações exclusivamente dentro de sua empresa desde que todos os avisos do proprietário sejam preservados. O Cliente não pode fazer trabalhos derivados destas publicações ou reproduzir, distribuir ou exibir estas publicações, ou qualquer parte delas, fora de sua empresa, sem o consentimento expresso da IBM.

Direitos
Exceto como expressamente concedido nesta permissão, nenhuma outra permissão, licença ou direito é concedido, seja expresso ou implícito, para as publicações ou para quaisquer informações, dados, software ou outra propriedade intelectual nelas contidos.

A IBM reserva-se o direito de retirar as permissões concedidas aqui sempre que, a seu critério, o uso das publicações prejudicar seus interesses ou, conforme determinação da IBM, as instruções anteriores não estão sendo seguidas adequadamente.

O Cliente não pode fazer download, exportar ou reexportar estas informações, exceto em conformidade total com todas as leis e regulamentos aplicáveis, incluindo todas as leis e regulamentos de exportação dos Estados Unidos.

A IBM NÃO GARANTE O CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS "NO ESTADO EM QUE SE ENCONTRAM", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO A, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO, NÃO INFRAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO.

Considerações sobre política de privacidade

Os produtos de Software IBM, incluindo as soluções de software como serviço (“Ofertas de Software”), podem usar cookies ou outras tecnologias para coletar informações sobre o uso do produto, para ajudar a melhorar a experiência do usuário final, para customizar interações com o usuário final ou para outros propósitos. Em muitos casos, nenhuma informação pessoalmente identificável é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem permitir a coleta de informações identificáveis pessoalmente. Se esta Oferta de Software usar cookies para coletar informações de identificação pessoal, informações específicas sobre o uso de cookies desta oferta serão apresentadas abaixo.

Esta Oferta de Software não usa cookies ou outras tecnologias para coletar informações pessoalmente identificáveis.

Se as configurações implementadas para esta Oferta de software fornecerem a você, como cliente, a capacidade de coletar informações de identificação pessoal de usuários finais por meio de cookies e outras tecnologias, é necessário buscar seu próprio conselho jurídico legal sobre quaisquer leis aplicáveis a este tipo de coleção de dados, incluindo quaisquer requisitos de aviso e consentimento.

Para obter informações adicionais sobre o uso de várias tecnologias, incluindo cookies, para estes propósitos, consulte a Política de privacidade da IBM em http://www.ibm.com/privacy e a Declaração de privacidade on-line da IBM em http://www.ibm.com/privacy/details na seção intitulada “Cookies, Web Beacons and Other Technologies” e “IBM Software Products and Software-as-a-Service Privacy Statement” em http://www.ibm.com/software/info/product-privacy.

Glossário

Está disponível um glossário com termos e definições para a família de produtos IBM Spectrum Protect.

Consulte o IBM Spectrum Protectglossário.

Índice Remissivo

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

Número do Programa: 5725-W99
5725-W98
5725-X15