IBM Spectrum Protect
Versão 8.1.10

Guia de solução de fita

Observação:

Antes de utilizar essas informações e o produto que elas suportam, leia as informações em “Aviso” na página 221.

Aviso de Edição

Esta edição aplica-se à versão 8, liberação 1, modificação 10 do IBM Spectrum Protect (números do produto 5725-W98, 5725-W99, 5725-X15) e a todas as liberações e modificações subsequentes até que haja outro tipo de indicação em novas edições.

Índice

Sobre esta publicação

Esta publicação fornece informações sobre como planejar, implementar, monitorar e operar uma solução de proteção de dados que usa as melhores práticas do IBM Spectrum Protect.

Quem Deve Ler este Guia

Esse guia a destinado a qualquer pessoa que está registrada como um administrador do IBM Spectrum Protect. Um único administrador pode gerenciar o IBM Spectrum Protect, ou várias pessoas podem compartilhar responsabilidades administrativas.

É necessário estar familiarizado com o sistema operacional no qual o servidor reside e com os protocolos de comunicação requeridos para o ambiente do cliente ou do servidor. Também é necessário entender as práticas de gerenciamento de armazenamento de sua organização, sobre como você está atualmente fazendo backup de arquivos da estação de trabalho e como está usando dispositivos de armazenamento.

Publicações

A família de produtos IBM Spectrum Protect inclui o IBM Spectrum Protect Plus, Ambientes IBM Spectrum Protect for Virtual, 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 nesta liberação

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

Para obter uma lista de novos recursos e atualizações desta liberação, consulte os tópicos a seguir:

- O que há de novo nos componentes do servidor
- O que há de novo nos componentes do cliente

As informações novas e alteradas nesta documentação de produto são indicadas por uma barra vertical (|) à esquerda da mudança.

Parte 1. Planejando-se para uma solução de proteção de dados baseada em fita

Planeje uma solução de proteção de dados que inclua operações de backup de disco para disco para fita e de disco para fita para otimizar o armazenamento.

Planejando o roteiro
Planeje a solução de fita revisando o layout da arquitetura em Figura 1 na página 1 e, em seguida, concluindo as tarefas de roteiro que seguem o diagrama.

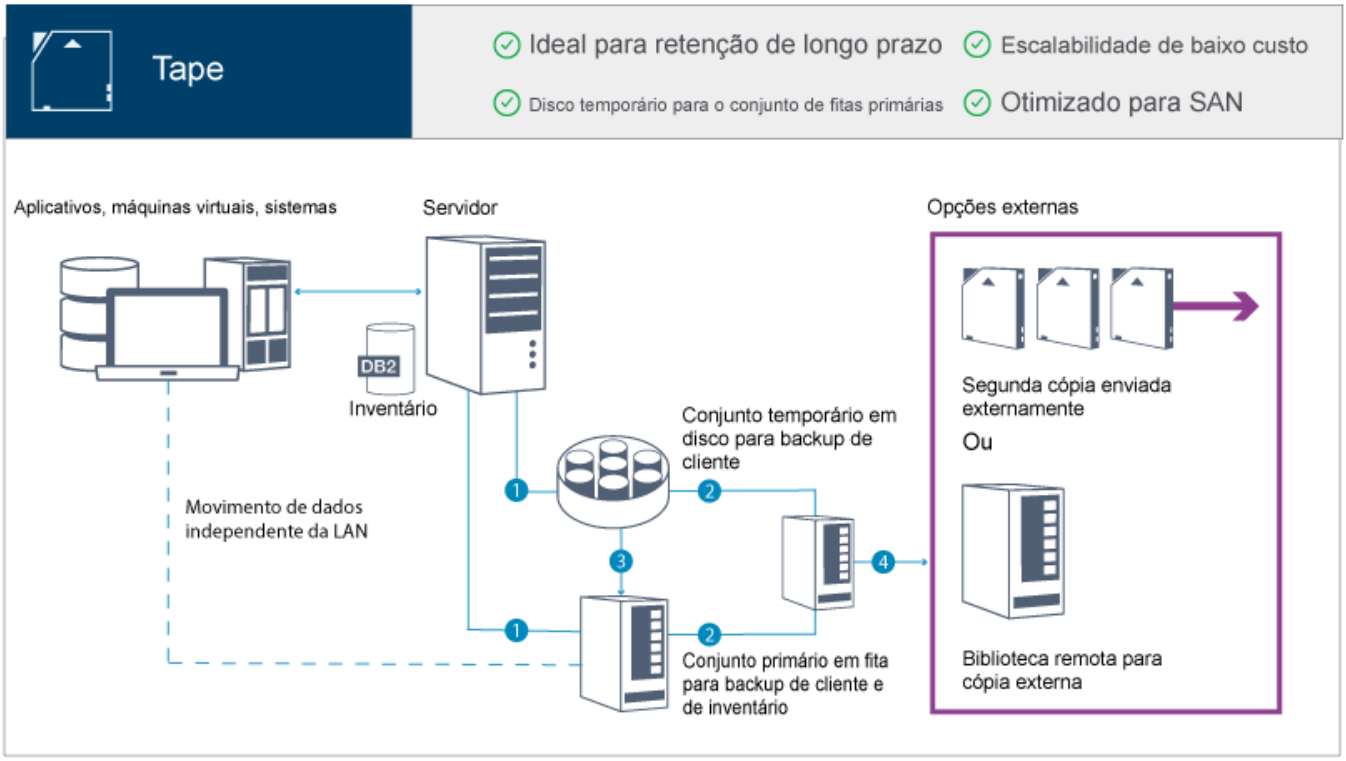


Figura 1. Solução de fita

Nesta configuração de proteção de dados, o servidor usa o hardware de armazenamento em disco e em fita. É usada a preparação do conjunto de armazenamentos, na qual os dados de cliente são inicialmente armazenados em conjuntos de armazenamentos em disco e, posteriormente, migrados para conjuntos de armazenamentos em fita. Para recuperação de desastre, os volumes de fita podem ser armazenados externamente. As opções externas incluem mover fisicamente uma segunda cópia externa por um transportador ou cópias de criação de área segura eletronicamente externas para uma biblioteca remota.

Dicas:

- Na solução descrita, os dados são *migrados* de conjuntos de armazenamento em disco para conjuntos de armazenamentos de fita. No entanto, em vez de migrar os dados, é possível usar o recurso de definição de camada para a fita que foi introduzido no IBM Spectrum Protect Versão 8.1.8. Com esse recurso, é possível classificar automaticamente os dados de camadas dos conjuntos de armazenamento em contêiner de diretório no disco para o armazenamento em fita. É possível especificar que todos os dados sejam em camadas com base em um limite de idade especificado ou que apenas os dados inativos sejam em camadas com base em um limite de idade. Para obter mais informações sobre a definição de camada de dados para armazenamento em fita, consulte Dados de definição de camada para armazenamento em nuvem ou em fita.

- A solução descrita não inclui replicação de nó. Se você deseja usar a replicação do nó para fazer backup de um conjunto de armazenamentos de disco em disco, verifique se a operação de replicação foi concluída antes que os dados sejam migrados do disco para a fita. Também é possível usar a replicação de nó para fazer backup de um conjunto de armazenamentos em um dispositivo de fita local para um conjunto de armazenamento de cópia em um dispositivo de fita local.

Para planejar-se para uma solução baseada em fita, conclua as seguintes tarefas:

1. Atenda aos requisitos do sistema para hardware e software.
2. Registre valores para configuração do seu sistema nas planilhas de planejamento.
3. Planeje-se para armazenamento em disco.
4. Planeje-se para armazenamento em fita.
5. Planeje a segurança.

Requisitos de planejamento de fita

Antes de implementar uma solução de fita, revise as diretrizes gerais sobre os requisitos do sistema. Determine se deve ser feito backup de dados para o disco ou para a fita ou uma combinação de ambos.

Largura da banda da rede
A rede deve ter largura da banda suficiente para as transferências de dados esperadas entre o cliente e o servidor, e para as operações de restauração entre sites que são necessárias para a recuperação de desastre. Use uma rede de área de armazenamento (SAN) para transferências de dados entre o servidor, os dispositivos de disco e os dispositivos de fita. Para obter informações adicionais, consulte “Requisitos de Hardware” na página 3.

Migração de dados
Migre todos os dados do disco para a fita diariamente. Especifique uma classe de dispositivo FILE para conjuntos de armazenamentos baseados em disco. Planeje a migração para controlar quando o processamento ocorre. Para evitar a migração automática com base no limite de migração, especifique um valor de 100 para o parâmetro **HIGHMIG** e 0 para o parâmetro **LOWMIG** quando emitir o comando **DEFINE STGPOOL**. Você deve manter pelo menos 20% das unidades de fita disponíveis para operações de restauração. Para usar até 80% das unidades de fita disponíveis e melhorar o desempenho do rendimento, especifique o parâmetro **MIGPROCESS**.

Considere as seguintes informações com base no tipo de dados que são migrados:

- Use uma fita para fazer backup de dados de clientes que têm objetos grandes, como banco de dados.

  Dica: Verifique com seu fabricante de unidade de fita para obter orientação sobre o tamanho do banco de dados que é adequado para gravação em fita.
- Use o disco para fazer backup de dados de clientes que têm objetos menores.
- Para fazer backup de dados diretamente para a fita, use a movimentação de dados sem LAN. Para obter informações adicionais, consulte “Configurando a Movimentação de Dados sem LAN” na página 117.
- Não faça backup de máquinas virtuais para fita. Use um conjunto de armazenamentos baseado em disco separado que não migra para um conjunto de armazenamentos baseado em fita. Para obter informações adicionais sobre o suporte de máquina virtual, consulte O suporte ao IBM Spectrum Protect e ao guest IBM Tivoli Storage Manager (TSM) para máquinas virtuais e virtualização.

Capacidade do conjunto de armazenamentos
Mantenha a capacidade do conjunto de armazenamentos suficiente para permitir 2 dias de backups do cliente e um buffer de 20%. Pode ser necessário planejar backups completos durante alguns dias para assegurar que você tenha espaço do conjunto de armazenamentos suficiente.

Unidades de fita

Revise as especificações do fabricante e estime a capacidade de uma unidade de fita. Determine a quantidade de espaço que é necessário para operações de backup e migração. Reserve 20% de unidades de fita para operações de restauração.

Informações relacionadas

MIGRATE STGPOOL (Migrar conjunto de armazenamento para próximo conjunto de armazenamento)

Requisitos do sistema para uma solução baseada em fita

Os requisitos de hardware e de software são fornecidos para uma solução de armazenamento baseada em fita que tem uma taxa de ingestão de dados de 14 TB por hora.

Revise as informações para determinar os requisitos de hardware e de software para seu ambiente de armazenamento. Poderá ser necessário fazer ajustes com base no tamanho do seu sistema.

Requisitos de Hardware

Os requisitos de hardware para sua solução IBM Spectrum Protect são baseados no tamanho do sistema. Escolha componentes equivalentes ou melhores que os itens que estão listados para assegurar o desempenho ideal para seu ambiente.

Para obter informações adicionais sobre como planejar dispositivos de disco, consulte Planejando o armazenamento em disco.

Para obter informações adicionais sobre como planejar dispositivos de fita, consulte Planejando o armazenamento em fita.

A tabela a seguir inclui requisitos mínimos de hardware para o servidor e armazenamento. Se estiver usando partições locais (LPARs) ou partições de trabalho (WPARs), ajuste os requisitos de rede para considerar os tamanhos de partições. As figuras na tabela são baseadas em uma taxa de ingestão de dados de 14 TB por hora.

Componente de hardware	Requisitos do sistema
Processador do servidor	AIX 8 núcleos do processador, 3.42 GHz ou mais rápido. Por exemplo, use um servidor baseado em processador POWER8. Linux Windows 16 núcleos do processador, 2.0 GHz ou mais rápido. Por exemplo, use um processador Intel Xeon.
Memória do servidor	64 GB de RAM.
Rede	O seguinte dimensionamento gerencia aproximadamente 14 TB de dados por hora: • Ethernet de 10 Gb (um mínimo de quatro portas) • Adaptador Fibre Channel de 8 Gb (um mínimo de quatro portas) O número de portas depende da porcentagem de ingestão de dados diária para conjuntos de armazenamentos em disco versus armazenamento em fita. Use adaptadores Fibre Channel separados para dados de fita e de disco.

Componente de hardware	Requisitos do sistema

Armazenamento	**Disco**
	Com base na quantidade de dados que estão sendo gravados em disco, especifique o número de discos necessários.
	Assegure-se de que o rendimento sequencial de entrada/saída (E/S) da rede de área de armazenamento (SAN) corresponda ao rendimento de E/S para a rede na linha anterior.
	Por exemplo, se deve ser feito o backup de 10 TB de dados em uma janela de quatro horas, o rendimento será de aproximadamente 700 MB por segundo. Nesse caso, o servidor requererá uma rede de front-end (caminho cliente-para-servidor) que suporte um rendimento mínimo de 700 MB por segundo. A SAN do backend (o caminho do dispositivo servidor-para-armazenamento) também deverá suportar um rendimento mínimo de 700 MB por segundo.
	Para calcular a velocidade do disco necessária, use as seguintes fórmulas:
	`(Quantidade total de ingestão de dados diária - quantidade de ingestão de dados diária diretamente na fita) ÷ (Número de horas para operações de backup do cliente diárias) = Megabytes de ingestão de dados para o disco por hora`
	`(Megabytes de ingestão de dados para o disco por hora) ÷ (3600 segundos por hora) = Megabytes de ingestão de dados por segundo que devem ser suportados pela tecnologia de disco`
	Tape
	Selecione a tecnologia de fita que melhor atende às suas necessidades de negócios. Por exemplo, use unidades de fita IBM Linear Tape-Open (LTO) ou IBM TS1150. Certifique-se de que tenha pontos de montagem suficientes para operações de backup do cliente e para migração. Para obter informações adicionais sobre como planejar o armazenamento em fita, consulte Planejando o armazenamento em fita. Para obter uma lista de dispositivos de fita suportados, consulte IBM Support Portal for IBM Spectrum Protect.
	Dica: Para otimizar a movimentação de dados, use a movimentação de dados sem LAN.

Adaptadores de E/S SAN	Separe a E/S de disco e fita. Para obter informações adicionais sobre como selecionar um adaptador, consulte a documentação para produtos de hardware Brocade e para soluções de armazenamento IBM Storwize. **Disco** Use pelo menos dois adaptadores. **Tape** Use pelo menos dois adaptadores.

Estimando requisitos de espaço para o Operations Center

Os requisitos de hardware para o Operations Center estão incluídos na tabela anterior, exceto para o banco de dados e espaço do log de archive (inventário) que o Operations Center usa para conter registros para clientes gerenciados.

Se você não planeja instalar o Operations Center no mesmo sistema que o servidor IBM Spectrum Protect, é pode estimar os requisitos do sistema separadamente. Para calcular os requisitos do sistema para o Operations Center, consulte a calculadora dos requisitos do sistema na nota técnica 1641684.

O gerenciamento do Operations Center no servidor IBM Spectrum Protect é uma carga de trabalho que requer espaço extra para operações do banco de dados no servidor do hub e em servidores spoke. A

quantidade de espaço no servidor do hub para o log de archive será maior se o servidor do hub estiver monitorando um ou mais servidores spoke. Revise as seguintes diretrizes para estimar a quantidade de espaço requerido por seu servidor IBM Spectrum Protect.

Espaço de banco de dados para o Operations Center

O Operations Center usa aproximadamente 4,4 GB de espaço de banco de dados para cada 1000 clientes que são monitorados nesse servidor. Este cálculo se aplica a servidores do hub e a servidores spoke em uma configuração.

Por exemplo, considere um servidor do hub com 2000 clientes que também gerencia três servidores spoke, cada um com 1000 clientes. Essa configuração tem um total de 5000 clientes entre os quatro servidores. Cada um dos servidores spoke requer 4,4 GB de espaço de banco de dados. Se os servidores spoke estiverem no IBM Spectrum Protect Versão 8.1.2 ou mais recente, o servidor do hub irá requerer 8,8 GB de espaço de banco de dados para monitorar somente seus 2000 clientes:

```
(4,4 GB x 2) = 8,8 GB
```

Espaço de banco de dados para dados gerenciados

Dados gerenciados são a quantidade de dados protegidos, incluindo a quantidade de dados para todas as versões retidas.

- Para tipos de clientes que executam backups incrementais contínuos, a seguinte fórmula pode ser usada para estimar o total de dados gerenciados:

  ```
  Front-end + (front-end × taxa de mudança × (retenção - 1))
  ```

  Por exemplo, se você fizer backup de 100 TB de dados de front-end, use um período de retenção de 30 dias e tenha uma taxa de mudança de 5%, calcule o seu total de dados gerenciados usando as figuras a seguir:

  ```
  100 TB + (100 TB × 0,05 × (30-1)) = total de 245 TB de dados gerenciados
  ```

- Para tipos de clientes que executam backups completos todos os dias, a seguinte fórmula pode ser usada para estimar o total de dados gerenciados:

  ```
  Front-end × retenção × (1 + taxa de mudança)
  ```

  Por exemplo, se você fizer backup de 10 TB de dados de front-end, use um período de retenção de 30 dias e tenha uma taxa de mudança de 3%, calcule o seu total de dados gerenciados usando as figuras a seguir:

  ```
  10 TB × 30 × (1 + .03) = Total de 309 TB de dados gerenciados
  ```

  Dados não estruturados, média de tamanho do objeto: 4 MB

  Dados estruturados, média de tamanho do objeto: 128 MB

  Dados não estruturados, número de objetos =

  `(245 TB × 1024 × 1024) / 4 MB = 64225280`

  Dados estruturados, número de objetos =

  `(309 TB × 1024 × 1024) / 128 MB = 2531328`

  Número total de objetos: 66756608

  Custo de dados gerenciados (1 KB por objeto) =

  `(66756608 KB) / (1024 × 1024) = 63,66 GB`

  Planeje 20% de espaço adicional para que os sistemas de banco de dados não fiquem com 100% da capacidade:

  ```
  Total de requisitos de armazenamento físico do banco de dados =
  (espaço para dados gerenciados + Espaço do Operations Center) × (1,20)
  ```

Para esse exemplo, você calcula o espaço usando os seguintes números:

```
(66,33 GB + 8,4 GB) × 1,20 = 76,41 GB
```

Espaço de log de archive

O Operations Center usa aproximadamente 18 GB de espaço de log de archive a cada 24 horas, por servidor, para cada 1000 clientes monitorados nesse servidor. Além disso, para cada 1000 clientes que são monitorados em servidores spoke, o espaço de log de archive adicional é usado no servidor do hub. Para servidores spoke na V8.1.2 ou mais recentes, essa quantidade incluída é de 1,2 GB de espaço de log de archive no servidor do hub por 1000 clientes monitorados a cada 24 horas.

Por exemplo, considere um servidor do hub com 2000 clientes que também gerencia três servidores spoke, cada um com 1000 clientes. Essa configuração tem um total de 5000 clientes entre os quatro servidores. É possível calcular o espaço de log de archive para o servidor do hub usando a seguinte fórmula:

```
((18 GB x 2) + (1,2 GB x 3)) = 39,6 GB de espaço de log de archive
```

Essas estimativas são baseadas no intervalo de coleta de status padrão de 5 minutos. Se você reduzir o intervalo de coleta de uma vez a cada 5 minutos para uma vez a cada 3 minutos, os requisitos de espaço aumentarão. Os exemplos a seguir mostram o aumento aproximado nos requisitos de espaço de log com um intervalo de coleta de uma vez a cada 3 minutos para uma configuração na qual servidores spoke V8.1.2 ou mais recente são monitorados:

- Servidor do hub: No intervalo de 39,6 GB a 66 GB
- Cada servidor spoke: no intervalo de 18 GB a 30 GB

Aloque espaço de log de archive para que seja possível suportar o Operations Center sem afetar operações do servidor.

Requisitos de Software

A documentação para a solução baseada em fita do IBM Spectrum Protect inclui tarefas de instalação e de configuração para os sistemas operacionais IBM AIX, Linux® e Microsoft Windows. É necessário atender aos requisitos mínimos de software que são listados.

Para obter informações sobre os requisitos de software para a IBM em drivers de dispositivo de fita, consulte o IBM Tape Device Drivers: Guia de Instalação e do Usuário.

Sistemas AIX

Tipo de software	Requisitos Mínimos de Software
Sistema Operacional	IBM AIX 7.1 Para obter mais informações sobre os requisitos do sistema operacional, consulte AIX: requisitos mínimos do sistema para sistemas AIX.
Utilitário Gunzip	O utilitário gunzip deve estar disponível em seu sistema antes de instalar ou fazer o upgrade do IBM Spectrum Protect . Certifique-se de que o utilitário gunzip esteja instalado e o caminho para ele esteja configurado na variável de ambiente PATH.

Tipo de software	Requisitos Mínimos de Software
Tipo de sistema de arquivos	Sistemas de arquivos JFS2 Os sistemas AIX podem armazenar em cache uma grande quantidade de dados do sistema de arquivos, o que pode reduzir a memória necessária para os processos do servidor e do IBM Db2. Para evitar paginação com o servidor AIX, use a opção de montagem `rbrw` para o sistema de arquivos JFS2. Menos memória é usada para o cache do sistema de arquivos e mais está disponível para o IBM Spectrum Protect. Não use as opções de montagem do sistema de arquivos, Concurrent I/O (CIO) e Direct I/O (DIO), para sistemas de arquivos que contêm o banco de dados do IBM Spectrum Protect, logs ou volumes do conjunto de armazenamentos. Essas opções podem causar degradação de desempenho de muitas operações do servidor. O IBM Spectrum Protect e o Db2 ainda podem usar o DIO se isso for benéfico, mas o IBM Spectrum Protect não requererá as opções de montagem para aproveitar seletivamente essas técnicas.
Outro software	Korn Shell (ksh)

Sistemas Linux

Tipo de software	Requisitos Mínimos de Software
Sistema Operacional	Red Hat Enterprise Linux 7 (x86_64)
Bibliotecas	Bibliotecas GNU C, Versão 2.3.3-98.38 ou posterior, que estejam instaladas no sistema IBM Spectrum Protect. Red Hat Enterprise Linux Servers: • libaio • libstdc++.so.6 (os pacotes de 32 bits e de 64 bits são necessários) • numactl.x86_64
Tipo de sistema de arquivos	Sistemas de arquivos relacionados ao banco de dados de formato com ext3 ou ext4. Para sistemas de arquivos relacionados ao conjunto de armazenamentos, use XFS.
Outro software	Korn Shell (ksh)

Sistemas Windows

Tipo de software	Requisitos Mínimos de Software
Sistema Operacional	Microsoft Windows Server 2012 R2 (64 bits) ou Windows Server 2016
Tipo de sistema de arquivos	NTFS

Tipo de software	Requisitos Mínimos de Software
Outro software	O Windows 2012 R2 ou Windows 2016 com .NET Framework 3.5 está instalado e ativado. As políticas a seguir de Controle de Conta do Usuário devem ser desativadas: • Controle de Conta do Usuário: Modo de Aprovação do Administrador para contagem do Administrador Integrado • Controle de Conta do Usuário: Execute todos os administradores no Modo de Aprovação do Administrador

Planilhas de planejamento

Use as planilhas de planejamento para registrar valores que são usados para configurar o sistema e configurar o servidor do IBM Spectrum Protect. Use os valores padrão de melhor prática que estão listados nas planilhas.

Cada planilha ajuda-o a preparar-se para diferentes partes da configuração do sistema usando valores de melhor prática:

Pré-configuração do sistema do servidor
Use as planilhas de pré-configuração para planejar os sistemas de arquivos e diretórios criados ao configurar sistemas de arquivos para o IBM Spectrum Protect durante a configuração de sistema. Todos os diretórios que você criar para o servidor devem estar vazios.

Configuração do servidor
Use as planilhas de configuração quando configurar o servidor. Os valores padrão são sugeridos para a maioria dos itens, exceto onde indicado.

Tabela 1. Planilha para pré-configuração de um sistema do servidor

Item	Valor padrão	Seu valor	Tamanho mínimo do diretório	Informações adicionais
Endereço de porta TCP/IP para comunicações com o servidor	1500		Não aplicável.	Certifique-se de que essa porta esteja disponível ao instalar e configurar o sistema operacional. O número da porta pode ser um número no intervalo de 1024 a 32767.

Tabela 1. Planilha para pré-configuração de um sistema do servidor (continuação)				
Item	**Valor padrão**	**Seu valor**	**Tamanho mínimo do diretório**	**Informações adicionais**
Diretório da instância do servidor	Linux AIX `/home/tsminst1/tsminst1` Windows `C:\tsminst1`		AIX 50 GB. Linux Windows 25 GB.	Se você mudar o valor padrão do diretório de instância do servidor, modifique também o valor do proprietário da instância do Db2 no Tabela 2 na página 10.
Diretório para instalação de servidor	• Linux AIX `/` • Windows `C:`		AIX Espaço disponível que é necessário para o diretório: 5 GB. Linux Windows Espaço mínimo que é necessário para o diretório: 30 GB	
Diretório para instalação de servidor	`/usr`		AIX Espaço disponível que é necessário para o diretório: 5 GB.	
Diretório para instalação de servidor	AIX `/var`		AIX Espaço disponível que é necessário para o diretório: 5 GB.	
Diretório para instalação de servidor	AIX `/tmp`		AIX Espaço disponível que é necessário para o diretório: 5 GB.	
Diretório para instalação de servidor	AIX `/opt`		AIX Espaço disponível que é necessário para o diretório: 10 GB.	
Diretório para o log ativo	Linux AIX `/tsminst1/TSMalog` Windows `C:\tsminst1\TSMalog`		128 GB.	Ao criar o log ativo durante a configuração inicial do servidor, configure o tamanho como 128 GB.

Tabela 1. Planilha para pré-configuração de um sistema do servidor (continuação)				
Item	**Valor padrão**	**Seu valor**	**Tamanho mínimo do diretório**	**Informações adicionais**
Diretório para o log de archive	Linux AIX /tsminst1/TSMarchlog Windows C:\tsminst1\TSMarchlog		3 TB.	
Diretórios para o banco de dados	Linux AIX /tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 Windows C:\tsminst1\TSMdbspace00 C:\tsminst1\TSMdbspace01 C:\tsminst1\TSMdbspace02 C:\tsminst1\TSMdbspace03		Para obter instruções sobre como calcular requisitos de espaço, consulte “Requisitos de Hardware” na página 3.	Crie quatro sistemas de arquivos para o banco de dados.
Diretórios para armazenamento	Linux AIX /tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ... Windows C:\tsminst1\TSMfile00 C:\tsminst1\TSMfile01 C:\tsminst1\TSMfile02 C:\tsminst1\TSMfile03 ...		Determine o mínimo de capacidade total para todos os diretórios usando o seguinte cálculo: `Diário percentage of ingested data that is written to disk + 20% = Minimum total capacity`	O método preferencial é definir pelo menos um diretório para cada dispositivo de fita.

Tabela 2. Planilha para configuração do IBM Spectrum Protect			
Item	**Valor padrão**	**Seu valor**	**Informações adicionais**
Proprietário da instância do Db2	tsminst1		Se você mudou o valor padrão do diretório de instância do servidor no Tabela 1 na página 8, modifique também o valor para o proprietário da instância do Db2.

Tabela 2. Planilha para configuração do IBM Spectrum Protect (continuação)			
Item	**Valor padrão**	**Seu valor**	**Informações adicionais**

Senha do proprietário da instância do Db2	Linux AIX
	`passw0rd`
	Windows
	`pAssW0rd`
			Selecione um valor para a senha do proprietário da instância diferente do padrão. Certifique-se de registrar esse valor em um local seguro.

Grupo primário para o proprietário da instância do Db2	Linux AIX `tsmsrvrs`		
Nome do Servidor	O valor padrão para o nome do servidor é o nome do host do sistema.		
Senha do servidor	`passw0rd`		Selecione um valor diferente do padrão para a senha do servidor. Certifique-se de registrar esse valor em um local seguro.
ID de administrador: ID do usuário para a instância do servidor	`admin`		
Senha de ID de administrador	`passw0rd`		Selecione um valor diferente do padrão para a senha do administrador. Certifique-se de registrar esse valor em um local seguro.

Tabela 2. Planilha para configuração do IBM Spectrum Protect (continuação)			
Item	**Valor padrão**	**Seu valor**	**Informações adicionais**
Horário de início do planejamento	23h00		O horário de início de planejamento padrão inicia a fase de carga de trabalho do cliente, que são predominantemente as atividades de backup e archive do cliente. Durante a fase de carga de trabalho do cliente, os recursos do servidor suportam operações do cliente. Normalmente, essas operações são concluídas durante a janela de planejamento noturna. Os planejamentos para operações de manutenção do servidor são definidos para iniciar 10 horas após o início da janela de backup do cliente. Neste guia, o horário sugerido para iniciar operações de backup do cliente é 23h.

Tabela 3. Planilha para configuração da fita			
Item	**Valor padrão**	**Seu valor**	**Informações adicionais**
Arquivos de dispositivo robótico	Dispositivos IBM com um driver de dispositivo de fita IBM: • AIX /dev/smcX • Linux /dev/IBMchangerX • Windows ChangerX Dispositivos não IBM com um driver de dispositivo IBM Spectrum Protect: • AIX /dev/lbX • Linux /dev/tsmscsi/lbX • Windows lbA.B.C.D		Para definir manualmente os arquivos de dispositivo de biblioteca, use os seguintes comandos: • **DEFINE LIBRARY** • **DEFINE DRIVE** • **DEFINE PATH** Para SCSI, é possível usar o comando **PERFORM LIBACTION** para definir todas as unidades e seus caminhos para uma única biblioteca em uma etapa. Para usar esse comando para definir todas as unidades e caminhos, a opção SANDISCOVERY deve ser suportada e ativada.

Tabela 3. Planilha para configuração da fita (continuação)			
Item	**Valor padrão**	**Seu valor**	**Informações adicionais**
Unidades de fita	Dispositivos IBM com um driver de dispositivo de fita IBM: • AIX /dev/rmtX • Linux /dev/IBMtapeX • Windows TapeX Dispositivos não IBM com um driver de dispositivo IBM Spectrum Protect: • AIX /dev/mtX • Linux /dev/tsmscsi/mtX • Windows mtA.B.C.D		

Planejando para armazenamento em disco

Escolha a tecnologia de armazenamento mais eficaz para componentes do IBM Spectrum Protect para assegurar o desempenho e operações eficientes do servidor.

Os dispositivos de hardware de armazenamento possuem diferentes características de capacidade e desempenho, que determinam como podem ser usadas de forma eficiente com o IBM Spectrum Protect. Para obter orientação geral sobre como selecionar o hardware de armazenamento e a configuração apropriados para sua solução, revise as seguintes diretrizes.

Banco de dados, log ativo e log de archive

- Use um disco de estado sólido (SSD) ou um disco rápido, de 15.000 rpm para o banco de dados e log ativo do IBM Spectrum Protect.
- Ao criar matrizes para o banco de dados, use o nível do RAID 5.
- Use discos separados para o log de archive e armazenamento de backup de banco de dados.

Conjunto de armazenamentos

Use o nível 6 do RAID para matrizes do conjunto de armazenamentos para incluir proteção contra falhas de unidades duplas ao usar tipos de discos grandes.

Planejando as matrizes de armazenamento

Prepare a configuração de armazenamento em disco planejando matrizes e volumes RAID de acordo com o tamanho do sistema IBM Spectrum Protect.

Você projeta as matrizes de armazenamento com características de tamanho e de desempenho que sejam adequadas para um dos componentes de armazenamento do servidor do IBM Spectrum Protect, como o banco de dados do servidor ou um conjunto de armazenamentos. A atividade de planejamento de armazenamento deve considerar o tipo de unidade, o nível do RAID, o número de unidades, o número de unidades sobressalentes, etc. Nas configurações de solução, os grupos de armazenamentos contêm matrizes RAID de armazenamento interno e consistem em vários discos físicos que são apresentados como volumes lógicos no sistema. Ao configurar o sistema de armazenamento em disco, você cria grupos de armazenamentos, ou conjuntos de armazenamentos de dados e, em seguida, cria matrizes de armazenamento nos grupos.

Você cria volumes, ou LUNs, a partir dos grupos de armazenamentos. O grupo de armazenamentos define quais discos fornecem o armazenamento que forma o volume. Ao criar volumes, torne-os totalmente alocados. Os tipos de discos mais rápidos são usados para conter os volumes do banco de dados e volumes de log ativo. Os tipos de discos mais lentos podem ser usados para os volumes do conjunto de armazenamentos, log de archive e volumes de backup de banco de dados. Se você usar um conjunto de armazenamentos em disco menor para estagiar dados, poderá ser necessário usar discos mais rápidos para gerenciar o desempenho da carga de trabalho diária para ingerir e migrar dados.

A Tabela 4 na página 14 e a Tabela 5 na página 14 descrevem os requisitos de layout para grupos de armazenamentos e configuração de volume.

Tabela 4. Componentes de configuração do grupo de armazenamentos

Componente	**Detalhes**
Requisito de armazenamento do servidor	Como o armazenamento é usado pelo servidor.
Tipo de disco	Tamanho e velocidade para o tipo de disco que é usado para o requisito de armazenamento.
Quantidade de disco	Número de cada tipo de disco que é necessário para o requisito de armazenamento.
Capacidade de hot spare	Número de discos que são reservados como sobressalentes para assumir o controle se ocorrerem falhas de disco.
Nível do RAID	Nível de matriz RAID que é usado para armazenamento lógico. O nível do RAID define o tipo de redundância que é fornecido pela matriz, por exemplo, 5 ou 6.
Quantidade de matrizes RAID	Número de matrizes RAID a serem criadas.
DDMs por matriz RAID	Quantos módulos da unidade de disco (DDMs) devem ser usados em cada uma das matrizes RAID.
Tamanho utilizável por matriz RAID	Tamanho que está disponível para armazenamento de dados em cada matriz RAID após contabilizar o espaço perdido devido à redundância.
Tamanho utilizável total	Tamanho total que está disponível para armazenamento de dados nas matrizes RAID: `Quantidade x tamanho utilizável`
Nomes sugeridos de grupos de armazenamentos e de matrizes	Nome preferencial a ser usado para MDisks e grupos de MDisk.
Uso	Componente do servidor que usa parte do disco físico.

Tabela 5. Componentes da configuração de volume

Componente	**Detalhes**
Requisito de armazenamento do servidor	Requisito para o qual o disco físico é usado.
Nome do volume	Nome exclusivo que é dado a um volume específico.

Tabela 5. Componentes da configuração de volume (continuação)	
Componente	**Detalhes**
Grupo de armazenamentos	Nome do grupo de armazenamento do qual o espaço é obtido para criar o volume.
Tamanho	Tamanho de cada volume.
Ponto de montagem do servidor desejado	Diretório no sistema do servidor no qual o volume é montado.
Quantidade	Número de volumes a serem criados para um requisito específico. Use o mesmo padrão de nomenclatura para cada volume que é criado para o mesmo requisito.
Uso	Componente do servidor que usa parte do disco físico.

Exemplos

Exemplos de configuração para grupos de armazenamentos e volumes estão disponíveis no link a seguir: Exemplos de planilhas para o planejamento de matrizes de armazenamento. Os exemplos mostram como planejar o armazenamento para tamanhos de servidores diferentes. Nas configurações de exemplo, há um mapeamento um-para-um entre discos e grupos de armazenamentos. É possível fazer download dos exemplos e editar as planilhas para planejar a configuração de armazenamento para seu servidor.

Planejando para armazenamento em fita

Determine quais dispositivos de fita usar e como configurá-los. Para otimizar o desempenho do sistema, planeje usar dispositivos de fita rápidos, de alta capacidade. Forneça unidades de fita suficientes para atender às suas necessidades de negócios.

Dispositivos de fita e bibliotecas suportados

O servidor pode usar uma ampla variedade de dispositivos de fita e de bibliotecas. Selecione dispositivos de fita e as bibliotecas que atendam às suas necessidades de negócios.

Para obter uma lista de dispositivos e de formatos de classes de dispositivos válidos suportados, consulte o website para seu sistema operacional:

- AIX Windows Dispositivos Suportados para AIX e Windows
- Linux Dispositivos Suportados para Linux

Para obter informações adicionais sobre dispositivos de armazenamento e objetos de armazenamento, consulte Tipos de dispositivos de armazenamento.

Cada dispositivo que for definido para o IBM Spectrum Protect é associado a uma *classe de dispositivo*. A classe de dispositivo especifica as informações de tipo de dispositivo e de gerenciamento de mídia, como o formato de gravação, a capacidade estimada e prefixos de rotulagem.

Um *tipo de dispositivo* identifica um dispositivo como um membro de um grupo de dispositivos que compartilham características de mídia semelhantes. Por exemplo, o tipo de dispositivo LTO se aplica a todas as gerações de unidades de fita LTO.

Uma classe de dispositivo para uma unidade de fita também deve especificar uma biblioteca. Uma *biblioteca física* é uma coleção de uma ou mais unidades que compartilham requisitos semelhantes de montagem de mídia. Ou seja, a unidade pode ser montada por um operador ou por um mecanismo de montagem automatizado.

Uma *definição de objeto de biblioteca* especifica o tipo de biblioteca e outras características que estiverem associadas a esse tipo de biblioteca.

A tabela a seguir lista os tipos de biblioteca preferenciais para uma solução de fita do IBM Spectrum Protect Versão 8.1.6 .

Tabela 6. Tipos de biblioteca para uma solução de fita do IBM Spectrum Protect 8.1.6

Tipo de biblioteca	**descrição**	**Informações adicionais**
SCSI	Uma biblioteca SCSI é controlada por meio de uma interface SCSI, conectada diretamente ao host do servidor usando cabeamento SCSI ou por uma rede de área de armazenamento. Um robô ou outro mecanismo manipula automaticamente as montagens e desmontagens de volumes de fita. Se criar diferentes tipos de unidades para uma biblioteca SCSI, você cria várias bibliotecas lógicas que não podem ser divididas entre diferentes tipos de unidades. Uma biblioteca SCSI pode conter unidades de tecnologias combinadas, incluindo unidades LTO Ultrium e digital linear tape (DLT). Por exemplo: • A biblioteca do Oracle StorageTek L700 • O dispositivo de fita IBM 3592	"Configurando bibliotecas para uso por um servidor" na página 87 As restrições se aplicam ao combinar diferentes gerações de mídia e unidades. Para obter mais informações, consulte: • "Combinando gerações de unidades e mídia 3592 em uma única biblioteca" na página 95 • "Combinando unidades e mídia LTO em uma biblioteca" na página 92
Compartilhado	Bibliotecas compartilhadas são bibliotecas lógicas que são representadas por SCSI. A biblioteca é controlada pelo servidor do IBM Spectrum Protect que estiver configurado como um gerenciador de biblioteca. Os servidores do IBM Spectrum Protect que usam o tipo de biblioteca SHARED são clientes de biblioteca para o servidor do gerenciador de bibliotecas. As bibliotecas compartilhadas fazem referência a um gerenciador de biblioteca.	

Configurações do dispositivo de fita suportadas

Revise as informações sobre redes locais (LAN) e redes de área de armazenamento (SAN). Para otimizar a movimentação de dados, planeje configurar a movimentação de dados sem LAN. Além disso, considere se usar compartilhamento de biblioteca.

Selecione a configuração do dispositivo que atenda às suas necessidades de negócios.

Movimentação de dados baseada em LAN e sem LAN

É possível mover dados entre clientes e dispositivos de armazenamento que estão conectados a uma rede local (LAN), ou a dispositivos de armazenamento que estão conectados a uma rede de área de armazenamento (SAN), conhecida como movimentação de dados sem LAN.

Em uma configuração de LAN convencional, uma ou mais bibliotecas de fitas estão associadas a um único servidor IBM Spectrum Protect. A movimentação de dados sem LAN torna uma largura da banda de LAN disponível para outros usos e reduz a carga no servidor IBM Spectrum Protect.

Em uma configuração de LAN, as informações de dados de cliente, e-mail, conexão de terminal, programa de aplicativo e de controle de dispositivo devem ser manipuladas pela mesma rede. As informações de controle de dispositivo e os dados de backup e restauração do cliente fluem pela LAN.

Uma SAN é uma rede de armazenamento dedicado que pode melhorar o desempenho do sistema.

Usando o IBM Spectrum Protect em uma SAN, você se beneficia das seguintes funções:

- Compartilhando dispositivos de armazenamento entre múltiplos servidores do IBM Spectrum Protect.

  Restrição: Um dispositivo de armazenamento com o tipo de dispositivo GENERICTAPE não pode ser compartilhado entre servidores.
- Movendo dados de cliente do IBM Spectrum Protect diretamente para dispositivos de armazenamento (movimentação de dados sem a LAN) configurando um agente de armazenamento no sistema do cliente.

Em um SAN, é possível compartilhar unidades de fita e bibliotecas que sejam suportadas pelo servidor do IBM Spectrum Protect, incluindo os dispositivos de fita SCSI mais recentes.

Quando servidores IBM Spectrum Protect compartilham uma fita SCSI, um servidor, o *gerenciador de biblioteca*, possui e controla o dispositivo. Os agentes de armazenamento, junto com outros servidores IBM Spectrum Protect que compartilham essa biblioteca são *clientes de biblioteca*. Um cliente de biblioteca solicita recursos da biblioteca compartilhada, como unidades ou mídia, do gerenciador de biblioteca, mas usa os recursos de forma independente. O gerenciador de biblioteca coordena o acesso a esses recursos. Os servidores do IBM Spectrum Protect que estiverem definidos como clientes de biblioteca usam comunicação entre servidores para entrar em contato com o gerente da biblioteca e com o serviço de dispositivo da solicitação. Os dados são movidos para o SAN entre cada servidor e o dispositivo de armazenamento.

Exigência: Se você definir um servidor do gerenciador de bibliotecas que é compartilhado com o servidor IBM Spectrum Protect, a opção **SANDISCOVERY** deve ser configurada como ON. Por padrão, essa opção é configurada como OFF.

Os servidores do IBM Spectrum Protect usam os seguintes recursos ao compartilhar uma biblioteca automatizada:

Particionamento do inventário de volume
O inventário de volumes de mídia na biblioteca compartilhada é particionado entre os servidores. Qualquer servidor possui um volume específico ou o volume está no conjunto inicial global. Nenhum servidor possui o conjunto inicial.

Acesso serializado à unidade
Apenas um servidor acessa cada unidade de fita por vez. O acesso da unidade é serializado. O IBM Spectrum Protect controla o acesso da unidade, para que os servidores não desmontem os volumes de outros servidores ou gravem em unidades onde outros servidores montam seus volumes.

Acesso de montagem serializado
O alterador de mídia de biblioteca conclui uma operação de montagem ou de desmontagem por vez. O gerenciador de biblioteca conclui todas as operações de montagem para fornecer essa serialização.

Compartilhamento da biblioteca

É possível otimizar a eficiência de sua solução de fita configurando compartilhamento de biblioteca. O compartilhamento de biblioteca permite que múltiplos servidores do IBM Spectrum Protect usem a mesma biblioteca e unidades de fita em uma rede de área de armazenamento (SAN) e melhorar o desempenho do backup e de recuperação e a utilização de hardware de fita.

Quando os servidores do IBM Spectrum Protect compartilham uma biblioteca, um servidor é configurado como o gerenciador de biblioteca e controla as operações da biblioteca, como montagem e desmontagem. O gerenciador de biblioteca também controla propriedade de volume e inventário de biblioteca inventário de biblioteca. Outros servidores são configurados como clientes de biblioteca e usam comunicação servidor-para-servidor para entrar em contato com o gerente da biblioteca e solicitar recursos.

Os clientes da biblioteca devem estar na mesma versão ou anterior do servidor do gerenciador de bibliotecas. Um gerenciador de biblioteca não pode suportar clientes da biblioteca que estiverem em uma versão mais recente. Para obter mais informações, consulte Compatibilidade do agente de armazenamento e do cliente de biblioteca com um servidor IBM Spectrum Protect.

Movimento de dados independente da LAN

O IBM Spectrum Protect fornece o recurso para um cliente, por meio de um agente de armazenamento, para fazer backup e restaurar dados diretamente para uma biblioteca de fitas em uma SAN. Este tipo de movimentação de dados também é conhecido como movimentação de dados sem a LAN.

Restrição: Dispositivos de armazenamento Centera não podem ser destinos para operações sem a LAN.

A Figura 2 na página 18 mostra uma configuração de SAN na qual um cliente acessa diretamente uma fita para ler ou gravar dados.

Figura 2. Movimento de dados independente da LAN

A movimentação de dados sem LAN requer a instalação de um agente de armazenamento no sistema do cliente. O servidor mantém o banco de dados e o log de recuperação e age como o gerenciador de biblioteca para controlar as operações do dispositivo. O agente de armazenamento no cliente manipula a transferência de dados para o dispositivo na SAN. Essa implementação libera largura de banda na LAN que de outra forma seria utilizada para movimentação de dados do cliente.

Tipos de dispositivos combinados em bibliotecas

O IBM Spectrum Protect suporta a mistura de diferentes tipos de dispositivos dentro de uma única biblioteca automatizada, se a biblioteca puder distinguir entre a mídia diferente para os diferentes tipos de dispositivos. Para simplificar o processo de configuração, não planeje combinar tipos de dispositivos diferentes dentro de uma biblioteca. Se tiver que combinar tipos de dispositivo, revise as restrições.

As bibliotecas com esse recurso são modelos que possuem unidades combinadas integradas, ou que suportam a inclusão de unidades combinadas. Para obter informações sobre modelos específicos,

consulte a documentação do fabricante. Para aprender sobre bibliotecas que foram testadas no IBM Spectrum Protect com tipos de dispositivo combinados, consulte as informações para seu sistema operacional:

- Dispositivos suportados do IBM Spectrum Protect para AIX, HP-UX, Solaris e Windows
- Dispositivos suportados do IBM Spectrum Protect for Linux

Por exemplo, é possível ter unidades LTO Ultrium e unidades IBM TS4500 em uma única biblioteca que é definida para o servidor IBM Spectrum Protect.

Diferentes gerações de mídia em uma biblioteca
O servidor IBM Spectrum Protect permite tipos de dispositivos combinados em uma biblioteca automatizada, mas a combinação de diferentes gerações do mesmo tipo de unidade geralmente não é suportada. Novas unidades não podem gravar em formatos de mídia mais antigos e unidades antigas não podem ler novos formatos. As unidades LTO Ultrium são uma exceção a essa regra.

Se a nova tecnologia de unidade não puder gravar em mídia que é formatada por unidades de geração mais antigas, a mídia mais antiga deverá ser marcada como somente leitura para evitar problemas de operações do servidor. Além disso, as unidades mais antigas devem ser removidas da biblioteca, ou as definições das unidades mais antigas devem ser removidas do servidor. Por exemplo, o servidor IBM Spectrum Protect não suporta o uso de unidades Oracle StorageTek 9940A com unidades 9940B em combinação com outros tipos de dispositivo em uma única biblioteca.

Em geral, o IBM Spectrum Protect não suporta a combinação de gerações de unidades LTO Ultrium e mídia. No entanto, as combinações a seguir são suportadas:

- LTO Ultrium Geração 3 (LTO-3) com LTO Ultrium Geração 4 (LTO-4)
- LTO Ultrium Geração 4 (LTO-4) com LTO Ultrium Geração 5 (LTO-5)
- LTO Ultrium Geração 5 (LTO-5) com LTO Ultrium Geração 6 (LTO-6)
- LTO Ultrium Geração 6 (LTO-6) com LTO Ultrium Geração 7 (LTO-7)
- Mídia LTO Ultrium Geração 7 (LTO-7) com mídia LTO Ultrium Geração 8 (LTO-8 e LTO-M8) em uma biblioteca com unidades de fita LTO-8 ou uma biblioteca com unidades de fita LTO-8 e LTO-7 combinadas

O servidor suporta essas combinações, já que unidades diferentes podem ler e gravar em mídia diferente. Se você planeja fazer upgrade de todas as unidades para Geração 4 (ou Geração 5, 6, 7 ou 8), deve-se excluir todas as definições de unidades LTO Ultrium existentes e os caminhos que estão associados a elas. Em seguida, é possível definir as novas unidades e os caminhos Geração 4 (ou Geração 5, 6, 7 ou 8).

Restrições que se aplicam à combinação de unidades de fita e mídia LTO Ultrium

- As unidades LTO-5 podem ser somente mídia LTO-3. Se estiver combinando unidades e mídia LTO-3 com LTO-5 em uma única biblioteca, deve marcar a mídia LTO-3 como somente leitura. Você deve efetuar check-out de todos os volumes utilizáveis LTO-3.
- As unidades LTO-6 podem ler somente mídia LTO-4. Se estiver combinando unidades e mídia LTO-4 com LTO-6 em uma única biblioteca, deve marcar a mídia LTO-4 como somente leitura. Você deve efetuar check-out de todos os volumes utilizáveis LTO-4.
- As unidades LTO-7 podem ser somente mídia LTO-5. Se estiver combinando unidades e mídia LTO-5 com LTO-7 em uma única biblioteca, deve marcar a mídia LTO-5 como somente leitura. Você deve efetuar check-out de todos os volumes utilizáveis LTO-5.
- As unidades LTO-8 não conseguem ler a mídia LTO-6. Se você estiver combinando unidade e mídia LTO-6 e LTO-8 em uma única biblioteca, deverá particionar a biblioteca em duas bibliotecas. Uma biblioteca tem somente unidades e mídia LTO-8 e a outra tem unidades e mídia LTO-6.

Restrições que se aplicam a unidades de fita LTO Ultrium de geração combinada em uma biblioteca
Você deve usar cartuchos de fita que são de uma geração anterior à unidade de fita. Uma unidade de fita de geração mais recente pode ler e gravar dados em um cartucho de fita de geração anterior. Por exemplo, se uma biblioteca tiver unidades de fita LTO-7 e LTO-6, você deve usar cartuchos de fita LTO-6. As unidades de fita LTO-7 e LTO-6 podem ler e gravar dados em cartuchos de fita LTO-6.

Restrições que se aplicam a cartuchos de fita LTO Ultrium de geração combinada em uma biblioteca
Você deve usar um cartucho de fita que é da mesma geração que a unidade de fita, ou de uma geração anterior. Por exemplo, se uma biblioteca tiver unidades de fita LTO-7, será possível usar cartuchos de fita LTO-7 ou cartuchos de fita LTO-7 e LTO-6 combinados. Se essa biblioteca tiver cartuchos de fita LTO-7, LTO-6 e LTO-5, deverá mudar o modo de acesso para READONLY para os cartuchos de fita LTO-5.

Para saber sobre considerações adicionais ao combinar gerações de LTO Ultrium, consulte "Definindo classes de dispositivo LTO" na página 92.

Ao usar o IBM Spectrum Protect, não será possível combinar unidades que forem gerações de unidades 3592, TS1130, TS1140, TS1150 e mais recentes. Use uma das três configurações especiais. Para obter detalhes, consulte a seção "Definindo classes de dispositivo 3592" na página 95.

Se você planeja criptografar volumes em uma biblioteca, não combine gerações de mídia na biblioteca.

Mídia e conjuntos de armazenamentos combinados
É possível otimizar a eficiência de sua solução de fita ao não combinar formatos de mídia em um conjunto de armazenamentos. Em vez de combinar formatos, mapeie cada formato de mídia exclusivo para um conjunto de armazenamentos separado usando sua própria classe de dispositivo. Essa restrição também se aplica aos formatos LTO.

Múltiplos conjuntos de armazenamentos e suas classes de dispositivo de diferentes tipos podem apontar para a mesma biblioteca que pode suportá-los, conforme descrito em "Diferentes gerações de mídia em uma biblioteca" na página 19.

É possível migrar para uma nova geração de um tipo de mídia dentro do mesmo conjunto de armazenamentos seguindo estas etapas:

1. Substitua todas as unidades mais antigas pelas unidades de geração mais novas dentro da biblioteca. As unidades devem ser combinadas.
2. Marque como somente leitura os volumes existentes com os formatos mais antigos se a nova unidade não puder anexar essas fitas no formato antigo. Se a nova unidade puder gravar na mídia existente no formato antigo, isso não será necessário, mas a Etapa 1 ainda será necessária. Se for necessário manter diferentes gerações de unidades que são lidas mas não são compatíveis com gravação na mesma biblioteca, use conjuntos de armazenamentos separados para cada uma.

Definições necessárias para dispositivos de armazenamento em fita

Antes que o servidor do IBM Spectrum Protect possa usar um dispositivo de fita, deve-se configurar o dispositivo para o sistema operacional e para o servidor. Como parte do processo de planejamento, determine quais definições são necessárias para seus dispositivos de armazenamento em fita.

Dica: É possível usar o comando **PERFORM LIBACTION** para simplificar o processo ao incluir dispositivos para tipos de biblioteca SCSI e VTL.

O Tabela 7 na página 20 resume as definições que são necessárias para tipos de dispositivos diferentes.

Tabela 7. Definições necessárias para dispositivos de armazenamento

Dispositivo	Tipos de Dispositivo	Definições necessárias			
		Biblioteca	**Unidade**	**Caminho**	**Classe de dispositivo**
Disco magnético	DISCO	—	—	—	Sim [1]
	FILE [2]	—	—	—	SIM
	AIX Windows CENTERA Linux CENTERA [3]	—	—	—	SIM

Tabela 7. Definições necessárias para dispositivos de armazenamento (continuação)					
Dispositivo	**Tipos de Dispositivo**	**Definições necessárias**			
		Biblioteca	**Unidade**	**Caminho**	**Classe de dispositivo**
Tape	3590 3592 DLT LTO NAS VOLSAFE AIX Windows GENERICTAPE ECARTRIDGE [4]	SIM	Sim	Sim	SIM
Mídia removível (sistema de arquivos)	REMOVABLEFILE	SIM	SIM	Sim	SIM

1. A classe de dispositivo DISK existe na instalação e não pode ser mudada.
2. Bibliotecas, unidades e caminhos FILE são necessários para compartilhamento com agentes de armazenamento.
3. Linux O tipo de dispositivo CENTERA está disponível somente para sistemas Linux x86_64.
4. O tipo de dispositivo ECARTRIDGE é para unidades de fita de cartucho Oracle StorageTek, como unidades 9840 e T10000.

Planejando a hierarquia do conjunto de armazenamentos

Planeje a hierarquia do conjunto de armazenamentos para assegurar os dados sejam migrados diariamente do disco para a fita. A migração libera espaço no dispositivo de disco e move os dados para a fita para retenção de longo prazo. Dessa forma, é possível aproveitar a escalabilidade, a eficiência de custo e recursos de segurança do armazenamento em fita.

Antes de Iniciar

A hierarquia do conjunto de armazenamentos ajuda a gerenciar o fluxo de dados. Para entender o fluxo de dados, revise Figura 3 na página 22.

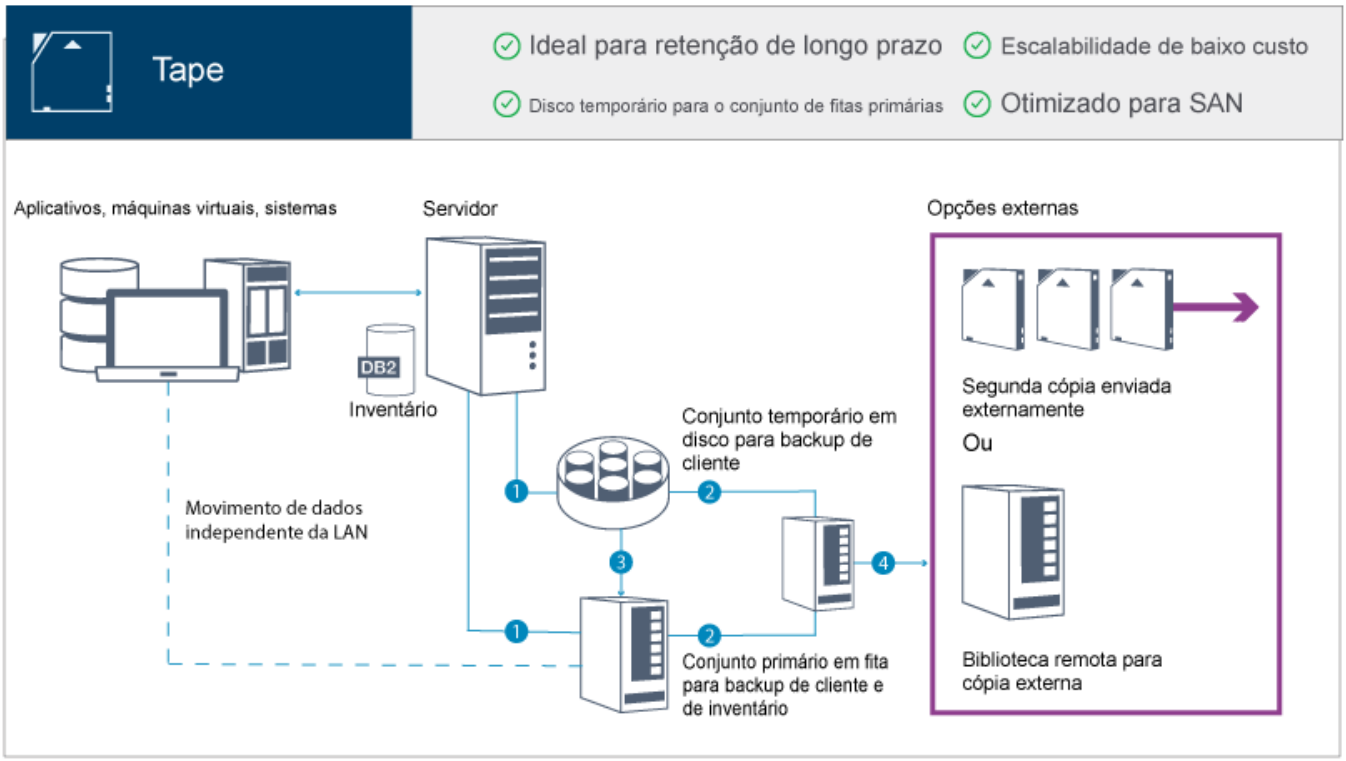


Figura 3. Solução de fita

As seguintes etapas correspondem aos números na figura:

1. O servidor recebe dados de clientes (aplicativos, máquinas virtuais ou sistemas) e armazena os dados em conjuntos de armazenamentos primários. Dependendo do tipo de cliente, os dados são armazenados em um conjunto de armazenamentos primários em disco ou fita.
2. É feito backup dos dados em disco e fita para um conjunto de armazenamento de cópia na fita.
3. Os dados no conjunto de armazenamentos primários em disco são migrados diariamente para o conjunto de armazenamentos primários em fita.
4. Os dados do conjunto de armazenamento de cópia em fita são movidos externamente para suportar a retenção de longo prazo e a recuperação de desastre.

Procedimento

Para planejar a hierarquia do conjunto de armazenamentos, responda às seguintes perguntas:

a. Quais clientes devem fazer backup de dados para o disco e quais clientes devem fazer backup de dados para a fita?

- O método preferencial é fazer backup dos clientes que hospedam grandes objetos, como bancos de dados, para a fita.
- O método preferencial é fazer backup de todos os outros clientes para o disco.
- Pode ser feito backup de clientes de máquina virtual (VM) para o disco ou fita. O método preferencial é fazer backup de um cliente de VM para um conjunto de armazenamentos em disco separado, que não é migrado para a fita. Se tiver que migrar um cliente de VM para a fita, crie um conjunto de armazenamentos em disco menor para conter os arquivos de controle do VMware. Este conjunto de armazenamentos em disco menor não pode ter permissão para migrar para a fita. Para obter informações adicionais sobre como fazer backup de um cliente de VM para a fita, consulte Diretrizes da mídia de fita e O suporte ao IBM Spectrum Protect e ao guest IBM Tivoli Storage Manager (TSM) para máquinas virtuais e virtualização.

Dica: Se muitos clientes tiverem que fazer backup de dados para um único conjunto de armazenamentos, considere usar um conjunto de armazenamentos em disco, porque é possível

especificar muitos pontos de montagem. É possível especificar um valor máximo de 999 para o parâmetro **MAXNUMMP** no comando **REGISTER NODE**.

b. Quais são as considerações para especificar a capacidade de conjuntos de armazenamentos baseados em disco?

   No mínimo, planeje capacidade suficiente para armazenar dados de um único dia de operações de backup. O método preferencial é planejar capacidade suficiente para armazenar dados de dois dias de operações de backup e incluir um buffer de 20%.

c. Quais são as considerações para especificar a classe de dispositivo para o conjunto de armazenamentos baseado em disco?

   O método preferencial é especificar uma classe de dispositivo FILE. Configure o parâmetro **MOUNTLIMIT** como 4000. Além disso, certifique-se de que o nó tenha um número suficientemente alto de pontos de montagem, que pode ser especificado usando o parâmetro **MAXNUMMP** no comando **REGISTER NODE**.

d. A deduplicação de dados deve ser especificada para o conjunto de armazenamentos em disco?

   Não, porque os dados são armazenados em disco somente por um dia antes de serem migrados para a fita.

e. A migração automática de dados deve ser especificada com base em um limite de migração?

   Não. Em vez disso, planeje a programação de migração diária usando o comando **MIGRATE STGPOOL**. (Para evitar a migração automática com base no limite de migração, especifique um valor de 100 para o parâmetro **HIGHMIG** e 0 para o parâmetro **LOWMIG** quando emitir o comando **DEFINE STGPOOL**.)

f. Um atraso de migração deve ser especificado?

   O método preferencial é especificar a migração do disco para a fita diariamente, e não especificar um atraso de migração, que requer planejamento adicional. Para obter informações adicionais sobre atrasos de migração, consulte Migrando arquivos em uma hierarquia do conjunto de armazenamentos.

g. Como o número de unidades de fita pode ser calculado?

   1) Determine a taxa de transferência de dados nativa da unidade, revisando a documentação do fabricante. Para obter uma estimativa da taxa de transferência de dados suportada em seu ambiente de armazenamento, subtraia 30% da taxa de transferência de dados nativos.
   2) Calcule a taxa necessária de ingestão de dados pelo servidor. Em seguida, divida esse número pela taxa de transferência de dados suportada de um único dispositivo de fita. O resultado é o número mínimo de unidades para suportar a ingestão de dados.
   3) Calcule o número de pontos de montagem que são requeridos por clientes que fazem backup de dados para a fita, incluindo os clientes que usam várias sessões. É possível distribuir os pontos de montagem na janela de backup, considerando que os clientes provavelmente estão fazendo backup de objetos grandes, o que pode usar a maior parte da janela.
   4) Calcule os requisito de desempenho *e* os pontos de montagem que são necessários para tarefas de manutenção, como migração de disco para fita e cópias de fita para fita. Ao fazer backup de dados para a fita, é possível evitar o processamento de migração, mas fazer cópias de fita para fita irá dobrar o requisito da unidade de fita.
   5) Calcule o número de unidades adicionais que podem ser necessárias, por exemplo:

      - Se uma unidade de fita tiver mau funcionamento, o problema afeta o número de pontos de montagem disponíveis e a taxa de ingestão. Considere o fornecimento de unidades sobressalentes. Por exemplo, se você precisar de cinco unidades de fita para operações normais, considere o fornecimento de duas unidades sobressalentes.
      - Operações de restauração e recuperação podem requerer unidades de fita adicionais, se você planeja executar as operações simultaneamente com ingestão de dados e operações de manutenção. Se necessário, forneça unidades de fita adicionais e certifique-se de que elas não tenham sido utilizadas quando iniciar as operações de restauração ou recuperação.

h. Quais alternativas estão disponíveis para otimizar as operações de restauração?

É possível usar a disposição para melhorar o desempenho do sistema e otimizar a organização de dados. A disposição pode reduzir o número de volumes que devem ser acessados quando uma grande quantidade de dados tiver que ser restaurada:

- Para conjuntos de armazenamentos baseados em disco, o método preferencial é usar a disposição por nó. O servidor armazena os dados para o nó no menor número de volumes possível.
- Para conjuntos de armazenamentos baseados em fita, o método preferencial é usar a disposição por grupo. A disposição por grupo resulta em uma redução da capacidade de fita não usada, que permite mais dados dispostos em fitas individuais.

Para obter informações adicionais sobre a disposição, consulte "Otimizando operações ativando a disposição de arquivos do cliente" na página 167.

Se você for um administrador do sistema experiente, pode planejar ações adicionais para otimizar operações de restauração. Consulte Otimizando operações de restauração para clientes, Técnicas de Backup de Arquivo e MOVE NODEDATA (Mover dados por nó em um conjunto de armazenamento de acesso sequencial).

Armazenamento de dados externo

Para facilitar a recuperação de dados e como parte de sua estratégia de recuperação de desastre, armazene cópias de fita externas.

Use a função do gerenciador de recuperação de desastre (DRM) para configurar e gerar automaticamente um plano de recuperação de desastres que contém as informações, scripts e procedimentos que são necessários para restaurar automaticamente o servidor e recuperar dados do cliente após um desastre. Escolha uma das seguintes opções de armazenamento de dados externo como uma estratégia de recuperação de desastre para proteger cópias de fita:

Criação de área segura externa de um único site de produção
Volumes de armazenamento, como cartuchos de fita e volumes da mídia, são colocados em uma área segura em um local externo. Um transportador transporta os dados do recurso de armazenamento externo para o site de recuperação. Se ocorrer um desastre, os volumes são enviados de volta para o site de produção após a restauração do hardware e do servidor IBM Spectrum Protect.

Criação de área segura externa com um site de recuperação
Um transportador move volumes de armazenamento do site de produção para um recurso de armazenamento externo. Tendo um site de recuperação dedicado, é possível reduzir o tempo de recuperação em comparação com o único site de produção. No entanto, essa opção aumenta o custo da recuperação de desastre, porque mais hardwares e softwares devem ser mantidos. Por exemplo, o site de recuperação deve ter dispositivos de fita e o software do servidor do IBM Spectrum Protect compatíveis. Antes da recuperação do site de produção, o hardware e o software no site de recuperação devem estar configurados e em execução.

Segurança Eletrônica
Para usar a criação de área segura eletrônica como uma estratégia de recuperação de desastre, o site de recuperação deve ter um servidor IBM Spectrum Protect em execução. Os dados críticos são colocados em uma área segura eletronicamente do site de produção para o site de recuperação. O DRM também é usado para criação de área segura externa de dados não críticos. A criação de área segura eletrônica move dados críticos externos mais rapidamente e mais frequentemente do que os métodos de transporte tradicionais. O tempo de recuperação é reduzido porque os dados críticos já estão armazenados no site de recuperação. No entanto, como o site de recuperação é executado continuamente, o custo da estratégia de recuperação de desastre é mais caro do que o da criação de área segura externa.

Conceitos relacionados

Preparando para um desastre e recuperando-se de um desastre usando o DRM
O IBM Spectrum Protect fornece uma função gerenciador de recuperação de desastre (DRM) para recuperar seus dados do servidor e do cliente durante um desastre.

Planejando a segurança

Planeje proteger a segurança de sistemas na solução do IBM Spectrum Protect com controles de acesso e autenticação, e considere criptografar a transmissão de dados e de senha.

Planejando funções de administrador

Defina os níveis de autoridade que você deseja designar a administradores que têm acesso à solução do IBM Spectrum Protect.

É possível designar um dos seguintes níveis de autoridade a administradores:

Sistema
Administradores com autoridade do sistema têm o nível de autoridade mais alto. Os administradores com este nível de autoridade podem concluir qualquer tarefa. Eles podem gerenciar todos os domínios de política e conjuntos de armazenamentos e conceder autoridade a outros administradores.

Política
Os administradores que possuem autoridade de política podem gerenciar todas as tarefas relacionadas ao gerenciamento de política. Esse privilégio pode ser irrestrito ou pode ser restrito a domínios de política específicos.

Armazenamento
Os administradores que possuírem autoridade de armazenamento podem alocar e controlar recursos de armazenamento para o servidor.

Operador
Os administradores que possuírem autoridade de operador podem controlar a operação imediata do servidor e a disponibilidade de mídia de armazenamento, como bibliotecas e unidades de fitas.

Os cenários na Tabela 8 na página 25 fornecem exemplos sobre por que talvez você queira designar níveis variados de autoridade para que os administradores possam executar tarefas:

Tabela 8. Cenários para funções de administrador

Cenário	Tipo de ID de administrador para configuração
Um administrador em uma empresa pequena gerencia o servidor e é responsável por todas as atividades do servidor.	• Autoridade do sistema: 1 ID de administrador
Um administrador para vários servidores também gerencia o sistema geral. Vários outros administradores gerenciam seus próprios conjuntos de armazenamentos.	• Autoridade do sistema em todos os servidores: 1 ID de administrador para o administrador do sistema geral • Autoridade de armazenamento para conjuntos de armazenamentos designados: 1 ID de administrador para cada um dos outros administradores
Um administrador gerencia 2 servidores. Outra pessoa ajuda com as tarefas de administração. Dois assistentes são responsáveis por ajudar a assegurar que seja feito backup dos sistemas importantes. Cada assistente é responsável por monitorar os backups planejados em um dos servidores do IBM Spectrum Protect.	• Autoridade do sistema em ambos os servidores: 2 IDs de administrador • Autoridade de operador: 2 IDs de administrador para os assistentes com acesso ao servidor pelo qual cada pessoa é responsável

Tarefas relacionadas
Gerenciando administradores

Um administrador que tem autoridade do sistema pode concluir qualquer tarefa com o servidor IBM Spectrum Protect, incluindo designar níveis de autoridade a outros administradores. Para concluir algumas tarefas, deve-se ter recebido autoridade sendo designado a um ou mais níveis de autoridade.

Planejando comunicações seguras

Planejar-se para proteger as comunicações entre os componentes da solução IBM Spectrum Protect.

Determine o nível de proteção que é necessário para seus dados, com base nos regulamentos e necessidades de negócios nos quais sua empresa opera.

Se sua empresa requer um alto nível de segurança para senhas e transmissão de dados, planeje implementar a comunicação segura com os protocolos Segurança da Camada de Transporte (TLS) ou Secure Sockets Layer (SSL).

O TLS e o SSL fornecem comunicações seguras entre o servidor e o cliente, mas podem afetar o desempenho do sistema. Para melhorar o desempenho do sistema, use TLS para autenticação sem criptografar dados do objeto. Para especificar se o servidor usa o TLS 1.2 para a sessão inteira ou apenas para autenticação, consulte a opção do cliente SSL para comunicação cliente-para-servidor e o parâmetro **UPDATE SERVER=SSL** para a comunicação servidor-para-servidor. A partir da versão V8.1.2, o TLS é usado para autenticação por padrão. Se você decidir usar TLS para criptografar sessões inteiras, use o protocolo somente para sessões em que ele é necessário e inclua recursos do processador no servidor para gerenciar o aumento no tráfego de rede. Você também pode tentar outras opções. Por exemplo, alguns dispositivos de rede, como roteadores e comutadores, fornecem a função TLS ou SSL.

É possível usar TLS e SSL para proteger alguns ou todos os diferentes caminhos de comunicação possíveis, por exemplo:

- Operations Center: navegador para hub; hub para spoke
- Cliente para servidor
- Servidor para servidor: replicação de nó

Tarefas relacionadas

Configurando comunicações seguras com a Segurança da Camada de Transporte
Para criptografar os dados e as comunicações seguras em seu ambiente, o Secure Sockets Layer (SSL) ou a Segurança da Camada de Transporte (TLS) é ativada no servidor IBM Spectrum Protect e no cliente de backup-archive. Um certificado SSL é usado para verificar solicitações de comunicação entre o servidor e o cliente.

Planejando o armazenamento de dados criptografados

Determine se sua empresa requer que os dados armazenados sejam criptografados e escolha o método que melhor se adequa às suas necessidades.

Tabela 9. Selecionando um método de criptografia de dados

Necessidade de negócios	Método de Criptografia	Informações adicionais
Proteja dados no nível do cliente.	Criptografia do Cliente IBM Spectrum Protect	É possível criptografar dados no nível do arquivo usando uma lista de inclusões/exclusões. Dessa forma, é possível manter um alto grau de controle sobre quais dados são criptografados. São necessários recursos de cálculo extras no cliente que podem afetar o desempenho de processos de backup e restauração. Para obter mais informações sobre esse método, consulte IBM Spectrum Protect criptografia do cliente.

Tabela 9. Selecionando um método de criptografia de dados (continuação)		
Necessidade de negócios	**Método de Criptografia**	**Informações adicionais**
Proteja dados em volumes do conjunto de armazenamentos em uma unidade de fita.	Método da aplicação	Ao usar o método de Aplicativo, o IBM Spectrum Protect gerencia as chaves de criptografia para proteger dados em volumes do conjunto de armazenamentos. Você deve ter cuidado extra para proteger backups de banco de dados, porque as chaves de criptografia são armazenadas no banco de dados do servidor. Sem acessar backups de banco de dados e chaves de criptografia correspondentes, você não pode restaurara seus dados. Não é possível usar este método para criptografar backups de banco de dados, dados exportados ou conjuntos de backup. Para obter informações adicionais sobre o método de Aplicativo, consulte "Métodos de criptografia de fita" na página 118.
Proteja dados em uma unidade de fita.	Método da biblioteca	Ao usar o método de Biblioteca, a biblioteca gerencia chaves de criptografia. É possível criptografar dados em conjuntos de armazenamentos e outros dados em uma unidade de fita. É possível controlar quais volumes são criptografados usando os números de série do código de barras. Para obter informações adicionais sobre o método de Biblioteca, consulte "Métodos de criptografia de fita" na página 118.
Proteja dados em uma unidade de fita.	Método do sistema	Ao usar o método de Sistema, um driver de dispositivo ou o sistema operacional AIX gerencia a criptografia. Esse método de criptografia está disponível somente no sistema operacional AIX. É possível criptografar dados em conjuntos de armazenamentos e outros dados em uma unidade de fita. Para obter informações adicionais sobre o método de Sistema, consulte "Métodos de criptografia de fita" na página 118.

Planejando acesso ao firewall

Determine os firewalls que estão configurados e as portas que devem ser abertas para o funcionamento da solução do IBM Spectrum Protect.

Tabela 10 na página 27 descreve as portas que são usadas pelo servidor, cliente e Operations Center.

Tabela 10. Portas que são usadas pelo servidor, pelo cliente e o Operations Center			
Item	**Padrão**	**Direção**	**descrição**
Porta base (**TCPPORT**)	1500	Saída/entrada	Cada instância do servidor requer uma porta exclusiva. É possível especificar um número de porta alternativo. A opção **TCPPORT** atende a sessões ativadas para TCP/IP e SSL do cliente. É possível usar a opção **TCPADMINPORT** e a opção **ADMINONCLIENTPORT** para configurar valores de porta para tráfego do cliente administrador.
Porta somente SSL (**SSLTCPPORT**)	Sem padrão	Saída/entrada	Essa porta será usada se você desejar restringir a comunicação na porta somente a sessões ativadas para SSL. Um servidor pode suportar comunicação SSL e não SSL usando as opções **TCPPORT** ou **TCPADMINPORT**.

Tabela 10. Portas que são usadas pelo servidor, pelo cliente e o Operations Center (continuação)			
Item	**Padrão**	**Direção**	**descrição**
SMB	45	Entrada/saída	Essa porta é usada por assistentes de configuração que se comunicam usando protocolos nativos com vários hosts.
SSH	22	Entrada/saída	Essa porta é usada por assistentes de configuração que se comunicam usando protocolos nativos com vários hosts.
SMTP	25	Saída	Esta porta é usada para enviar alertas de e-mail do servidor.
Replicação	Sem padrão	Saída/entrada	A porta e protocolo para a porta de saída para replicação são configurados pelo comando **DEFINE SERVER** que é usado para configurar a replicação. As portas de entrada para replicação são as portas TCP e as portas SSL são especificadas para o servidor de origem no comando **DEFINE SERVER**.
Porta de planejamento de cliente	Porta do cliente: 1501	Saída	O cliente atende na porta nomeada e comunica o número da porta ao servidor. O servidor entra em contato com o cliente se o planejamento solicitado pelo servidor for usado. É possível especificar um número de porta alternativo no arquivo de opções do cliente.
Sessões de longa execução	Configuração de **KEEPALIVE**: YES	Saída	Quando a opção **KEEPALIVE** é ativada, os pacotes keep-alive são enviados durante as sessões do cliente/servidor para evitar que o software de firewall encerre conexões inativas de longa execução.
Operations Center	HTTPS: 11090	Entrada	Essas portas são usadas para o navegador da web do Operations Center. É possível especificar um número de porta alternativo.
Porta de serviço de gerenciamento de cliente	Porta do cliente: 9028	Entrada	Se você planeja usar o IBM Spectrum Protect, a porta de serviço de gerenciamento de cliente deve ser acessível a partir do Operations Center. Assegure-se de que os firewalls não possam impedir conexões. O serviço de gerenciamento de cliente usa a porta TCP do servidor para o nó cliente para autenticação usando uma sessão administrativa.

Informações relacionadas

Coletando informações de diagnóstico com os serviços de gerenciamento do cliente do IBM Spectrum Protect

Opção do servidor ADMINONCLIENTPORT

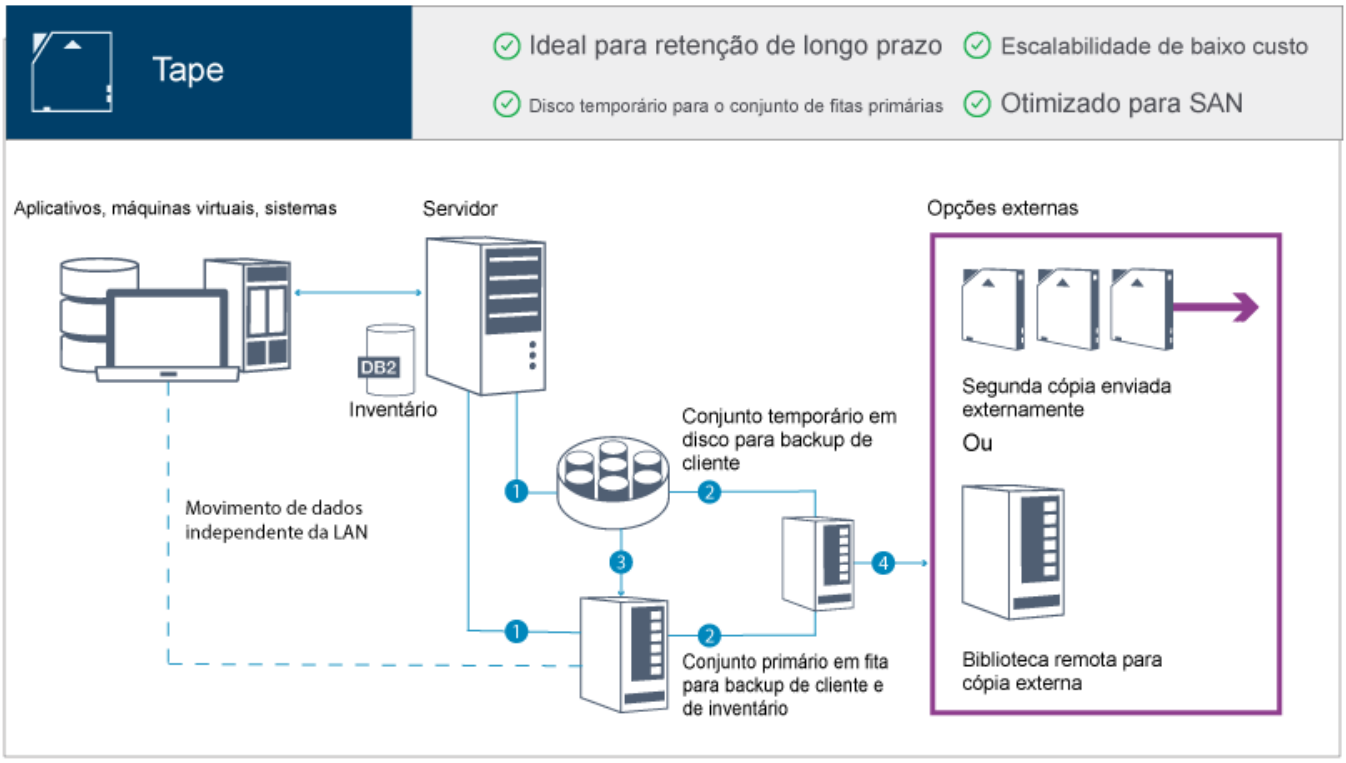
DEFINE SERVER (Definir um Servidor para Comunicações Servidor-para-Servidor)

opção do servidor TCPADMINPORT

Opção do servidor TCPPORT

Parte 2. Implementação de uma solução de proteção de dados baseada em fita

Implemente a solução baseada em fita, que usa o backup de disco para disco para fita e a preparação de disco para otimizar o armazenamento. Ao implementar a solução de fita, é possível ativar a retenção de dados de longo prazo e alcançar escalabilidade com baixo custo.



Dicas:

- Na solução descrita, os dados são *migrados* de conjuntos de armazenamento em disco para conjuntos de armazenamentos de fita. No entanto, em vez de migrar os dados, é possível usar o recurso de definição de camada para a fita que foi introduzido no IBM Spectrum Protect Versão 8.1.8. Com esse recurso, é possível classificar automaticamente os dados de camadas dos conjuntos de armazenamento em contêiner de diretório no disco para o armazenamento em fita. É possível especificar que todos os dados sejam em camadas com base em um limite de idade especificado ou que apenas os dados inativos sejam em camadas com base em um limite de idade. Para obter mais informações sobre a definição de camada de dados para armazenamento em fita, consulte Dados de definição de camada para armazenamento em nuvem ou em fita.
- A solução descrita não inclui replicação de nó. Se você deseja usar a replicação do nó para fazer backup de um conjunto de armazenamentos de disco em disco, verifique se a operação de replicação foi concluída antes que os dados sejam migrados do disco para a fita. Também é possível usar a replicação de nó para fazer backup de um conjunto de armazenamentos em um dispositivo de fita local para um conjunto de armazenamento de cópia em um dispositivo de fita local.

Roteiro de implementação

As etapas a seguir são necessárias para configurar uma solução baseada em fita.

1. Configure o sistema.
2. Instale o servidor e o Operations Center.
3. Configure o servidor e o Operations Center.

4. Conectar dispositivos de fita para o servidor.
5. Configurar bibliotecas de fitas para uso pelo servidor.
6. Configurar uma hierarquia do conjunto de armazenamentos.
7. Instalar e configurar clientes.
8. Configure movimentação de dados sem a LAN.
9. Selecionar um método de criptografia e configurar a criptografia.
10. Configure operações de armazenamento em fita.
11. Conclua a implementação.

Configurando o sistema

Para configurar o sistema, primeiro é necessário configurar o hardware de armazenamento em disco e o sistema do servidor para o IBM Spectrum Protect.

Sobre Esta Tarefa

Dica: São descritos procedimentos para configurar o servidor e o sistema de armazenamento em disco. Para iniciar com a configuração de dispositivos de fita, consulte "Conectando dispositivos de fita para o servidor" na página 72.

Configurando o hardware de armazenamento

Para otimizar o armazenamento em disco, revise as diretrizes para configurar armazenamento em disco com o IBM Spectrum Protect. Em seguida, forneça uma conexão entre o servidor e os dispositivos de armazenamento em disco e conclua outras tarefas de configuração.

Antes de Iniciar

Para diretrizes sobre a configuração do armazenamento em disco, consulte Lista de verificação para conjuntos de armazenamento em DISK ou FILE

Procedimento

1. Forneça uma conexão entre o servidor e os dispositivos de armazenamento seguindo estas diretrizes:
   - Use um comutador ou conexão direta para conexões Fibre Channel.
   - Considere o número de portas conectadas e considere a quantia de largura da banda que é necessária.
   - Considere o número de portas no servidor e o número de portas do host no sistema de disco que estão conectadas.
2. Verifique se os drivers de dispositivo e o firmware para o sistema do servidor, adaptadores e o sistema operacional são atuais e nos níveis recomendados.
3. Configure as matrizes de armazenamento. Assegure-se de ter planejado adequadamente para garantir o desempenho ideal.

   Para obter informações adicionais, consulte "Planejando para armazenamento em disco" na página 13.
4. Assegure-se de que o sistema do servidor tenha acesso a volumes de disco criados. Execute as etapas a seguir:
   a) Se o sistema estiver conectado a um comutador Fibre Channel, particione o servidor para ver os discos.
   b) Mapeie todos os volumes para informar o sistema de disco de que esse servidor específico tem permissão de ver cada disco.

5. Certifique-se de que os dispositivos de fita e de disco usem portas do Adaptador de Barramento de Host (HBA) diferentes. Controle a E/S de fita e disco usando a SAN. Use portas Fibre Channel separadas para E/S de fita e de disco.

Tarefas relacionadas

Configurando a E/S de caminhos múltiplos
É possível ativar e configurar caminhos múltiplos para armazenamento em disco. Use a documentação que é fornecida com seu hardware para obter instruções detalhadas.

Instalando o sistema operacional do servidor

Instale o sistema operacional no sistema do servidor e certifique-se de que os requisitos do servidor do IBM Spectrum Protect sejam atendidos. Ajuste as configurações do sistema operacional, conforme instruções.

Instalando em sistemas AIX

Conclua as etapas a seguir para instalar o AIX no sistema do servidor.

Procedimento

1. Instale o AIX Versão 7.1, TL4, SP6 ou mais recente, de acordo com as instruções do fabricante.
2. Defina as configurações do TCP/IP de acordo com as instruções de instalação do sistema operacional.
3. Abra o arquivo `/etc/hosts` e conclua as seguintes ações:
   - Atualize o arquivo para incluir o endereço IP e o nome do host para o servidor. Por exemplo:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Verifique se o arquivo contém uma entrada para localhost com um endereço de 127.0.0.1. Por exemplo:

     ```
     127.0.0.1  localhost
     ```

4. Ative as portas de conclusão de E/S do AIX emitindo o seguinte comando:

   ```
   chdev -l iocp0 -P
   ```

   O desempenho do servidor pode ser afetado pela definição de fuso horário de Olson.
5. Para otimizar o desempenho, mude o formato de fuso horário do seu sistema de Olson para POSIX. Use o seguinte formato de comando para atualizar a configuração de fuso horário:

   ```
   chtz=local_timezone,date/time,date/time
   ```

   Por exemplo, se você morou em Tucson, Arizona, onde a Hora Padrão das Montanhas é usada, emita o seguinte comando para mudar para o formato POSIX:

   ```
   chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
   ```

6. No arquivo `.profile` do usuário da instância, verifique se a variável de ambiente a seguir está configurada:

   ```
   export MALLOCOPTIONS=multiheap:16
   ```

   Em versões posteriores do servidor IBM Spectrum Protect, este valor é configurado automaticamente quando o servidor é iniciado. Se o usuário da instância não estiver disponível, conclua esta etapa mais tarde, quando o usuário da instância se tornar disponível.
7. Configure o sistema para criar arquivos principais de aplicativo completos. Emita o seguinte comando:

   ```
   chdev -l sys0 -a fullcore=true -P
   ```

8. Para comunicações com o servidor e oOperations Center, certifique-se de que as portas a seguir estejam abertas em quaisquer firewalls existentes:
   - Para comunicações com o servidor, abra a porta 1500.
   - Para comunicações seguras com o Operations Center, abra a porta 11090 no servidor do hub.

   Se você não estiver usando os valores de porta padrão, certifique-se de que as portas que estiverem sendo usadas estejam abertas.
9. Ative aprimoramentos de alto desempenho TCP. Emita o seguinte comando:

```
no -p -o rfc1323=1
```

10. Para um rendimento e confiabilidade ideais, ligue duas portas Ethernet de 10 Gb para um sistema médio e quatro portas Ethernet de 10 Gb para um sistema grande. Use o System Management Interface Tool (SMIT) para ligar as portas usando Etherchannel.

    As configurações a seguir foram usadas durante o teste:

```
      mode            8023ad
      auto_recovery   yes             Ativar recuperação automática após failover
      backup_adapter  NONE            Adaptador utilizado quando o canal inteiro falha
      hash_mode       src_dst_port    Determina como o adaptador de saída é escolhido
      interval        long            Determina o valor do intervalo para IEEE
                                      modo 802.3ad
      mode            8023ad          Modo de operação EtherChannel
      netaddr         0               Endereço para executar ping
      noloss_failover yes             Ativar failover sem perdas após ping
                                      falha
      num_retries     3               Vezes para tentar executar ping novamente antes de
falhar
      retry_time      1               Tempo de espera (em segundos) entre pings
      use_alt_addr    no              Ativar Endereço de EtherChannel Alternativo
      use_jumbo_frame no              Ativar Quadros Gigantes de Gigabit Ethernet
```

11. Verifique se os limites de recurso do processo do usuário, também conhecidos como *ulimits*, estão configurados de acordo com as diretrizes em Tabela 11 na página 32. Se os valores de ulimit não estiverem configurados corretamente, pode haver instabilidade do servidor ou uma falha do servidor ao responder.

Tabela 11. Valores de limites do usuário (ulimit)

Tipo de limite do usuário	**Configuração**	**Valor**	**Comando para consultar valor**
Tamanho máximo dos arquivos principais criados	`core`	Sem limites	`ulimit -Hc`
Tamanho máximo de um segmento de dados para um processo	`dados`	Sem limites	`ulimit -Hd`
Tamanho máximo do arquivo	`fsize`	Sem limites	`ulimit -Hf`
Número máximo de arquivos abertos	`nofile`	65536	`ulimit -Hn`
Quantidade máxima de tempo do processador em segundos	`cpu`	Sem limites	`ulimit -Ht`
Número máximo de processos do usuário	`nproc`	16384	`ulimit -Hu`

Se precisar modificar quaisquer valores de limite do usuário, siga as instruções na documentação de seu sistema operacional.

Instalando em sistemas Linux

Conclua as etapas a seguir para instalar o Linux x86_64 no sistema do servidor.

Antes de Iniciar

O sistema operacional será instalado nos discos rígidos internos. Configure os discos rígidos internos usando uma matriz de hardware RAID 1. Por exemplo, se estiver configurando um sistema pequeno, os dois discos internos de 300 GB serão espelhados no RAID 1 para que um único disco de 300 GB apareça disponível para o instalador do sistema operacional.

Procedimento

1. Instale o Red Hat Enterprise Linux Versão 7.4 ou mais recente, de acordo com as instruções do fabricante.

   Obtenha um DVD inicializável que contenha o Red Hat Enterprise Linux Versão 7.4 ou mais recente e inicie o seu sistema por meio deste DVD. Consulte a seguinte orientação para obter opções de instalação. Se um item não for mencionado na lista a seguir, deixe a seleção padrão.

   a) Depois de iniciar o DVD, escolha **Instalar ou fazer upgrade de um sistema existente** no menu.

   b) Na tela Bem-vindo, selecione **Testar essa mídia e instalar o Red Hat Enterprise Linux 7.4**.

   c) Selecione seu idioma e preferências do teclado.

   d) Selecione a sua localização para configurar o fuso horário correto.

   e) Selecione **Seleção de software** e, em seguida, na próxima tela, selecione **Servidor com a GUI**.

   f) Na página de resumo de instalação, clique em **Destino de instalação** e verifique os itens a seguir:

   - O disco local de 300 GB está selecionado como o destino de instalação.
   - Em Outras opções de armazenamento, `Configurar particionamento automaticamente` está selecionado.

   Clique em **Pronto**.

   g) Clique em **Iniciar instalação**.

   Após o início da instalação, configure a senha root para a conta do usuário root.

   Após a instalação ser concluída, reinicie o sistema e efetue login como o usuário raiz. Emita o comando **df** para verificar seu particionamento básico.

   Por exemplo, em um sistema de teste, o particionamento inicial produziu o resultado a seguir:

```
[root@tvapp02]# df –h
Filesystem                      Size  Used  Avail  Use%  Mounted on
/dev/mapper/rhel-root   50G  3.0G   48G   6% /
devtmpfs                32G     0   32G   0% /dev
tmpfs                   32G   92K   32G   1% /dev/shm
tmpfs                   32G  8.8M   32G   1% /run
tmpfs                   32G     0   32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home  220G   37M  220G   1% /home
/dev/sda1              497M  124M  373M  25% /boot
```

2. Defina as configurações do TCP/IP de acordo com as instruções de instalação do sistema operacional.

   Para um rendimento e confiabilidade ideais, considere ligar várias portas de rede. Ligue duas portas para um sistema médio e quatro portas para um sistema grande. Isso pode ser feito criando uma conexão de rede Link Aggregation Control Protocol (LACP), que agrega várias portas subordinadas em uma única conexão lógica. O método preferencial é usar um modo de ligação de 802.3ad, uma configuração de **miimon** de 100 e uma configuração de **xmit_hash_policy** de layer3+4.

   Restrição: Para usar uma conexão de rede LACP, deve-se ter uma comutação de rede que suporte LACP.

Para obter instruções adicionais sobre configurar conexões de rede ligadas ao Red Hat Enterprise Linux Versão 7, consulte Criar uma interface de ligação de canal.

3. Abra o arquivo `/etc/hosts` e conclua as seguintes ações:
   - Atualize o arquivo para incluir o endereço IP e o nome do host para o servidor. Por exemplo:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Verifique se o arquivo contém uma entrada para localhost com um endereço de 127.0.0.1. Por exemplo:

     ```
     127.0.0.1  localhost
     ```

4. Instale os componentes que são necessários para a instalação do servidor. Conclua as etapas a seguir para criar um repositório Yellowdog Updater Modified (YUM) e instalar os pacotes obrigatórios.
   a) Monte o DVD de instalação do Red Hat Enterprise Linux em um diretório do sistema. Por exemplo, para montá-lo no diretório `/mnt`, emita o seguinte comando:

      ```
      mount -t iso9660 -o ro /dev/cdrom /mnt
      ```

   b) Verifique se o DVD foi montado emitindo o comando **mount**.
      Você deve ver uma saída semelhante ao seguinte exemplo:

      ```
      /dev/sr0 on /mnt type iso9660
      ```

   c) Altere para o diretório do repositório YUM emitindo o seguinte comando:

      ```
      cd /etc/yum/repos.d
      ```

      Se o diretório `repos.d` não existir, crie-o.
   d) Liste o conteúdo do diretório:

      ```
      ls rhel-source.repo
      ```

   e) Renomeie o arquivo repo original emitindo o comando **mv**.
      Por exemplo:

      ```
      mv rhel-source.repo rhel-source.repo.orig
      ```

   f) Crie um novo arquivo repo usando um editor de texto.
      Por exemplo, para usar o editor de vi, emita o seguinte comando:

      ```
      vi rhel74_dvd.repo
      ```

   g) Inclua as seguintes linhas no novo arquivo repo. O parâmetro **baseurl** especifica o ponto de montagem de seu diretório:

      ```
      [rhel74_dvd]
      name=DVD Redhat Enterprise Linux 7.4
      baseurl=file:///mnt
      enabled=1
      gpgcheck=0
      ```

   h) Instale o pacote obrigatório `ksh.x86_64`, emitindo o comando **yum**.
      Por exemplo:

      ```
      yum install ksh.x86_64
      ```

5. Quando a instalação de software estiver concluída, será possível restaurar os valores originais do repositório YUM concluindo as etapas a seguir:
   a) Desmonte o DVD de instalação do Red Hat Enterprise Linux emitindo o seguinte comando:

      ```
      unmount /mnt
      ```

b) Altere para o diretório do repositório YUM emitindo o seguinte comando:

```
cd /etc/yum/repos.d
```

c) Renomeie o arquivo repo criado:

```
mv rhel74_dvd.repo rhel74_dvd.repo.orig
```

d) Renomeie o arquivo original para o nome original:

```
mv rhel-source.repo.orig rhel-source.repo
```

6. Determine se as mudanças do parâmetro do kernel são necessárias. Execute as etapas a seguir:
   a) Use o comando **`sysctl -a`** para listar os valores de parâmetro.
   b) Analise os resultados usando as diretrizes em Tabela 12 na página 35 para determinar se quaisquer mudanças são necessárias.
   c) Se as mudanças forem necessárias, configure os parâmetros no arquivo `/etc/sysctl.conf`.
   As mudanças no arquivo são aplicadas quando o sistema é iniciado.

Dica: Ajustar automaticamente as configurações de parâmetro do kernel e eliminar a necessidade de atualizações manuais para essas configurações. No Linux, o Db2 software de banco de dados ajusta automaticamente os valores de parâmetro do kernel de comunicação interprocessual (IPC) para as configurações preferenciais. Para obter informações adicionais sobre configurações de parâmetro do kernel, procure parâmetros do kernel Linux no Documentação do produto IBM Db2 Versão 11.5.

Tabela 12. Configurações ideais de parâmetro do kernel do Linux

Parâmetro	**descrição**
`kernel.shmmni`	O número máximo de segmentos.
`kernel.shmmax`	O tamanho máximo de um segmento de memória compartilhada (bytes). Este parâmetro deve ser configurado antes do início automático do servidor do IBM Spectrum Protect na inicialização do sistema.
`kernel.shmall`	A alocação máxima das páginas de memória compartilhada (páginas).
`kernel.sem` Há quatro valores para o parâmetro **`kernel.sem`**.	(SEMMSL) O máximo de semáforos por matriz.
	(SEMMNS) O máximo de semáforos por sistema.
	(SEMOPM) O máximo de operações por chamada de semáforo.
	(SEMMNI) O número máximo de matrizes.
`kernel.msgmni`	O número máximo de filas de mensagens de todo o sistema.
`kernel.msgmax`	O tamanho máximo de mensagens (bytes).
`kernel.msgmnb`	O tamanho máximo padrão da fila (bytes).

Tabela 12. Configurações ideais de parâmetro do kernel do Linux (continuação)	
Parâmetro	**descrição**
kernel.randomize_va_space	O parâmetro **kernel.randomize_va_space** configura o uso da memória ASLR para o kernel. Ative o ASLR para a V7.1 e para servidores posteriores. Para saber mais detalhes sobre o Linux ASLR e o Db2, consulte a nota técnica 1365583.
vm.swappiness	O parâmetro **vm.swappiness** define se o kernel pode descarregar a memória do aplicativo na memória de acesso aleatório (RAM) física. Para obter informações adicionais sobre os parâmetros do kernel, consulte o Informações do produto Db2.
vm.overcommit_memory	O parâmetro **vm.overcommit_memory** influencia quanta memória virtual o kernel permite alocar. Para obter informações adicionais sobre os parâmetros do kernel, consulte o Informações do produto Db2.

7. Abra as portas de firewall para se comunicar com o servidor. Execute as etapas a seguir:
   a) Determine a zona usada pela interface de rede. Por padrão, a zona é pública.

      Emita o seguinte comando:

      ```
      #  firewall-cmd --get-active-zones
      public
        interfaces: ens4f0
      ```

   b) Para usar o endereço de porta padrão para comunicações com o servidor, abra a porta TCP/IP 1500 no firewall Linux.

      Emita o seguinte comando:

      ```
      firewall-cmd --zone=public --add-port=1500/tcp --permanent
      ```

      Se desejar usar um valor diferente do padrão, é possível especificar um número no intervalo de 1024 a 32767. Se você abrir uma porta diferente do padrão, será necessário especificar essa porta quando executar o script de configuração.

   c) Se você planeja usar esse sistema como um hub, abra a porta 11090, que é a porta padrão para comunicações seguras (https).

      Emita o seguinte comando:

      ```
      firewall-cmd --zone=public --add-port=11090/tcp --permanent
      ```

   d) Recarregue as definições de firewall para que as mudanças entrem em vigor.

      Emita o seguinte comando:

      ```
      firewall-cmd --reload
      ```

8. Verifique se os limites de recurso do processo do usuário, também conhecidos como *ulimits*, estão configurados de acordo com as diretrizes em Tabela 13 na página 37. Se os valores de ulimit não estiverem configurados corretamente, pode haver instabilidade do servidor ou uma falha do servidor ao responder.

Tabela 13. Valores de limites do usuário (ulimit)			
Tipo de limite do usuário	**Configuração**	**Valor**	**Comando para consultar valor**
Tamanho máximo dos arquivos principais criados	`core`	Sem limites	`ulimit -Hc`
Tamanho máximo de um segmento de dados para um processo	`dados`	Sem limites	`ulimit -Hd`
Tamanho máximo do arquivo	`fsize`	Sem limites	`ulimit -Hf`
Número máximo de arquivos abertos	`nofile`	65536	`ulimit -Hn`
Quantidade máxima de tempo do processador em segundos	`cpu`	Sem limites	`ulimit -Ht`
Número máximo de processos do usuário	`nproc`	16384	`ulimit -Hu`

Se precisar modificar quaisquer valores de limite do usuário, siga as instruções na documentação de seu sistema operacional.

Instalando em sistemas Windows

Instale o Microsoft Windows Server 2012 Standard Edition no sistema do servidor e prepare o sistema para instalação e configuração do servidor do IBM Spectrum Protect.

Procedimento

1. Instale o Windows Server 2016 Standard Edition de acordo com as instruções do fabricante.
2. Altere as políticas de controle de conta do Windows concluindo as etapas a seguir.
   a) Abra o editor Política de segurança local executando `secpol.msc`.
   b) Clique em **Políticas locais** > **Opções de segurança** e assegure-se de que as políticas de Controle de conta do usuário a seguir estejam desativadas:
      - Modo de aprovação de administrador para a conta do Administrador integrado
      - Execute todos os administradores no Modo de aprovação de administrador
3. Defina as configurações de TCP/IP de acordo com as instruções de instalação para o sistema operacional.
4. Aplique atualizações do Windows e ative recursos opcionais concluindo as etapas a seguir:
   a) Aplique as atualizações mais recentes do Windows Server 2016.
   b) Instale e ative o recurso Microsoft .NET Framework 3.5 do Windows 2012 R2 a partir do Windows Server Manager.
   c) Se necessário, atualize os drivers de dispositivo HBA FC e Ethernet para níveis mais recentes.
   d) Instale o driver de E/S de caminhos múltiplos que seja apropriado para o sistema de disco que está sendo usado.
5. Abra a porta TCP/IP padrão, 1500, para comunicações com o servidor do IBM Spectrum Protect. Por exemplo, emita o seguinte comando:

```
netsh advfirewall firewall add rule name="Backup server port 1500"
dir=in action=allow protocol=TCP localport=1500
```

6. No servidor do hub do Operations Center, abra a porta padrão para comunicações seguras (https) com o Operations Center.

   O número da porta é 11090.

   Por exemplo, emita o seguinte comando:

   ```
   netsh advfirewall firewall add rule name="Operations Center port 11090"
   dir=in action=allow protocol=TCP localport=11090
   ```

Configurando a E/S de caminhos múltiplos

É possível ativar e configurar caminhos múltiplos para armazenamento em disco. Use a documentação que é fornecida com seu hardware para obter instruções detalhadas.

Sistemas AIX

Conclua as etapas a seguir para ativar e configurar caminhos múltiplos para armazenamento em disco.

Procedimento

1. Determine o endereço de porta Fibre Channel que deve ser usado para a definição de host no subsistema de disco. Emita o comando **lscfg** para cada porta.
   - Em sistemas pequenos e médios, emita os seguintes comandos:

     ```
     lscfg -vps -l fcs0 | grep "Network Address"
     lscfg -vps -l fcs1 | grep "Network Address"
     ```

   - Em sistemas grandes, emita os seguintes comandos:

     ```
     lscfg -vps -l fcs0 | grep "Network Address"
     lscfg -vps -l fcs1 | grep "Network Address"
     lscfg -vps -l fcs2 | grep "Network Address"
     lscfg -vps -l fcs3 | grep "Network Address"
     ```

2. Certifique-se de que os seguintes conjuntos de arquivos do AIX estejam instalados:
   - devices.common.IBM.mpio.rte
   - devices.fcp.disk.rte
3. Emita o comando **cfgmgr** para que o AIX varra novamente o hardware e descubra os discos disponíveis. Por exemplo:

   ```
   cfgmgr
   ```

4. Para listar os discos disponíveis, emita o seguinte comando:

   ```
   lsdev -Ccdisk
   ```

   A saída é semelhante ao seguinte exemplo:

   ```
   hdisk0  Available 00-00-00 SAS Disk Drive
   hdisk1  Available 00-00-00 SAS Disk Drive
   hdisk2  Available 01-00-00 SAS Disk Drive
   hdisk3  Available 01-00-00 SAS Disk Drive
   hdisk4  Available 06-01-02 MPIO IBM 2076 FC Disk
   hdisk5  Available 07-01-02 MPIO IBM 2076 FC Disk
   ...
   ```

5. Use a saída do comando **lsdev** para identificar e listar IDs de dispositivos para cada dispositivo de disco.

   Por exemplo, um ID do dispositivo pode ser `hdisk4`. Salve a lista de IDs de dispositivos a ser usada ao criar sistemas de arquivos para o servidor do IBM Spectrum Protect.
6. Correlacione os IDs de dispositivos SCSI com LUNs de disco específicos do sistema de disco, listando informações detalhadas sobre todos os volumes físicos no sistema. Emita o seguinte comando:

```
lspv -u
```

Em um sistema IBM Storwize, as informações a seguir são um exemplo do que é mostrado para cada dispositivo:

```
hdisk4  00f8cf083fd97327  None  active
 3321360050763008101057800000000000030042145O3IBMfcp
```

No exemplo, *600507630081010578000000000000030* é o UID do volume, conforme relatado pela interface de gerenciamento do Storwize.

Para verificar o tamanho do disco em megabytes e comparar o valor com o que estiver listado para o sistema, emita o comando a seguir:

```
bootinfo -s hdisk4
```

Sistemas Linux

Conclua as etapas a seguir para ativar e configurar caminhos múltiplos para armazenamento em disco.

Procedimento

1. Edite o arquivo `/etc/multipath.conf` para ativar caminhos múltiplos para hosts do Linux.

   Se o arquivo `multipath.conf` não existir, é possível criá-lo emitindo o seguinte comando:

   ```
   mpathconf --enable
   ```

   Os parâmetros a seguir foram configurados em `multipath.conf` para teste em um sistema de armazenamento IBM FlashSystem:

   ```
   defaults {
            user_friendly_names no
   }

   devices {
            device {
                     vendor "IBM "
                     product "2145"
                     path_grouping_policy group_by_prio
                     user_friendly_names no
                     path_selector "round-robin 0"
                     Prioridade "alua"
                     path_checker "tur"
                     retorno "imediato"
                     no_path_retry 5
                     rr_weight uniform
                     rr_min_io_rq "1"
                     dev_loss_tmo 120
           }
   }
   ```

2. Configure a opção de caminhos múltiplos para iniciar quando o sistema for iniciado.

   Emita os seguintes comandos:

   ```
   systemctl enable multipathd.service
   systemctl start multipathd.service
   ```

3. Para verificar se os discos estão visíveis para o sistema operacional e são gerenciados por caminhos múltiplos, emita o seguinte comando:

   ```
   multipath -l
   ```

4. Certifique-se de que cada dispositivo esteja listado e que tenha a quantidade de caminhos esperada. É possível usar informações de tamanho e de ID do dispositivo para identificar quais discos estão listados.

   Por exemplo, a seguinte saída mostra que um disco de 2 TB possui dois grupos de caminhos e quatro caminhos ativos. O tamanho de 2 TB confirma que o disco corresponde a sistema de arquivos do

conjunto. Use parte do número do ID do dispositivo longo (12, nesse exemplo) para procurar o volume na interface de gerenciamento de sistemas de disco.

```
[root@tapsrv01 code]# multipath -l
36005076802810c509800000000000012 dm-43 IBM,2145
 size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='round-robin 0' prio=0 status=active
| |- 2:0:1:18 sdcw 70:64   active undef running
| `- 4:0:0:18 sdgb 131:112 active undef running
`-+- policy='round-robin 0' prio=0 status=enabled
  |- 1:0:1:18 sdat 66:208  active undef running
  `- 3:0:0:18 sddy 128:0   active undef running
```

a) Se necessário, corrija as designações de host do LUN de disco e force uma nova varredura de barramento.
Por exemplo:

```
echo "- - -" > /sys/class/scsi_host/host0/scan
echo "- - -" > /sys/class/scsi_host/host1/scan
echo "- - -" > /sys/class/scsi_host/host2/scan
```

Também é possível reiniciar o sistema para varrer novamente as designações de host do LUN de disco.

b) Confirme se os discos agora estão disponíveis para E/S de caminhos múltiplos emitindo novamente o comando **multipath -l**.

5. Use a saída de caminhos múltiplos para identificar e listar IDs de dispositivos para cada dispositivo de disco.

   Por exemplo, o ID do dispositivo para seu disco de 2 TB é 36005076802810c509800000000000012.

   Salve a lista de IDs de dispositivos para usar na próxima etapa.

Sistemas Windows

Conclua as etapas a seguir para ativar e configurar caminhos múltiplos para armazenamento em disco.

Procedimento

1. Certifique-se de que o recurso E/S de Caminhos Múltiplos esteja instalado. Se necessário, instale drivers de caminhos múltiplos adicionais específicos do fornecedor.
2. Para verificar se os discos estão visíveis para o sistema operacional e são gerenciados por E/S de caminhos múltiplos, emita o seguinte comando:

```
c:\program files\IBM\SDDDSM\datapath.exe query device
```

3. Revise a saída de caminhos múltiplos e certifique-se de que cada dispositivo esteja listado e tenha a quantidade de caminhos esperada. É possível usar informações de tamanho e de série do dispositivo para identificar quais discos estão listados.

   Por exemplo, usando parte do número de série longo do dispositivo (34, nesse exemplo), é possível procurar o volume na interface de gerenciamento de sistemas de disco. O tamanho de 2 TB confirma que o disco corresponde a um sistema de arquivos do conjunto de armazenamentos.

```
DEV#:   4  DEVICE NAME: Disk5 Part0   TYPE: 2145    POLICY: OPTIMIZED
SERIAL: 600507630081010578000000000000034          LUN SIZE: 2.0TB
============================================================================
Path#          Adapter/Hard Disk       State   Mode    Select  Errors
    0   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
    1   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL   27176       0
    2   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL   28494       0
    3   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
```

4. Crie uma lista de IDs de dispositivo de disco usando os números de série que são retornados da saída de caminhos múltiplos na etapa anterior.

   Por exemplo, o ID do dispositivo para seu disco de 2 TB é 600507630081010578000000000000034

Salve a lista de IDs de dispositivos para usar na próxima etapa.

5. Para colocar novos discos on-line e limpar o atributo de leitura, execute `diskpart.exe` com os seguintes comandos. Repita para cada um dos discos:

```
diskpart
   select Disk 1
   online disk
   attribute disk clear readonly
   select Disk 2
   online disk
   attribute disk clear readonly
   < ... >
   select Disk 49
   online disk
   attribute disk clear readonly
   exit
```

Criando o ID do usuário para o servidor

Crie o ID do usuário que possui a instância do servidor IBM Spectrum Protect. Você especifica esse ID do usuário ao criar a instância do servidor durante a configuração inicial do servidor.

Sobre Esta Tarefa

É possível especificar apenas letras minúsculas (a-z), numerais (0-9) e o caractere de sublinhado (_) para o ID do usuário. 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.

Procedimento

1. Use comandos do sistema operacional para criar um ID do usuário.
   - Linux AIX Crie um grupo e um ID do usuário no diretório inicial do usuário que possui a instância do servidor.

     Por exemplo, para criar o ID do usuário `tsminst1` no grupo `tsmsrvrs` com uma senha de `tsminst1`, emita os seguintes comandos a partir de um ID do usuário administrativo:

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

     Linux
     ```
     groupadd
     tsmsrvrs
     useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
     passwd tsminst1
     ```

     Efetue logoff e, em seguida, efetue login em seu sistema. Mude para a conta do usuário que você criou. Use um programa de login interativo, como telnet, para que você solicite a senha e possa alterá-la se necessário.
   - Windows Crie um ID do usuário e, em seguida, inclua o novo ID no grupo de Administradores. Por exemplo, para criar o ID do usuário `tsminst1`, emita o seguinte comando:

     ```
     net user tsminst1 * /add
     ```

     Após criar e verificar uma senha para o novo usuário, inclua o ID do usuário no grupo de Administradores emitindo os seguintes comandos:

```
net localgroup Administrators tsminst1 /add
net localgroup DB2ADMNS tsminst1 /add
```

2. Efetue logoff no novo ID do usuário.

Preparando sistemas de arquivos para o servidor

Deve-se concluir a configuração do sistema de arquivos para o armazenamento em disco a ser usado pelo servidor.

Sistemas AIX

Deve-se criar grupos lógicos, volumes lógicos e sistemas de arquivos para o servidor usando o Gerenciador de Volume Lógico AIX.

Procedimento

1. Aumente a profundidade da fila e o tamanho máximo de transferência para todos os discos *hdiskX* disponíveis. Emita os seguintes comandos para cada disco:

```
chdev -l hdisk4 -a max_transfer=0x100000
chdev -l hdisk4 -a queue_depth=32
chdev -l hdisk4 -a reserve_policy=no_reserve
chdev -l hdisk4 -a algorithm=round_robin
```

   Não execute esses comandos para discos internos do sistema operacional, por exemplo, *hdisk0*.

2. Crie grupos de volumes para o banco de dados, log ativo, log de archive, backup de banco de dados e conjunto de armazenamentos do IBM Spectrum Protect. Emita o comando **mkvg**, especificando os IDs do dispositivo para discos correspondentes que foram identificados anteriormente.

   Por exemplo, se os nomes de dispositivos *hdisk4, hdisk5* e *hdisk6* corresponderem a discos do banco de dados, inclua-os no grupo de volumes do banco de dados e assim por diante.

   Tamanho do sistema: Os seguintes comandos são baseados na configuração do sistema médio. Para sistemas pequenos e grandes, deve-se ajustar a sintaxe conforme necessário.

```
mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
mkvg -S -y tsmactlog hdisk5
mkvg -S -y tsmarchlog hdisk6
mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
```

3. Determine os nomes de volumes físicos e o número de partições físicas livres a serem usadas ao criar volumes lógicos. Emita **lsvg** para cada grupo de volumes criado na etapa anterior.

   Por exemplo:

```
lsvg -p tsmdb
```

   A saída é semelhante à seguinte. A coluna *FREE PPs* representa as três partições físicas livres:

```
tsmdb:
PV_NAME  PV STATE   TOTAL PPs  FREE PPs  FREE DISTRIBUTION
hdisk4   active     1631       1631      327..326..326..326..326
hdisk5   active     1631       1631      327..326..326..326..326
hdisk6   active     1631       1631      327..326..326..326..326
```

4. Crie volumes lógicos em cada grupo de volumes usando o comando **mklv**. O tamanho do volume, o grupo de volumes e os nomes dos dispositivos variam, dependendo do tamanho do seu sistema e de variações na configuração do disco.

Por exemplo, para criar os volumes para o banco de dados do IBM Spectrum Protect em um sistema médio, emita os seguintes comandos:

```
mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
```

5. Formate sistemas de arquivos em cada volume lógico usando o comando **crfs**.

   Por exemplo, para formatar sistemas de arquivos para o banco de dados em um sistema médio, emita os seguintes comandos:

```
crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
 -a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
 -a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
 -a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
```

6. Monte todos os sistemas de arquivos recém-criados emitindo o seguinte comando:

```
mount -a
```

7. Liste todos os sistemas de arquivos emitindo o comando **df**.

   Verifique se os sistemas de arquivos estão montados no LUN correto e no ponto de montagem correto. Verifique também o espaço disponível.

   O exemplo de saída de comando a seguir mostra que a quantia de espaço usado geralmente é 1%:

```
tapsrv07> df -g /tsminst1/*
Filesystem      GB blocks  Free     %Used   Iused   %Iused   Mounted on
/dev/tsmact00   195.12     194.59   1%      4       1%       /tsminst1/TSMalog
```

8. Verifique se o ID do usuário que você criou em “Criando o ID do usuário para o servidor” na página 41 tem acesso de leitura e gravação aos diretórios do servidor.

Sistemas Linux

Deve-se formatar sistemas de arquivos `ext4` ou `xfs` em cada um dos LUNs de disco a ser usado pelo servidor do IBM Spectrum Protect.

Procedimento

1. Usando a lista de IDs de dispositivos que você gerou anteriormente, emita o comando **mkfs** para criar e formatar um sistema de arquivos para cada dispositivo LUN de armazenamento. Especifique o ID do dispositivo no comando. Consulte os exemplos a seguir.
   Para o banco de dados, formate os sistemas de arquivos `ext4`:

```
mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c509800000000000012
```

   Para LUNs do conjunto de armazenamentos, formate os sistemas de arquivos `xfs`:

```
mkfs -t xfs /dev/mapper/360050763008101057800000000002c3
```

   É possível emitir o comando **mkfs** até 50 vezes, dependendo de quantos dispositivos diferentes você possui.

2. Crie diretórios de ponto de montagem para sistemas de arquivos.

   Emita o comando **mkdir** para cada diretório que você deve criar. Use os valores de diretório registrados nas planilhas de planejamento.

   Por exemplo, para criar o diretório de instância do servidor usando o valor padrão, emita o seguinte comando:

```
mkdir /tsminst1
```

Repita o comando **mkdir** para cada sistema de arquivos.

3. Inclua uma entrada no arquivo `/etc/fstab` para cada sistema de arquivos para que os sistemas de arquivos sejam montados automaticamente quando o servidor for iniciado.

   Por exemplo:

   ```
   /dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4
   defaults 0 0
   ```

4. Monte os sistemas de arquivos que foram incluídos no arquivo `/etc/fstab` emitindo o comando **mount -a**.
5. Liste todos os sistemas de arquivos emitindo o comando **df**.

   Verifique se os sistemas de arquivos estão montados no LUN correto e no ponto de montagem correto. Verifique também o espaço disponível.

   O exemplo a seguir em um sistema IBM Storwize mostra que a quantia de espaço usado geralmente é 1%:

   ```
   [root@tapsrv04 ~]# df -h /tsminst1/*
   Filesystem                                      Size  Used Avail Use% Mounted on
   /dev/mapper/360050763008101057800000000000003 134G  188M 132G  1%   /tsminst1/
   TSMalog
   ```

6. Verifique se o ID do usuário que você criou em "Criando o ID do usuário para o servidor" na página 41 tem acesso de leitura e gravação aos diretórios para o servidor do IBM Spectrum Protect.

Sistemas Windows

Deve-se formatar sistemas de arquivos NTFS em cada um dos LUNs de disco a serem usados pelo servidor do IBM Spectrum Protect.

Procedimento

1. Crie diretórios de ponto de montagem para sistemas de arquivos.

   Emita o comando **md** para cada diretório que você deve criar. Use os valores de diretório registrados nas planilhas de planejamento. Por exemplo, para criar o diretório de instância do servidor usando o valor padrão, emita o seguinte comando:

   ```
   md c:\tsminst1
   ```

   Repita o comando **md** para cada sistema de arquivos.

2. Crie um volume para cada LUN de disco que é mapeado para um diretório no diretório de instância do servidor usando o gerenciador de volume do Windows.

   Acesse **Gerenciador do servidor** > **Serviços de arquivo e armazenamento** e conclua as etapas a seguir para cada disco que corresponda ao mapeamento de LUN que foi criado na etapa anterior:

   a) Torne o disco online.

   b) Inicialize o disco para o tipo básico de GPT, que é o padrão.

   c) Crie um volume simples que ocupe todo o espaço no disco. Formate o sistema de arquivos usando NTFS e designe um rótulo que corresponda ao propósito do volume, como `TSMfile00`. Não designe o novo volume a uma letra da unidade. Em vez disso, mapeie o volume para um diretório no diretório de instâncias, como `C:\tsminst1\TSMfile00`.

      Dica: Determine o rótulo de volume e os rótulos de mapeamento de volume com base no tamanho do disco relatado.

3. Verifique se os sistemas de arquivos estão montados no LUN correto e no ponto de montagem correto. Liste todos os sistemas de arquivos emitindo o comando **mountvol** e, em seguida, revise a saída. Por exemplo:

```
\\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
  C:\tsminst1\TSMdbspace00\
```

4. Após a conclusão da configuração do disco, reinicie o sistema.

O que Fazer Depois

É possível confirmar a quantidade de espaço livre para cada volume usando o Windows Explorer.

Instalando o servidor e o Operations Center

Use o assistente gráfico do IBM Installation Manager para instalar os componentes.

Instalando em sistemas AIX e Linux

Instale o servidor do IBM Spectrum Protect e o Operations Center no mesmo sistema.

Antes de Iniciar

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

1. AIX
   Verifique se os arquivos RPM necessários estão instalados em seu sistema.

   Consulte “Instalando arquivos RPM de pré-requisito para o assistente gráfico” na página 46 para obter mais detalhes.
2. Antes de fazer download do pacote de instalação, verifique se há espaço suficiente para armazenar os arquivos de instalação quando eles forem extraídos do pacote do produto.

   Para obter os requisitos de espaço, consulte o documento de download em nota técnica 588093.
3. Acesse Passport Advantage e faça download do arquivo de pacote para um diretório vazio de sua escolha.
4. 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
   ```
5. Extraia o pacote emitindo o seguinte comando:

   ```
   ./package_name.bin
   ```

   em que *package_name* é o nome do arquivo transferido por download.
6. AIX
   Assegure-se de que o comando a seguir esteja ativado para que os assistentes funcionem adequadamente:

   ```
   lsuser
   ```

   Por padrão, o comando está ativado.
7. Vá para o diretório onde colocou o arquivo executável.
8. Inicie o assistente de instalação emitindo o seguinte comando:

   ```
   ./install.sh
   ```

   Ao selecionar os pacotes para instalar, escolha o servidor e o Operations Center.

O que Fazer Depois

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

  Para visualizar arquivos de log de instalação da ferramenta do Installation Manager, clique em **Arquivo** > **Visualizar log**. Para coletar esses arquivos de log da ferramenta do Installation Manager, clique em **Ajuda** > **Exportar dados para análise de problemas**.
- Após instalar o servidor e antes de customizá-lo para seu uso, acesse Site de suporte do IBM Spectrum Protect. Clique em **Suporte e Downloads** e aplique todas as correções aplicáveis.

AIX Instalando arquivos RPM de pré-requisito para o assistente gráfico

Os arquivos RPM são necessários para o assistente gráfico do IBM Installation Manager.

Procedimento

1. Verifique se os seguintes arquivos estão instalados no sistema. Se os arquivos não estiverem instalados, acesse a Etapa 2.

```
atk-1.12.3-2.aix5.2.ppc.rpm                libpng-1.2.32-2.aix5.2.ppc.rpm
cairo-1.8.8-1.aix5.2.ppc.rpm               libtiff-3.8.2-1.aix5.2.ppc.rpm
expat-2.0.1-1.aix5.2.ppc.rpm               pango-1.14.5-4.aix5.2.ppc.rpm
fontconfig-2.4.2-1.aix5.2.ppc.rpm          pixman-0.12.0-3.aix5.2.ppc.rpm
freetype2-2.3.9-1.aix5.2.ppc.rpm           xcursor-1.1.7-3.aix5.2.ppc.rpm
gettext-0.10.40-6.aix5.1.ppc.rpm           xft-2.1.6-5.aix5.1.ppc.rpm
glib2-2.12.4-2.aix5.2.ppc.rpm              xrender-0.9.1-3.aix5.2.ppc.rpm
gtk2-2.10.6-4.aix5.2.ppc.rpm               zlib-1.2.3-3.aix5.1.ppc.rpm
libjpeg-6b-6.aix5.1.ppc.rpm
```

2. Assegure-se de que haja pelo menos 150 MB de espaço livre no sistema de arquivos `/opt`.
3. No diretório em que o pacote de instalação foi extraído, acesse o diretório `gtk`.
4. Faça o download dos arquivos RPM para o diretório atualmente em funcionamento no website do IBM AIX Toolbox for Linux Applications emitindo o comando a seguir:

```
download-prerequisites.sh
```

5. No diretório que contém os arquivos RPM transferidos por download, instale-os emitindo o seguinte comando:

```
rpm -Uvh *.rpm
```

Instalando em sistemas Windows

Instale o servidor do IBM Spectrum Protect e o Operations Center no mesmo sistema.

Antes de Iniciar

Certifique-se de que os seguintes requisitos sejam atendidos:

- 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.
- Certifique-se de que o ID do usuário que você planeja usar durante a instalação seja um usuário com autoridade do Administrador local.

Procedimento

1. Antes de fazer download do pacote de instalação, verifique se há espaço suficiente para armazenar os arquivos de instalação quando eles forem extraídos do pacote do produto.

   Para obter os requisitos de espaço, consulte o documento de download em nota técnica 588095.
2. Acesse Passport Advantage e faça download do arquivo de pacote para um diretório vazio de sua escolha.

3. Vá para o diretório onde colocou o arquivo executável.
4. Dê um clique duplo no arquivo executável para extrair para o diretório atual.
5. No diretório em que os arquivos de instalação foram extraídos, inicie o assistente de instalação dando um clique duplo no arquivo `install.bat`.

   Ao selecionar os pacotes para instalar, escolha o servidor e o Operations Center.

O que Fazer Depois

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

  Para visualizar arquivos de log de instalação da ferramenta do Installation Manager, clique em **Arquivo** > **Visualizar log**. Para coletar esses arquivos de log da ferramenta do Installation Manager, clique em **Ajuda** > **Exportar dados para análise de problemas**.
- Após instalar o servidor e antes de customizá-lo para seu uso, acesse Site de suporte do IBM Spectrum Protect. Clique em **Suporte e Downloads** e aplique todas as correções aplicáveis.

Configurando o servidor e o Operations Center

Depois de instalar os componentes, conclua a configuração para o servidor IBM Spectrum Protect e o Operations Center.

Configurando a instância do servidor

Use o assistente de configuração da instância do servidor do IBM Spectrum Protect para concluir a configuração inicial do servidor.

Antes de Iniciar
Certifique-se de que os requisitos a seguir sejam atendidos:

Linux AIX

- 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*.
- É necessário poder efetuar login no IBM Spectrum Protect com o ID do usuário 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.
- Se você mudou alguma configuração nas etapas anteriores, reinicie o servidor antes de continuar com o assistente de configuração.

Windows Verifique se o serviço de registro remoto foi iniciado concluindo as etapas a seguir:

1. Clique em **Iniciar** > **Ferramentas administrativas** > **Serviços**. Na janela **Serviços**, selecione **Registro remoto**. Se ele não estiver iniciado, clique em **Iniciar**.
2. Assegure-se de que as portas 137, 139 e 445 não estejam bloqueadas por um firewall:
   a. Clique em **Iniciar** > **Painel de controle** > **Windows Firewall**.
   b. Selecione **Configurações avançadas**.
   c. Selecione **Regras de Entrada**.
   d. Selecione **Nova regra**.

e. Crie uma regra de porta para as portas TCP 137, 139 e 445 para permitir conexões para redes de domínio e privadas.

3. Configure o controle de conta do usuário acessando as opções de política de segurança local e concluindo as etapas a seguir.
   a. Clique em **Iniciar** > **Ferramentas administrativas** > **Política de segurança local**. Expanda **Políticas locais** > **Opções de segurança**.
   b. Se ainda não estiver ativada, ative a conta do administrador integrado, selecionando **Contas: Status da conta do administrador** > **Ativar** > **OK**.
   c. Se ainda não estiver desativado, desative o controle de conta do usuário para todos os administradores do Windows, selecionando **Controle de conta do usuário: executar todos os administradores no modo de aprovação de administrador** > **Desativar** > **OK**.
   d. Se ainda não estiver desativado, desative o Controle de conta do usuário para a conta do Administrador integrado, selecionando **Controle de conta do usuário: modo de aprovação do administrador para a conta do administrador integrado** > **Desativar** > **OK**.
4. Se você mudou alguma configuração nas etapas anteriores, reinicie o servidor antes de continuar com o assistente de configuração.

Sobre Esta Tarefa

O assistente pode ser interrompido e reiniciado, mas o servidor não estará operacional até que todo o processo de configuração esteja concluído.

Procedimento

1. Inicie a versão local do assistente.
   - Linux AIX Abra o programa `dsmicfgx` no diretório `/opt/tivoli/tsm/server/bin`. Este assistente pode ser executado somente como um usuário raiz.
   - Windows Clique em **Iniciar** > **Todos os programas** > **IBM Spectrum Protect** > **Assistente de configuração**.
2. Siga as instruções para concluir a configuração.

   Use as informações que você registrou no “Planilhas de planejamento” na página 8 durante a configuração do sistema IBM Spectrum Protect para especificar diretórios e opções no assistente.

   Linux AIX Na janela **Informações do servidor**, configure o servidor para iniciar automaticamente usando o ID do usuário da instância quando o sistema for inicializado.

   Windows Usando o assistente de configuração, o servidor é configurado para iniciar automaticamente quando reinicializado.

Instalando o cliente de backup-archive

Como uma melhor prática, instale o cliente de backup-archive do IBM Spectrum Protect no sistema do servidor para que o cliente da linha de comando administrativo e o planejador estejam disponíveis.

Procedimento

- Para instalar o cliente de backup-archive, siga as instruções de instalação para seu sistema operacional.
  - Instale deus clientes de archive de backup do UNIX e do Linux
  - Instalando o cliente Windows pela primeira vez

Configurando opções para o servidor

Revise o arquivo de opções do servidor que está instalado com o servidor do IBM Spectrum Protect para verificar se os valores corretos estão configurados para seu sistema.

Procedimento

1. Acesse o diretório de instância do servidor e abra o arquivo `dsmserv.opt`.
2. Revise os valores na tabela a seguir e verifique as configurações de opção do servidor, com base no tamanho do sistema.

Opção do servidor	Valor
ACTIVELOGDIRECTORY	Caminho do diretório especificado durante a configuração
ACTIVELOGSIZE	131072
ARCHLOGCOMPRESS	Sim
ARCHLOGDIRECTORY	Caminho do diretório especificado durante a configuração
COMMMETHOD	TCPIP
COMMTIMEOUT	3600
DEVCONFIG	`devconf.dat`
EXPINTERVAL	0
IDLETIMEOUT	60
MAXSESSIONS	500
NUMOPENVOLSALLOWED	20
TCPADMINPORT	1500
TCPPORT	1500
VOLUMEHISTORY	`volhist.dat`

Atualize as configurações de opção do servidor, se necessário, para que correspondam aos valores na tabela. Para fazer atualizações, feche o arquivo `dsmserv.opt` e use o comando **SETOPT** a partir da interface da linha de comandos administrativa para configurar as opções.

Por exemplo, para atualizar a opção `IDLETIMEOUT` para 60, emita o seguinte comando:

```
setopt idletimeout 60
```

3. Para configurar comunicações seguras para o servidor, clientes e o Operations Center, verifique as opções na tabela a seguir.

Opção do servidor	Todos os tamanhos do sistema
SSLDISABLELEGACYTLS	YES
SSLFIPSMODE	NO
SSLTCPPORT	Especifique o número da porta SSL. O driver de comunicação TCP/IP do servidor aguarda solicitações nessa porta para sessões ativadas para SSL do cliente.
SSLTCPADMINPORT	Especifique o endereço de porta no qual o servidor aguarda solicitações para sessões ativadas para SSL do cliente administrador da linha de comandos.
TLS12	YES

Se algum dos valores da opção tiver que ser atualizado, edite o arquivo `dsmserv.opt` usando as seguintes diretrizes:

- Remova o asterisco no início de uma linha para ativar uma opção.
- Em cada linha, insira apenas uma opção e o valor especificado para a opção.
- Se uma opção ocorrer em diversas entradas no arquivo, o servidor usará a última entrada.

Salve suas mudanças e feche o arquivo. Se você editar o arquivo `dsmserv.opt` diretamente, será necessário reiniciar o servidor para que as mudanças entrem em vigor.

Conceitos de segurança

É possível proteger o IBM Spectrum Protect de riscos de segurança usando protocolos de comunicação, protegendo senhas e fornecendo diferentes níveis de acesso para administradores.

Segurança da Camada de Transporte

É possível usar o protocolo de Secure Sockets Layer (SSL) ou de Segurança da Camada de Transporte (TLS) para fornecer segurança da camada de transporte para uma conexão segura entre servidores, clientes e agentes de armazenamento. Se você enviar dados entre o servidor, o cliente e o agente de armazenamento, use SSL ou TLS para criptografar os dados.

Dica: Qualquer documentação do IBM Spectrum Protect que indique "SSL" ou "selecionar SSL" se aplica ao TLS.

O SSL é fornecido pelo Global Security Kit (GSKit) que está instalado com o servidor do IBM Spectrum Protect que é usado pelo servidor, cliente e agente de armazenamento.

Restrição: Não use os protocolos SSL ou TLS para comunicações com uma instância de banco de dados do IBM Db2 usada por qualquer servidor do IBM Spectrum Protect.

Cada servidor, cliente ou agente de armazenamento que ativa o SSL deve usar um certificado autoassinado confiável ou obter um certificado exclusivo que seja assinado por uma autoridade de certificação (CA). É possível usar seus próprios certificados ou comprar certificados de uma CA. O certificado deve ser instalado e incluído no banco de dados de chaves no servidor, cliente ou agente de armazenamento do IBM Spectrum Protect. O certificado é verificado pelo cliente ou servidor SSL que solicita ou inicia a comunicação de SSL. Alguns certificados de CA são pré-instalados nos bancos de dados de chaves, por padrão.

O SSL é configurado de forma independente no servidor, cliente e agente de armazenamento do IBM Spectrum Protect.

Níveis de Autoridade

Com cada servidor IBM Spectrum Protect, há diferentes níveis de autoridade administrativa disponíveis que determinam quais tarefas um administrador pode concluir.

Após o registro, um administrador deve receber autoridade, sendo designado a um ou mais níveis de autoridade administrativa. Um administrador com autoridade do sistema pode concluir qualquer tarefa com o servidor e designar níveis de autoridade a outros administradores usando o comando **GRANT AUTHORITY**. Os administradores com autoridade de política, de armazenamento ou de operador podem concluir subconjuntos de tarefas.

Um administrador pode registrar outros IDs de administrador, conceder níveis de autoridade a eles, renomear IDs, remover IDs e bloquear e desbloqueá-los do servidor.

Um administrador pode controlar o acesso a nós clientes específicos para IDs do usuário raiz e IDs do usuário não raiz. Por padrão, um ID do usuário não raiz não pode fazer backup de dados no nó. Use o comando **UPDATE NODE** para alterar as configurações do nó para ativar o backup.

Senhas

Por padrão, o servidor usa automaticamente a autenticação de senha. Com a autenticação de senha, todos os usuários devem inserir uma senha quando acessarem o servidor.

Use o Lightweight Directory Access Protocol (LDAP) para aplicar requisitos mais rigorosos para senhas. Para obter informações adicionais, consulte Gerenciando senhas e procedimentos de logon (V7.1.1).

Tabela 14. Características de autenticação de senha

Característica	**Informações adicionais**
Distinção entre maiúsculas e minúsculas	Não distingue entre maiúsculas e minúsculas.
Expiração de senha padrão	90 dias. O período de expiração começa quando um ID de administrador ou nó cliente é registrado pela primeira vez no servidor. Se a senha não for mudada nesse período, ela deverá ser mudada na próxima vez que o usuário acessar o servidor.
Tentativas de senha inválida	É possível configurar um limite nas tentativas consecutivas de senha inválida para todos os nós clientes. Quando o limite for excedido, o servidor bloqueará o nó.
Comprimento de senha padrão	8 caracteres. O administrador pode especificar um comprimento mínimo. Começando com a Versão 8.1.4, o comprimento mínimo padrão para senhas do servidor mudou de 0 para 8 caracteres.

Segurança da Sessão

Segurança de sessão é o nível de segurança que é usado para a comunicação entre os nós clientes, clientes administrativos e servidores do IBM Spectrum Protect e é configurada usando o parâmetro **SESSIONSECURITY**.

O parâmetro **SESSIONSECURITY** pode ser configurado com um dos seguintes valores:

- O valor STRICT aplica o nível mais alto de segurança para a comunicação entre servidores, nós e administradores do IBM Spectrum Protect.
- O valor TRANSITIONAL especifica que o protocolo de comunicação existente é usado ao atualizar o software IBM Spectrum Protect para a V8.1.2 ou mais recente. Esse é o padrão. Quando o valor é **SESSIONSECURITY=TRANSITIONAL**, configurações de segurança mais restritas são automaticamente aplicadas quanto mais altas as versões do protocolo TLS utilizado e quando o software é atualizado para a V8.1.2 ou posterior. Após um nó, administrador ou servidor atender aos requisitos para o valor STRICT, a segurança de sessão é atualizada automaticamente para o valor STRICT e a entidade não poderá mais se autenticar usando uma versão anterior do cliente ou protocolos TLS anteriores.

  Nota: Não é necessário atualizar clientes de backup e archive para a V8.1.2 ou mais recente antes de fazer upgrade de servidores. Depois de fazer upgrade de um servidor para V8.1.2 ou posterior, nós e administradores que usam versões anteriores do software continuarão a se comunicar 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 archive de backup para a V8.1.2 ou posterior antes de fazer upgrade de seus servidores do IBM Spectrum Protect, mas não é obrigatório atualizar os servidores primeiro. A comunicação entre servidores e clientes não será interrompida.

Para obter mais informações sobre os valores do parâmetro **SESSIONSECURITY**, consulte os comandos a seguir.

Tabela 15. Comandos utilizados para configurar o parâmetro SESSIONSECURITY	
Entidade	**Command**
Nós clientes	• REGISTER NODE • UPDATE NODE
Administradores	• REGISTER ADMIN • UPDATE ADMIN
Servidores	• DEFINE SERVER • UPDATE SERVER

Os administradores que autenticam usando o comando **DSMADMC**, o comando **DSMC** ou o programa dsm não podem se autenticar usando uma versão anterior após executar a autenticação usando a V8.1.2 ou mais recente. Para resolver problemas de autenticação para administradores, consulte as seguintes dicas:

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.
- Depois que um administrador é autenticado no servidor com êxito usando as versões de software V8.1.2, V7.1.8 ou mais recentes, ele não pode mais se autenticar nesse servidor usando as versões de cliente ou de servidor anteriores a essas. 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.

Force o nível mais alto de segurança para a comunicação com o servidor IBM Spectrum Protect, assegurando que todos os nós, administradores e servidores usem a segurança de sessão STRICT. É possível usar o comando **SELECT** para determinar quais servidores, nós e administradores estão usando a segurança de sessão `TRANSITIONAL` e devem ser atualizados para usar a segurança de sessão `STRICT`.

Informações relacionadas

Protegendo Comunicações

Configurando comunicações seguras com a Segurança da Camada de Transporte

Para criptografar os dados e as comunicações seguras em seu ambiente, o Secure Sockets Layer (SSL) ou a Segurança da Camada de Transporte (TLS) é ativada no servidor IBM Spectrum Protect e no cliente de backup-archive. Um certificado SSL é usado para verificar solicitações de comunicação entre o servidor e o cliente.

Sobre Esta Tarefa

Conforme mostrado na figura a seguir, é possível configurar manualmente as comunicações seguras entre o servidor e o cliente de backup-archive, configurando opções nos arquivos de opções do servidor e do cliente e, em seguida, transferindo o certificado autoassinado, que é gerado no servidor, para o cliente. Como alternativa, é possível obter e transferir um certificado exclusivo que é assinado por uma autoridade de certificação (CA).

Para obter mais informações sobre como configurar o servidor e os clientes para comunicações de SSL ou de TLS, consulte Configurando agentes de armazenamento, servidores, clientes e o Operations Center para se conectar ao servidor usando SSL.

Configurando o Operations Center

Após instalar o Operations Center, conclua as etapas a seguir de configuração para começar a gerenciar seu ambiente de armazenamento.

Antes de Iniciar

Ao conectar-se ao Operations Center pela primeira vez, é necessário fornecer as informações a seguir:

- 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

Procedimento

1. Designe o servidor do hub.

   Em um navegador da web, insira o seguinte endereço:

   ```
   https://hostname:secure_port/oc
   ```

   onde:

   - *hostname* representa o nome do computador no qual o Operations Center está instalado
   - *secure_port* representa o número da porta que o Operations Center usa para comunicação HTTPS nesse computador

   Por exemplo, se seu nome do host for tsm.storage.mylocation.com e você estiver usando a porta segura padrão para o Operations Center, que é 11090, o endereço será:

   ```
   https://tsm.storage.mylocation.com:11090/oc
   ```

   Ao efetuar login no Operations Center pela primeira vez, um assistente o orienta por uma configuração inicial para configurar um novo administrador com autoridade do sistema no servidor.
2. Configure as comunicações seguras entre o Operations Center e o servidor do hub configurando o protocolo Secure Sockets Layer (SSL).

   Siga as instruções em “Protegendo as comunicações entre o Operations Center e o servidor do hub” na página 54.
3. Opcional: Para receber um relatório de email diário que resume o status do sistema, defina suas configurações de email no Operations Center.

   Siga as instruções em “Rastreando o status do sistema usando relatórios de e-mail” na página 154.

Protegendo as comunicações entre o Operations Center e o servidor do hub

Para proteger as comunicações entre o Operations Center e o servidor do hub, inclua o certificado Segurança da Camada de Transporte (TLS) do servidor do hub no 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. Ele 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 proteger a comunicação 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, poderá reconfigurá-la.

A figura a seguir ilustra os componentes para configurar SSL entre o Operations Center e o servidor do hub.

Sobre Esta Tarefa

Este procedimento fornece etapas para implementar comunicações seguras usando certificados autoassinados.

Procedimento

Para configurar a comunicação de SSL usando certificados autoassinados, conclua as etapas a seguir.

1. Especifique o certificado `cert256.arm` como o certificado padrão no arquivo do banco de dados de chaves do servidor do hub:
   a) Emita o comando a seguir a partir do diretório de instâncias do servidor do hub:

   ```
   gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
        -label "TSM Server SelfSigned SHA Key"
   ```

   b) Reinicie o servidor do hub para que possa receber as mudanças para o arquivo do banco de dados de chave.
   c) Verifique se o certificado `cert256.arm` está configurado como o padrão. Emita o seguinte comando:

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

2. Pare o servidor da web Operations Center.
3. Abra a linha de comandos do sistema operacional no sistema em que o Operations Center está instalado e mude para o diretório a seguir:
   - Linux AIX *installation_dir*/ui/jre/bin
   - Windows *installation_dir*\ui\jre\bin

   Em que *installation_dir* representa o diretório no qual o Operations Center está instalado.
4. Abra a janela IBM Key Management emitindo o seguinte comando:

```
ikeyman
```

5. Clique em **Arquivo do Banco de Dados de Chave** > **Abrir**.
6. Clique em **Procurar** e acesse o seguinte diretório, em que *installation_dir* representa o diretório no qual o Operations Center está instalado:
   - Linux AIX *installation_dir*/ui/Liberty/usr/servers/guiServer
   - Windows *installation_dir*\ui\Liberty\usr\servers\guiServer
7. No diretório guiServer, selecione o arquivo gui-truststore.jks.
8. Clique em **Abrir** e clique em **OK**.
9. Insira a senha para o arquivo de armazenamento confiável e clique em **OK**.
10. Na área Conteúdo do banco de dados de chaves da janela IBM Key Management, clique na seta e selecione **Certificados do assinante** da lista. Clique em **Incluir**.
11. Na janela Abrir, clique em **Procurar** e acesse o diretório de instância do servidor do hub:
    - Linux AIX /opt/tivoli/tsm/server/bin
    - Windows c:\Program Files\Tivoli\TSM\server1

    O diretório contém o cert256.arm certificado.

    Se não for possível acessar o diretório de instância do servidor do hub a partir da janela Abrir, conclua as etapas a seguir:

    a) Use o FTP ou outro método de transferência de arquivos para copiar os arquivos cert256.arm do servidor do hub para o seguinte diretório no computador em que o Operations Center está instalado:
       - Linux AIX *installation_dir*/ui/Liberty/usr/servers/guiServer
       - Windows *installation_dir*\ui\Liberty\usr\servers\guiServer

    b) Na janela Abrir, acesse o diretório guiServer.
12. Selecione o certificado cert256.arm como o certificado SSL.
13. Clique em **Abrir** e clique em **OK**.
14. Insira um rótulo para o certificado. Por exemplo, insira o nome do servidor do hub.
15. 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.
16. Feche a janela IBM Key Management.
17. Inicie o servidor da web Operations Center.

    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. Se a opção do servidor ADMINONCLIENTPORT estiver ativada para o servidor IBM Spectrum Protect, insira o número da porta que é especificado pela opção do servidor TCPADMINPORT. Se a opção do servidor ADMINONCLIENTPORT não estiver ativada, insira o número da porta especificado pela opção do servidor TCPPORT.

Registrando a licença do produto

Para registrar sua licença para o produto IBM Spectrum Protect, use o comando **REGISTER LICENSE**.

Sobre Esta Tarefa

As licenças são armazenadas em arquivos de certificado de inscrição, que contêm informações sobre licença para o produto. Os arquivos de certificado de inscrição estão na mídia de instalação e são colocados no servidor durante a instalação. Ao registrar o produto, as licenças são armazenadas em um arquivo NODELOCK no diretório atual.

Procedimento

Registre uma licença especificando o nome do arquivo de certificado de inscrição que contém a licença. Para usar o construtor de comando do Operations Center para essa tarefa, conclua as etapas a seguir.

1. Abra o Operations Center.
2. Abra o construtor de comando do Operations Center, passando o mouse sobre o ícone de configurações e clicando em **Construtor de comando**.
3. Emita o comando **REGISTER LICENSE**.
   Por exemplo, para registrar uma licença do IBM Spectrum Protect base, emita o seguinte comando:

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

O que Fazer Depois

Salve a mídia de instalação que contém seus arquivos de certificado de inscrição. Pode ser necessário registrar sua licença novamente se, por exemplo, ocorrer uma das seguintes condições:

- O servidor foi movido para um computador diferente.
- O arquivo NODELOCK está corrompido. O servidor armazena informações sobre licença no arquivo NODELOCK, que está no diretório a partir do qual o servidor é iniciado.
- Linux Se você mudar o chip do processador associado ao servidor no qual o servidor está instalado.

Definindo regras de retenção de dados para seus negócios

Após criar um conjunto de armazenamentos de contêiner de diretório para deduplicação de dados, atualize a política do servidor padrão para usar o novo conjunto de armazenamentos. O assistente **Incluir conjunto de armazenamentos** abre a página **Serviços** no Operations Center para concluir esta tarefa.

Procedimento

1. Na página **Serviços** do Operations Center, selecione o domínio STANDARD e clique em **Detalhes**.
2. Na página **Resumo** do domínio de política, clique na guia **Conjuntos de políticas**.
   A página **Conjuntos de políticas** indica o nome do conjunto de políticas ativas e lista todas as classes de gerenciamento para esse conjunto de políticas.
3. Clique na alternância **Configurar** e faça as seguintes mudanças:
   - Mude o destino de backup para a classe de gerenciamento STANDARD para o conjunto de armazenamentos de contêiner de diretório.
   - Mude o valor para a coluna Backups para **Sem limite**.
   - Mude o período de retenção. Configure a coluna Manter Backups Extras para 30 dias ou mais, dependendo de suas necessidades de negócios.
4. Salve suas mudanças e clique na alternância **Configurar** novamente de forma que o conjunto de políticas não seja mais editável.
5. Ative o conjunto de políticas clicando em **Ativar**.

Definindo planejamentos para atividades de manutenção de servidor

Crie planejamentos para cada operação de manutenção de servidor usando o comando **DEFINE SCHEDULE** no construtor de comando do Operations Center.

Sobre Esta Tarefa

Planeje operações de manutenção do servidor para serem executadas após as operações de backup de cliente. É possível controlar a sincronização de planejamentos configurando o horário de início em conjunto com o tempo de duração de cada operação.

A figura a seguir fornece um exemplo de como planejar operações de manutenção.

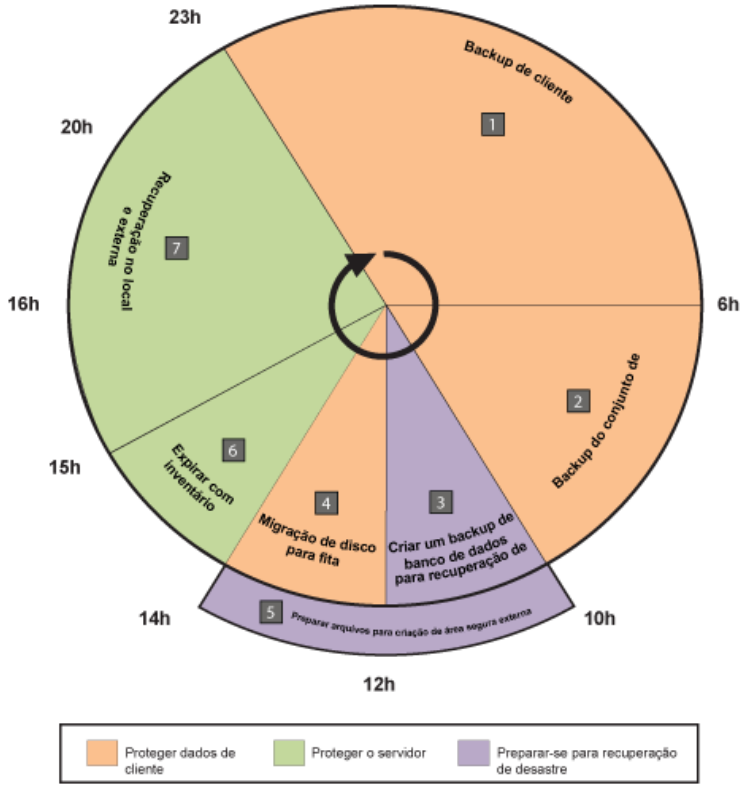


Figura 4. Planejamento diário de operações do servidor para uma solução de fita

A tabela a seguir mostra como é possível planejar processos de manutenção de servidor em conjunto com o planejamento de backup do cliente para uma solução de fita.

Operação	**Planejamento**
Backup de cliente	Começa às 23h.
Backup do conjunto de armazenamentos	Começa às 6h.
Processamento para arquivos do banco de dados e de recuperação de desastre	• A operação de backup de banco de dados começa às 10h ou 11 horas após o início da operação de backup do cliente. Este processo é executado até a conclusão. • As informações de configuração do dispositivo e as operações de backup de histórico do volume começam às 17h ou 7 horas após o início da operação de backup de banco de dados. • A exclusão do histórico do volume começa às 20h ou 10 horas após o início da operação de backup de banco de dados.
Preparação de arquivos para criação de área segura externa	Começa às 10h, ao mesmo tempo que o processamento para os arquivos do banco de dados e de recuperação de desastre.
Migração de disco para fita	Começa às 12h ou 2 horas após o início da operação de backup de banco de dados.

Operação	Planejamento
Expiração de inventário	Começa às 14h ou 15 horas após o início da operação de backup do cliente. Este processo é executado até a conclusão.
Solicitação de Espaço	Começa às 15h ou 16 horas após o início da operação de backup do cliente.

Procedimento

Depois de configurar a classe de dispositivo para as operações de backup de banco de dados, crie planejamentos para backup de banco de dados e outras operações de manutenção necessárias usando o comando **DEFINE SCHEDULE**. Dependendo do tamanho de seu ambiente, pode ser necessário ajustar os horários de início para cada planejamento no exemplo.

1. Defina uma classe de dispositivo para a operação de backup antes de criar o planejamento para backups de banco de dados.

   Use o comando **DEFINE DEVCLASS** para criar uma classe de dispositivo chamada LTOTAPE:

   ```
   define devclass ltotape devtype=lto library=ltolib
   ```

2. Configure a classe de dispositivo para backups de banco de dados automáticos. Use o comando **SET DBRECOVERY** para especificar a classe de dispositivo que você criou para o backup de banco de dados na etapa anterior.
   Por exemplo, se a classe de dispositivo for LTOTAPE, emita o seguinte comando:

   ```
   set dbrecovery ltotape
   ```

3. Crie planejamentos para as operações de manutenção, usando o comando **DEFINE SCHEDULE**. Consulte a tabela a seguir para as operações necessárias com exemplos dos comandos.

Operação	Comandos de exemplo e informações adicionais
Backup de conjuntos de armazenamentos.	Crie um planejamento para executar o comando **BACKUP STGPOOL**. Por exemplo, emita o seguinte comando para criar um planejamento de backup para um conjunto de armazenamentos primários chamado PRIMARY_POOL. O conjunto será submetido a backup para um conjunto de armazenamento de cópia, COPYSTG: `define schedule BACKUPSTGPOOL type=administrative cmd="backup stgpool primary_pool copystg" active=yes starttime=06:00 period=1`
Faça backup do banco de dados.	Crie um planejamento para executar o comando **BACKUP DB**. Por exemplo, emita o seguinte comando para criar um planejamento de backup que usa a nova classe de dispositivo: `define schedule DBBACKUP type=admin cmd="backup db devclass=ltotape type=full numstreams=3 wait=yes compress=yes" active=yes desc="Back up the database." startdate=today starttime=10:00:00 duration=45 durunits=minutes`
Replique os nós.	Opcionalmente, use a replicação de nó para proteger dados de cliente fazendo backup dos dados para um servidor secundário. Para obter instruções, consulte Replicando dados do cliente para outro servidor. Certifique-se de que a replicação de nó seja concluída antes do início das operações de migração.

Operação	Comandos de exemplo e informações adicionais
Migre dados do disco para a fita diariamente.	Crie um planejamento para a migração do conjunto de armazenamentos. Por exemplo, se um conjunto de armazenamentos em disco chamar-se DISKPOOL e o próximo conjunto de armazenamentos for TAPEPOOL, será possível planejar a migração do conjunto de armazenamentos emitindo o seguinte comando: `define schedule stgpool_migration type=administrative cmd="migrate stgpool diskpool lomig=0" active=yes description="migrate disk storagepool to tapepool" startdate=today starttime=12:00 duration=2 durunits=hours period=1 perunits=days` Para aumentar o rendimento, é possível especificar o número de processos paralelos a serem usados para arquivos de migração concluindo as seguintes etapas: a. Para o conjunto de armazenamento em fita, certifique-se de que a disposição esteja ativada. Para verificar se a disposição está ativada, execute o comando **QUERY STGPOOL**. Verifique se um valor de GROUP, NODE ou FILESPACE está especificado no campo COLLOCATE. Se um valor de GROUP, NODE ou FILESPACE não for especificado, use o comando **UPDATE STGPOOL** para especificar COLLOCATE=GROUP, COLLOCATE=NODE ou COLLOCATE=FILESPACE, dependendo da configuração do sistema. b. Para o conjunto de armazenamentos em disco, use o comando **DEFINE STGPOOL** ou **UPDATE STGPOOL** para especificar um valor para o parâmetro **MIGPROCESS**. Por exemplo, se você tiver 12 unidades de fita, especifique MIGPROCESS=10. Dessa forma, é usado um máximo de 10 unidades de fita para processos de migração. Duas unidades são reservadas para outras tarefas, como operações de restauração, backup de banco de dados e backup de cliente.
Prepare arquivos para criação de área segura externa.	a. Mova volumes de fita externos seguindo as instruções em “Movendo mídia de backup” na página 61. b. Crie o arquivo de plano de recuperação de desastres emitindo o comando **PREPARE** no servidor de origem: `preparar` c. Certifique-se de que todos os volumes que são necessários para recuperação de desastre sejam incluídos no arquivo de plano de recuperação. Para obter informações adicionais, consulte “Preparando para um desastre e recuperando-se de um desastre usando o DRM” na página 212.
Faça backup das informações de configuração do dispositivo.	Crie um planejamento para executar o comando **BACKUP DEVCONFIG**: `define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Backup the device configuration file." startdate=today starttime=17:00:00 duration=45 durunits=minutes`

Operação	Comandos de exemplo e informações adicionais
Faça backup do histórico do volume.	Crie um planejamento para executar o comando **BACKUP VOLHISTORY**: `define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Back up the volume history." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Remova versões mais antigas dos backups de banco de dados que não sejam mais necessárias.	Crie um planejamento para executar o comando **DELETE VOLHISTORY**: `define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Remove old database backups." startdate=today starttime=20:00:00 duration=45 durunits=minutes`
Remova objetos que excedem sua retenção permitida.	Crie um planejamento para executar o comando **EXPIRE INVENTORY**. Configure o parâmetro **RESOURCE** com base no tamanho do sistema que está sendo configurado para ser igual ao número de núcleos do processador especificado para seu sistema. Por exemplo, emita o seguinte comando para criar um planejamento chamado EXPINVENTORY: `define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=8 duration=120" active=yes desc="Remove expired objects." startdate=today starttime=14:00:00 duration=1 durunits=hours`
Recupere o espaço.	Crie um planejamento para executar o comando **RECLAIM STGPOOL**. Por exemplo, emita o seguinte comando para criar um planejamento chamado RECLAIM: `define schedule RECLAIM type=admin cmd="reclaim stgpool tapepool duration=60" startdate=today starttime=15:00:00 duration=5 durunits=hours` **Dica:** Para aumentar o rendimento, é possível especificar o número de processos paralelos a serem usados para recuperar espaço. Atualize o conjunto de armazenamento em fita usando o comando **UPDATE STGPOOL** e especifique um valor para o parâmetro **RECLAIMPROCESS**. Por exemplo, se você tiver 12 unidades de fita, especifique RECLAIMPROCESS=5. Como são usadas duas unidades para cada processo de recuperação, o número total de unidades que podem ser usadas para recuperação é 10. Duas unidades são reservadas para operações de backup.

O que Fazer Depois

Depois de criar planejamentos para tarefas de manutenção de servidor, é possível visualizá-los no Operations Center concluindo as etapas a seguir:

1. Na barra de menus do Operations Center, passe o mouse sobre **Servidores**.
2. Clique em **Manutenção**.

Informações relacionadas

UPDATE STGPOOL (Atualizar um conjunto de armazenamentos)
DEFINE SCHEDULE (Definir um planejamento de um comando administrativo)
DEFINE STGPOOL (definir um volume em um conjunto de armazenamentos)

Movendo mídia de backup

Para recuperar-se de um desastre, você precisa de volumes de backup de banco de dados, volumes do conjunto de armazenamentos de cópia e de arquivos adicionais. Para ficar preparado para um desastre, você deve concluir tarefas diárias.

Antes de Iniciar

Para exibir todos os volumes do conjunto de armazenamento de cópia virtual e de backup de banco de dados que têm seus objetos de backup no servidor de destino remoto, emita o comando **QUERY DRMEDIA**:

```
query drmedia * wherestate=remote
```

Sobre Esta Tarefa

A figura a seguir mostra o ciclo de vida de uma operação típica de movimentação de mídia de backup para fora e de volta a um local, como parte das operações de recuperação de desastres.

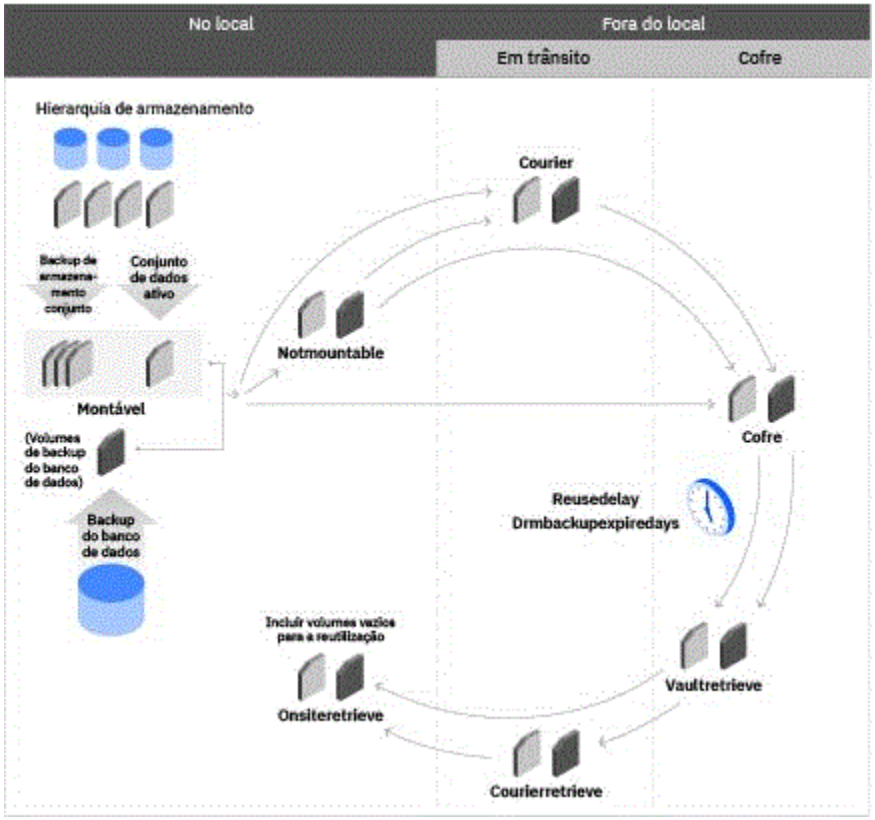


Figura 5. Ciclo de vida de mídia de recuperação

O gerenciador de recuperação de desastres (DRM) designa os estados de mídia a seguir aos volumes. Os estados de mídia rastreiam um volume conforme ele se move de um local para outro. Alguns estados de mídia são opcionais. Dependendo da precisão com a qual sua organização deseja rastrear os movimentos de um volume, será possível ignorar esses estados de mídia opcionais.

MOUNTABLE
O volume contém dados válidos, está no local e pode ser acessado pelo servidor IBM Spectrum Protect.

NOTMOUNTABLE
O volume contém dados válidos e está no local, mas não pode ser acessado pelo servidor IBM Spectrum Protect.

COURIER
O volume contém dados válidos e está em trânsito para a área segura.

VAULT
O volume contém dados válidos e está na área segura.

VAULTRETRIEVE
O volume, que está na área segura externa, não contém mais dados válidos e deve ser retornado para o local.

COURIERRETRIEVE
O volume não contém mais dados válidos e será retornado pelo courier.

ONSITERETRIEVE
O volume não contém mais dados válidos e será movido de volta para o local. Os registros de volume do backup do banco de dados, os volumes do conjunto de armazenamento de cópia de rascunho e os volumes do conjunto de dados ativos de rascunho são excluídos do banco de dados. Para os volumes de conjunto de armazenamento de cópia privados e os volumes de conjunto de dados ativos, o modo de acesso foi atualizado para READWRITE.

Movendo volumes do conjunto de armazenamentos de cópia externos

É possível enviar sua mídia de backup externa depois de criar as cópias de backup de seus conjuntos de armazenamentos primários e banco de dados. Para enviar mídia externa, marque os volumes como indisponíveis para o IBM Spectrum Protect e entregue-os ao transportador.

Antes de Iniciar

Certifique-se de que os processos de backup do conjunto de armazenamentos estejam concluídos. Dessa forma, é possível evitar problemas que podem ocorrer quando os comandos **MOVE DRMEDIA** e **BACKUP STGPOOL** forem executados simultaneamente.

Dica: Para mover os volumes de retenção para fora do local, ou seja, volumes de fita que contêm dados de um ou mais conjuntos de retenção, deve-se usar o comando **MOVE RETMEDIA** ou a ação **Mover mídia** no Operations Center. Para obter informações adicionais, consulte "Movendo dados do conjunto de retenção para/de armazenamento em fita" na página 65.

Procedimento

1. Identifique os volumes do conjunto de armazenamento de cópia e de backup de banco de dados a serem movidos externamente, emitindo o comando **QUERY DRMEDIA**:

   ```
   query drmedia * wherestate=mountable
   ```

2. Indique o movimento de volumes cujo estado atual é MOUNTABLE emitindo o comando **MOVE DRMEDIA**:

   ```
   move drmedia * wherestate=mountable
   ```

   Para todos os volumes no estado MOUNTABLE, o DRM conclui as seguintes tarefas:

   - Atualiza o estado de volume para NOTMOUNTABLE e atualiza o local do volume se você tiver emitido o comando **SET DRMNOTMOUNTABLENAME**. Se você não emitiu o comando, o local padrão é NOTMOUNTABLE.
   - Atualiza o modo de acesso como indisponível para um volume do conjunto de armazenamentos de cópia.
   - Efetua check-out de volumes de bibliotecas automatizadas.

   a) Durante o processamento de check-out, as bibliotecas SCSI solicitam a intervenção do operador. Ignore essas solicitações e ejete os cartuchos da biblioteca emitindo o seguinte comando:

   ```
   move drmedia * wherestate=mountable remove=no
   ```

   b) Acesse uma lista dos volumes para identificar e remover os cartuchos da biblioteca, emitindo o seguinte comando:

```
query drmedia wherestate=notmountable
```

3. Envie os volumes para a área segura externa.
4. Para rastrear os volumes externos, emita o comando **MOVE DRMEDIA**:

   ```
   move drmedia * wherestate=notmountable
   ```

   Para todos os volumes no estado NOTMOUNTABLE, o DRM atualiza o estado de volume para COURIER e o local do volume de acordo com o comando **SET DRMCOURIERNAME**. Se você não emitiu o comando **SET**, o local padrão será COURIER.

   Dica: É possível evitar passar por todos os estados do volume emitindo o comando **MOVE DRMEDIA** e especificando a configuração de parâmetro **TOSTATE** para nomear o estado de destino. Para mudar os volumes do estado NOTMOUNTABLE para o estado VAULT, emita o comando a seguir:

   ```
   move drmedia * wherestate=notmountable tostate=vault
   ```

   Para todos os volumes no estado NOTMOUNTABLE, o DRM atualiza o estado de volume para VAULT e o local do volume de acordo com o comando **SET DRMVAULTNAME**. Se o comando **SET** ainda não foi emitido, o local padrão será VAULT.
5. Quando o local da área segura confirmar o recebimento dos volumes, emita o comando **MOVE DRMEDIA** para especificar o estado COURIER:

   ```
   move drmedia * wherestate=courier
   ```

   Para todos os volumes no estado COURIER, o DRM atualiza o estado de volume para VAULT e o local do volume de acordo com o comando **SET DRMVAULTNAME**. Se você não emitiu o comando **SET**, o local padrão será VAULT.
6. Exiba uma lista de volumes que contêm dados válidos na área segura, emitindo o seguinte comando:

   ```
   query drmedia wherestate=vault
   ```

Movendo volumes do conjunto de armazenamentos de cópia no local
É possível expirar os volumes de backup de banco de dados não virtuais e retornar os volumes no local para reutilização ou descarte, como parte de operações de recuperação de desastre.

Antes de Iniciar

Dica: Para retornar a mídia de retenção no local, ou seja, volumes que contêm dados do conjunto de retenção, deve-se usar o comando **MOVE RETMEDIA** ou operações de movimentação de mídia no Operations Center. Para obter informações adicionais, consulte “Movendo dados do conjunto de retenção para/de armazenamento em fita” na página 65.

É possível expirar um volume de backup de banco de dados quando todas as seguintes condições forem verdadeiras:

- A idade do último volume da série excede o valor de expiração. O valor de expiração é o número de dias desde o último backup na série. Na instalação, o valor de expiração é 60 dias. Para substituir esse valor, é possível emitir o comando **SET DRMDBBACKUPEXPIREDAYS**.
- Todos os volumes na série estão no estado VAULT.
- O volume não faz parte das várias séries da cópia de segurança do banco de dados atualizadas.

Inicie o processo de expiração manualmente emitindo o comando **EXPIRE INVENTORY** ou automaticamente usando a opção de configuração EXPINTERVAL que é especificada no arquivo de opções do servidor.

Procedimento

1. Especifique o número de dias antes da expiração de uma série de backups do banco de dados, emitindo o comando **SET DRMDBBACKUPEXPIREDAYS**.

Por exemplo, para configurar o número de dias para 30, emita o seguinte comando:

```
set drmdbbackupexpiredays 30
```

Dica: Emita o comando **DEFINE STGPOOL** e especifique o mesmo valor para o parâmetro **REUSEDELAY** em sua definição de conjunto de armazenamento de cópia para assegurar que ocorrerá o seguinte:

- O banco de dados pode ser retornado para um nível anterior
- As referências do banco de dados a arquivos no conjunto de armazenamento de cópias ainda são válidas

Se os conjuntos de armazenamento de cópia que são gerenciados pelo DRM tiverem diferentes valores **REUSEDELAY**, emita o comando **SET DRMDBBACKUPEXPIREDAYS** e configure o parâmetro **REUSEDELAY** para o valor mais alto.

2. Identifique todos os volumes na área segura externa que não contêm mais dados válidos e podem ser retornados para o local. Emita o seguinte comando **QUERY DRMEDIA** e especifique o parâmetro **WHERESTATE=VAULTRETRIEVE**.

```
query drmedia * wherestate=vaultretrieve
```

3. Para iniciar o processo de mover um conjunto de armazenamento de cópia, emita o seguinte comando:

```
move drmedia * wherestate=vaultretrieve
```

Restrição: Um volume do conjunto de armazenamentos de cópia pode ser movido no local se for EMPTY para pelo menos o número de dias especificados pelo parâmetro **REUSEDELAY** no comando **DEFINE STGPOOL**.

O servidor conclui as seguintes ações para todos os volumes no estado **VAULTRETRIEVE**:

- Muda o estado do volume para **COURIERRETRIEVE**
- Atualiza o local do volume de acordo com o que está especificado no comando **SET DRMCOURIERNAME**

Dica:

Também é possível especificar o destino dos volumes emitindo o comando **MOVE DRMEDIA** e especificando a configuração de parâmetro **TOSTATE**. Por exemplo, para mover volumes do estado **VAULTRETRIEVE** para o estado **ONSITERETRIEVE**, emita o comando a seguir:

```
move drmedia * wherestate=vaultretrieve tostate=onsiteretrieve
```

O servidor conclui as seguintes ações para todos os volumes no estado **VAULTRETRIEVE**:

- Move os volumes locais para onde eles possam ser reutilizados ou descartados
- Exclui os volumes de backup de banco de dados da tabela de históricos do volume
- Exclui o registro no banco de dados para volumes do conjunto de armazenamentos de cópia utilizáveis. Para volumes de conjunto de armazenamento de cópias privados, atualiza o acesso de leitura/gravação

4. Quando o transportador retornar os volumes no local, emita o seguinte comando:

```
move drmedia * wherestate=courierretrieve
```

O servidor conclui as seguintes ações para todos os volumes no estado **COURIERRETRIEVE**:

- Move os volumes locais para onde eles possam ser reutilizados ou descartados
- Exclui os volumes de backup de banco de dados da tabela de históricos do volume

- Exclui o registro no banco de dados para volumes do conjunto de armazenamentos de cópia utilizáveis. Para volumes de conjunto de armazenamento de cópias privados, atualiza o acesso de leitura/gravação

Movendo dados do conjunto de retenção para/de armazenamento em fita

É possível copiar dados do conjunto de retenção para volumes da fita, que podem ser movidos de uma biblioteca no local para uma área segura de armazenamento em fita externa. As áreas seguras são projetadas para fornecer armazenamento seguro de longo prazo. Depois que o conjunto de retenção é copiado para a fita e o volume da fita é removido da biblioteca de fitas, é possível rastrear o movimento do volume externo e no local.

Um volume de fita que contém dados para um ou mais conjuntos de retenção é chamado de *volume de retenção*.

À medida que o volume da fita é movido de um local para outro, o estado do volume muda para refletir o novo local e é possível usar essas informações para rastrear o local físico do volume.

O ciclo de vida de um volume de retenção consiste nos principais estágios a seguir:

1. Quando o processo para gravar um conjunto de retenção em um volume da fita se inicia, um volume utilizável é adquirido do conjunto inicial da biblioteca de fitas ou um volume existente é selecionado do conjunto de retenção. Os dados de um ou mais conjuntos de retenções são gravados no volume. Quando o volume estiver cheio, ele será levado pelo courier para uma área segura externa.
2. Se o volume contém dados que devem ser restaurados, o volume é recuperado da área segura e trazido de volta no local por courier. Depois que os dados no conjunto de retenção são restaurados, o volume é movido de volta para a área segura externa.
3. Com o tempo, os dados em conjuntos de retenção podem expirar, com base em políticas de expiração. Se as datas de expiração forem atingidas para todos os conjuntos de retenção que têm dados no volume, o volume poderá ser retornado no local para reutilização.

A figura a seguir mostra o ciclo de vida de uma operação típica para mover os volumes de retenção para um local externo e de volta no local.

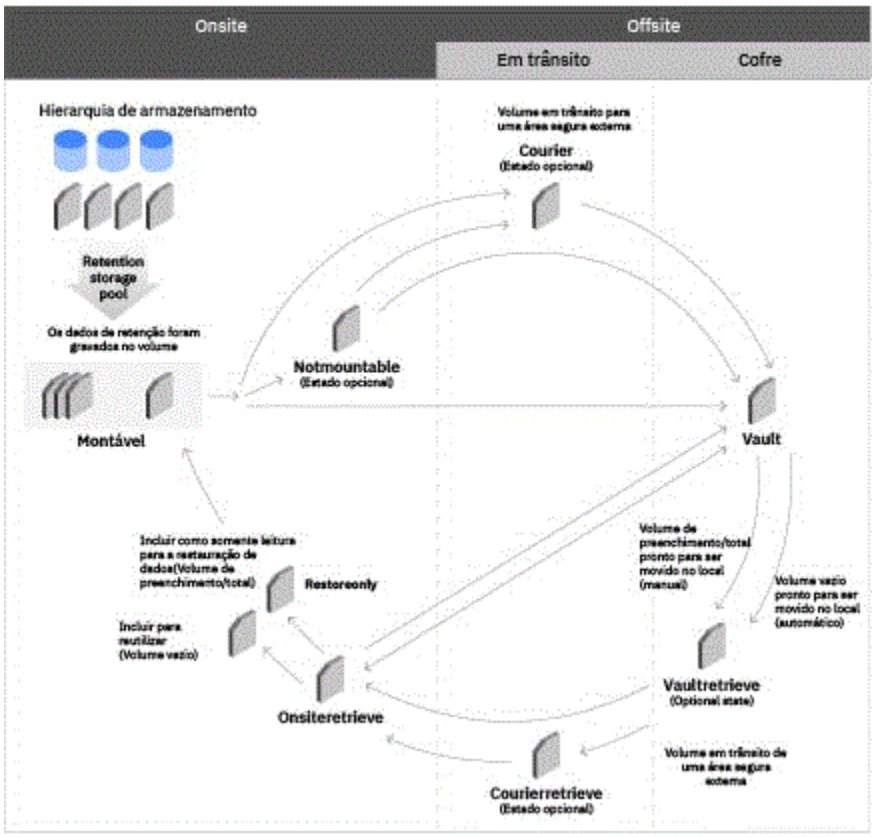


Figura 6. Movendo volumes de retenção para fora e de volta para o local

O estado de mídia do volume ajuda a identificar seu local atual à medida que ele é movido da biblioteca local para uma área segura externa e, em seguida, de volta ao local para a restauração de dados ou a reutilização de fita. O estado de mídia do volume é uma designação lógica relacionada à localização física do volume. Alguns estados de mídia são opcionais. Dependendo da precisão com a qual sua organização deseja rastrear os movimentos de um volume, será possível ignorar esses estados de mídia opcionais. Um dos estados de mídia a seguir é mostrado:

MOUNTABLE
O volume está no local e está incluído na biblioteca. Os dados de um ou mais conjuntos de retenções são gravados no volume.

NOTMOUNTABLE
O volume está no local, mas foi retirado da biblioteca e está pronto para ser enviado para fora.

COURIER
O volume está em trânsito para uma área segura externa.

VAULT
O volume está em uma área segura externa para armazenamento de longo prazo.

VAULTRETRIEVE
O volume está pronto para ser movido de volta para o local de uma área segura externa. Volumes vazios podem ser trazidos para o local e reutilizados. O servidor detecta que o volume contém apenas dados expirados e o coloca automaticamente no estado de mídia VAULTRETRIEVE. Os volumes de preenchimento ou totais também podem ser trazidos para o local para a restauração dos dados, mas deve-se especificar esta ação usando a configuração de parâmetro **TOSTATE** no comando **MOVE RETMEDIA**.

COURIERRETRIEVE
O volume está sendo movido de volta no local de uma área segura externa.

ONSITERETRIEVE
O volume foi recuperado da área segura externa e está de volta ao local. Volumes não vazios podem ser incluídos na biblioteca para a restauração dos dados do conjunto de retenção do volume. Volumes vazios podem ser incluídos e reutilizados.

RESTOREONLY
O volume tem check-in efetuado na biblioteca para ativar a restauração de dados do conjunto de retenções.

Movendo volumes de retenção para um local externo

É possível enviar volumes de retenção com dados de um ou mais conjuntos de retenção para um local externo. As áreas seguras externas são projetadas para fornecer armazenamento seguro para volumes da fita e ajudam a assegurar que os dados possam ser restaurados se necessário.

Antes de Iniciar

Dica: Se você não usar o comando **MOVE DRMEDIA** para mover os volumes de backup do banco de dados para fora e de volta para o local, também será possível usar o comando **MOVE RETMEDIA** para isso. Para obter informações adicionais, consulte "Movendo volumes do conjunto de armazenamentos de cópia externos" na página 62.

- Depois que o conjunto de retenção que você deseja enviar para um local externo for criado, faça backup dos volumes do banco de dados do servidor emitindo o comando **BACKUP DB**. Se você deseja assegurar que o volume de backup de banco de dados seja enviado para um local externo junto com o volume de retenção, deve-se especificar o parâmetro **SOURCE** no comando **MOVE RETMEDIA**.

  Restrição: Não é possível usar operações de movimentação de mídia no Operations Center para enviar um volume de backup de banco de dados para um local externo. Os volumes de backup de banco de dados são movidos usando o comando **MOVE RETMEDIA**.

  Para obter informações sobre como usar o Operations Center para mover os volumes de retenção, consulte a ajuda on-line do Operations Center.
- Certifique-se de que os conjuntos de retenção que você deseja copiar tenham o status Concluído. Esse status indica que os conjuntos de retenção foram copiados totalmente para a fita e que os volumes da fita podem ser movidos para uma área segura externa. Dessa forma, é possível evitar problemas decorrentes da execução concomitante das operações de movimentação de mídia e cópia de conjunto de retenção.

Procedimento

1. Identifique o conjunto de armazenamentos de retenção e os volumes de backup de banco de dados a serem movimentados, emitindo o comando **QUERY RETMEDIA**:

   ```
   query retmedia * wherestate=mountable
   ```

2. Inicie o movimento de volumes cujo estado atual é MOUNTABLE. Por padrão, todos os volumes não vazios serão incluídos se eles pertencerem a conjuntos de retenção que estão sendo copiados ou a conjuntos de retenção que são totalmente copiados. Emita o seguinte comando:

   ```
   move retmedia * wherestate=mountable
   ```

   a) Se você estiver usando uma biblioteca SCSI, durante o processamento de registro de saída, as bibliotecas SCSI solicitam a intervenção do operador. Ignore essas solicitações e ejete os cartuchos da biblioteca emitindo o seguinte comando:

   ```
   move retmedia * wherestate=mountable remove=no
   ```

   b) Obtenha uma lista dos volumes para identificar e remover da biblioteca emitindo o comando a seguir:

   ```
   query retmedia wherestate=notmountable
   ```

Para todos os volumes no estado MOUNTABLE, o comando **MOVE RETMEDIA** conclui as tarefas a seguir:

- Atualiza o estado de volume para NOTMOUNTABLE e, se você emitiu o comando **SET DRMNOTMOUNTABLENAME**, atualiza o local do volume. Se você não emitiu o comando **SET DRMNOTMOUNTABLENAME**, o local padrão será NOTMOUNTABLE.
- Atualiza o modo de acesso de volume para indisponível.
- Efetua check-out de volumes de bibliotecas automatizadas.

Dica: Dependendo do quanto minuciosamente sua organização deseja rastrear os movimentos de um volume, ela pode ignorar alguns estados de mídia. É possível evitar passar por todos os diferentes estados de mídia especificando o parâmetro **TOSTATE** no comando **MOVE RETMEDIA** para nomear o estado de destino. Por exemplo, para mudar os volumes diretamente do estado NOTMOUNTABLE para o estado VAULT, emita o comando a seguir:

```
move retmedia * wherestate=notmountable tostate=vault
```

3. Envie os volumes ao courier para trânsito para o local externo e emita o comando a seguir:

   ```
   move retmedia * wherestate=notmountable
   ```

   Para todos os volumes no estado NOTMOUNTABLE, o estado de volume é atualizado para o estado COURIER e o local do volume é atualizado de acordo com o comando **SET DRMCOURIERNAME**. Se você não emitiu o comando **SET DRMCOURIERNAME**, o local padrão será COURIER.
4. Acompanhe o movimento do volume da fita enquanto ele estiver em trânsito para uma área segura externa. Emita o seguinte comando:

   ```
   query retmedia * wherestate=courier
   ```

5. Quando o local da área segura confirmar o recebimento dos volumes, emita o comando **MOVE RETMEDIA** para especificar o estado COURIER:

   ```
   move retmedia * wherestate=courier
   ```

   Para todos os volumes no estado COURIER, o estado de volume é atualizado para VAULT e o local do volume é atualizado de acordo com o comando **SET DRMVAULTNAME**. Se você não emitiu o comando **SET DRMVAULTNAME**, o local padrão será VAULT.

   Para todos os volumes no estado NOTMOUNTABLE, o comando **MOVE RETMEDIA** atualiza o estado de volume para VAULT e o local do volume é atualizado de acordo com o comando **SET DRMVAULTNAME**. Se o comando **SET DRMVAULTNAME** ainda não tiver sido emitido, o local padrão será VAULT.

Resultados

Os volumes de retenção e quaisquer volumes de backup de banco de dados especificados são movidos para a área segura de fita externa. Se os dados do conjunto de retenção precisarem ser restaurados, os volumes poderão ser recuperados da área segura.

Movendo volumes de retenção no local

Caso um conjunto de retenção deva ser restaurado, será possível trazer os volumes da fita que contêm os dados do conjunto de retenção de volta no local para operações de restauração. Se as datas de expiração forem atingidas para todos os conjuntos de retenção que têm data dados sobre o volume de retenção, será possível trazer o volume nulo de volta no local para ser reutilizado.

Antes de Iniciar

Se você estiver retornando volumes vazios para a reutilização, confirme se todos os conjuntos de retenção com dados no volume atingiram as datas de expiração e se expiraram. É possível iniciar o processamento da expiração manualmente, emitindo o comando **EXPIRE INVENTORY**, ou usando o comando **DELETE RETSET** para marcar o conjunto de retenção para a exclusão.

Dica: Se você não usar o comando **MOVE DRMEDIA** para mover os volumes de backup do banco de dados para fora e de volta para o local, também será possível usar o comando **MOVE RETMEDIA** para isso. Para obter informações adicionais, consulte "Movendo volumes do conjunto de armazenamentos de cópia externos" na página 62.

Procedimento

Conclua as etapas a seguir para mover os volumes de retenção no local.

Tarefa	Procedimento

Mover um volume nulo no local para reutilização.	Para mover volumes de retenção nulos no local, conclua as etapas a seguir:
	a. Identifique os volumes de retenção na área segura externa que você deseja retornar no local. Para volumes nulos, o servidor detecta que o volume contém apenas dados expirados e coloca automaticamente o volume no estado de mídia VAULTRETRIEVE. Emita o seguinte comando:
	`query retmedia * wherestate=vaultretrieve volstatus=empty`
	b. Mova os volumes da fita no local. Especifique o destino dos volumes emitindo o comando **MOVE RETMEDIA** e especificando o parâmetro **TOSTATE**. Emita o seguinte comando:
	`move retmedia * wherestate=vaultretrieve volstatus=empty tostate=onsiteretrieve`
	Restrição: Um volume do conjunto de armazenamentos de retenção poderá ser movido no local se ele estiver no estado EMPTY por pelo menos o número de dias que são especificados pelo parâmetro **REUSEDELAY** no comando **DEFINE STGPOOL**.
	O servidor conclui as ações a seguir:
	• Muda o estado de volume para **ONSITERETRIEVE**
	• Exclui os volumes de backup de banco de dados da tabela de históricos do volume
	• Exclui o registro no banco de dados para volumes de retenção utilizáveis
	c. Verifique o volume nulo para a biblioteca de fitas e disponibilize para reutilização, emitindo o comando **CHECKIN LIBVOL** e especificando o volume como um volume utilizável.
	Dica: Para volumes de fita em bibliotecas SCSI, é possível diminuir o tempo de check-in especificando que o servidor lê a etiqueta de código de barras.
	Emita o seguinte comando:
	`checkin libvol libname search=bulk waittime=0 checklabel=barcode status=scratch`

Tarefa	Procedimento

Mova um volume não vazio no local para restauração de dados.	Para mover volumes de retenção no local para restauração de dados, conclua as etapas a seguir:
	a. Identifique os volumes que contêm os dados do conjunto de retenção que você deseja restaurar.
	• Para identificar os volumes que são usados por cada conjunto de retenção, emita o comando a seguir:
	`query retset listvolumes=yes`
	• Para identificar os conjuntos de retenção que têm dados em um volume de retenção, emita o comando a seguir:
	`query volume listretsets=yes`
	b. Localize o volume necessário em seu local externo emitindo o comando **QUERY RETMEDIA** e especificando o parâmetro **WHERESTATE**. Por exemplo, para visualizar todos os volumes que estão localizados na área segura externa, emita o comando a seguir:
	`query retmedia * wherestate=vault`
	c. Mova o volume necessário no local. Especifique o destino dos volumes emitindo o comando **MOVE RETMEDIA** e especificando o parâmetro **TOSTATE**. Por exemplo, para mover o volume VOL001 no local, emita o comando a seguir:
	`move retmedia VOL001 wherestate=vault tostate=onsiteretrieve`
	Importante: Se você retornar volumes no local para restaurar dados, mantenha o valor do limite de recuperação de conjunto de armazenamentos padrão. O valor padrão é 100. Dessa forma, quando você mover os volumes de retenção no local, emitindo o comando **MOVE RETMEDIA** e especificando o parâmetro **TOSTATE=ONSITERETRIEVE**, o processamento de recuperação de conjunto de armazenamentos não interferirá com a operação de movimentação.
	d. Verifique o volume para a biblioteca de fitas e disponibilize o volume para operações de restauração. Para assegurar que o volume possa ser usado apenas para restauração de dados, o seu modo de acesso é somente leitura. Para mover o volume do estado ONSITERETRIEVE para o estado RESTOREONLY, emita o comando **CHECKIN LIBVOL**. Emita o seguinte comando:
	`checkin libvol libname search=bulk waittime=0 checklabel=barcode status=private`
	Dica: Para volumes de fita em bibliotecas SCSI, é possível diminuir o tempo de check-in especificando que o servidor lê a etiqueta de código de barras.
	O volume é incluído em uma biblioteca automatizada e o estado de mídia dele muda para RESTOREONLY.

Resultados

Os volumes de retenção selecionados são retornados ao local e incluídos na biblioteca de fitas. Os volumes de fita vazios retornam ao status inicial e são disponibilizados para a reutilização. Volumes não vazios estão no estado RESTOREONLY e podem ser usados para restaurar os dados.

O que Fazer Depois
Após a conclusão da restauração de dados, é possível enviar os volumes de fita novamente para a área segura externa. Emita o seguinte comando:

```
move retmedia * wherestate=restoreonly tostate=vault
```

Mensagens de alerta para monitorar o movimento de volumes de retenção
Se você envia volumes de retenção para um local externo ou de volta no local, o servidor IBM Spectrum Protect gera alertas na forma de mensagens ANR para relatar quaisquer problemas e para ajudar a monitorar o status.

Para visualizar todas as mensagens, consulte o log de erro do IBM Spectrum Protect. Para obter a documentação detalhada sobre mensagens, consulte Mensagens ANR. As mensagens comumente emitidas são descritas na tabela a seguir:

Tabela 16. Enviando volumes da fita de retenção para uma área segura externa

Ação	Mensagem ANR	descrição
O conjunto de retenção é copiado para o volume da fita.	ANR3852I	Essa mensagem de informação indica que o conjunto de retenção foi copiado com sucesso para o volume da fita. Os detalhes da operação de cópia são fornecidos. O estado do conjunto de retenção é COMPLETED.
Os volumes da fita tiveram o check-out efetuado de uma biblioteca de fitas.	ANR6697I	Essa mensagem de informação indica que os volumes da fita em um estado MOUNTABLE tiverem o check-out efetuado com sucesso de uma biblioteca de fitas.
O volume da fita teve o check-out efetuado da biblioteca e movido de um estado MOUNTABLE para um estado VAULT.	ANR6683I	Essa mensagem de informação indica que os dados de retenção foram movidos com sucesso e o estado foi mudado.

Tabela 17. Efetuando o registro de entrada de volumes da fita para a biblioteca de fitas para serem usados em operações de restauração

Ação	Mensagem ANR	descrição
Um volume de retenção que contém dados teve o check-in efetuado na biblioteca de fitas no local com sucesso.	ANR8532I	Essa mensagem de informação indica que um volume com dados teve o check-in efetuado com sucesso na biblioteca de fitas no local. Para volumes de retenção, o estado de mídia do volume muda de ONSITERETRIEVE para RESTOREONLY e seu modo de acesso é somente leitura. Os dados do conjunto de retenção no volume agora podem ser restaurados. **Dica:** Essa mensagem não aparecerá se o volume da fita que está tendo o check-in efetuado estiver vazio.

Tabela 17. Efetuando o registro de entrada de volumes da fita para a biblioteca de fitas para serem usados em operações de restauração (continuação)

Ação	Mensagem ANR	descrição
Você está tentando efetuar check-in de um volume de retenção não vazio como um volume utilizável na biblioteca de fitas.	ANR8443E	Essa mensagem de erro é acionada porque um volume de retenção que contém dados não pode ter o check-in efetuado em uma biblioteca de fitas e ser designado a um status de SCRATCH. O volume não tem o check-in efetuado e os dados na fita não são sobrescritos.

Tabela 18. Efetuando o registro de entrada em volumes de retenção expirados para uma biblioteca de fitas

Ação	Mensagem ANR	descrição
Um volume de retenção vazio teve o check-in efetuado em uma biblioteca de fitas no local.	ANR8430I	Essa mensagem de informação indica que um volume vazio teve o check-in efetuado com sucesso em uma biblioteca de fitas no local. O volume é retornado ao status inicial.
Uma tentativa de efetuar check-in de um volume de retenção vazio em uma biblioteca de fitas no local falhou.	ANR8832E	Essa mensagem de erro indica que uma operação para efetuar o registro de entrada de um volume de retenção vazio em uma biblioteca de fitas no local falhou.

Definindo planejamentos de cliente

Use o Operations Center para criar planejamentos para operações do cliente.

Procedimento

1. Na barra de menus do Operations Center, passe o mouse sobre **Clientes**.
2. Clique em **Planejamentos**.
3. Clique em **+Schedule**.
4. Conclua as etapas no assistente **Criar planejamento**.

   Configure planejamentos de backup de cliente para iniciar às 22h, com base nas atividades de manutenção de servidor planejadas em “Definindo planejamentos para atividades de manutenção de servidor” na página 56.

Conectando dispositivos de fita para o servidor

Antes que o servidor possa usar um dispositivo de fita, deve-se conectar o dispositivo ao seu sistema do servidor e instalar o driver de dispositivo de fita apropriado.

Sobre Esta Tarefa

Para otimizar o desempenho do sistema, use dispositivos de fita rápidos, de alta capacidade. Forneça unidades de fita suficientes para atender às suas necessidades de negócios.

Conecte os dispositivos de fita em seus próprios adaptadores de barramento de host (HBA), não compartilhados com outros tipos de dispositivos, como disco. As unidades de fita IBM possuem alguns requisitos especiais para HBAs e drivers associados.

Conectando um dispositivo de biblioteca automatizada ao seu sistema

É possível conectar um dispositivo de biblioteca automatizada no seu sistema para armazenar seus dados em fitas.

Sobre Esta Tarefa

Antes de conectar um dispositivo de biblioteca automatizada, considere as seguintes restrições:

- Os dispositivos conectados devem estar em seus próprios Adaptadores de Barramento de Host (HBA).
- Um HBA não deve ser compartilhado com outros tipos de dispositivo, como um disco.
- Para HBAs Fibre Channel de múltiplas portas, os dispositivos devem ser conectados à sua própria porta. Essas portas não devem ser compartilhadas com outros tipos de dispositivo.
- As unidades de fita IBM têm alguns requisitos especiais sobre o HBA e drivers associados. Para obter mais informações sobre os dispositivos, consulte o website do seu sistema operacional:
  - IBM Spectrum Protect Dispositivos suportados para AIX
  - IBM Spectrum Protect Dispositivos suportados para Linux e Windows

Procedimento

Para usar o adaptador Fibre Channel (FC), conclua as seguintes etapas:

1. Instale o adaptador FC e os drivers associados.
2. Instale os drivers de dispositivo apropriados para dispositivos alteradores de mídia conectados.

Conceitos relacionados

Selecionando um driver de dispositivo de fita
Para usar dispositivos de fita com o IBM Spectrum Protect, deve-se instalar o driver de dispositivo de fita apropriado.

Configurando o modo de biblioteca

Para o servidor do IBM Spectrum Protect acessar uma biblioteca SCSI, o dispositivo de fita deverá ser configurado para o modo apropriado.

Sobre Esta Tarefa

Algumas bibliotecas possuem menus e visores no painel frontal que podem ser utilizados para solicitações expressas do operador. No entanto, se você configurar o dispositivo de fita para responder a essas solicitações, o dispositivo geralmente não responderá às solicitações do IBM Spectrum Protect.

Algumas bibliotecas podem ser colocadas no modo SEQUENCIAL, em que os volumes são montados automaticamente em unidades usando uma abordagem sequencial. Este modo entra em conflito com a maneira como o IBM Spectrum Protect acessa o dispositivo de fita. Uma biblioteca que é configurada no modo SEQUENTIAL não é detectada pelo driver de dispositivo do sistema como um alterador de mídia de biblioteca, um driver de dispositivo de fita IBM e um driver de dispositivo de fita IBM Spectrum Protect.

Procedimento

1. Consulte a documentação para seu dispositivo de fita para determinar como configurar o modo de biblioteca.
2. Configure o modo apropriado para seu dispositivo de fita. Para a maioria dos dispositivos de fita, o modo apropriado é chamado de modo RANDOM. Se o seu dispositivo de fita não tiver um modo RANDOM, consulte a documentação do seu dispositivo para identificar o modo apropriado.

Selecionando um driver de dispositivo de fita

Para usar dispositivos de fita com o IBM Spectrum Protect, deve-se instalar o driver de dispositivo de fita apropriado.

Referências relacionadas

Instalando e configurando drivers de dispositivo de fita
Antes de poder usar dispositivos de fita com o IBM Spectrum Protect, deve-se instalar o driver de dispositivo de fita correto.

Drivers de dispositivo de fita do IBM

Os drivers de dispositivo de fita IBM estão disponíveis para a maioria dos dispositivos de fita rotulados da IBM.

É possível fazer download dos drivers de dispositivo de fita IBM por meio do website Fix Central:

1. Acesse o website Fix Central: Website do Fix Central.
2. Clique em **Selecionar produto**.
3. Selecione **Armazenamento do sistema** para o menu **Grupo de produtos**.
4. Selecione **Sistemas de fita** para o menu **Armazenamento do sistema**.
5. Selecione **Drivers e software de fita** para o menu **Sistemas de fita**.
6. Selecione **Drivers de dispositivo de fita** para o menu **Drivers e software de fita**. Além dos drivers de fita, você também obtém acesso a ferramentas, como o IBM Tape Diagnostic Tool (ITDT).
7. Selecione seu sistema operacional para o menu **Plataforma**.

AIX Windows

Para obter a lista mais atualizada de dispositivos e níveis de sistemas operacionais que são suportados pelos drivers de dispositivos de fita IBM, consulte o website de Dispositivos suportados do IBM Spectrum Protect no Dispositivos Suportados para AIX e Windows .

Linux

Para obter a lista mais atualizada de dispositivos de fita e os níveis do sistema operacional que são suportados pelos drivers de dispositivo de fita IBM, consulte o website Dispositivos suportados do IBM Spectrum Protect no Dispositivos Suportados para Linux .

Os drivers de dispositivo de fita IBM suportam apenas alguns níveis de kernel do Linux. Para obter informações sobre níveis de kernel suportados, consulte o Website do Fix Central.

Drivers de dispositivo de fita do IBM Spectrum Protect

O servidor do IBM Spectrum Protect fornece drivers de dispositivo de fita.

Um driver de dispositivo de fita do IBM Spectrum Protect é instalado com o servidor.

AIX

É possível utilizar o driver de dispositivo de fita SCSI genérico que é fornecido pelo sistema operacional IBM AIX para trabalhar com dispositivos de fita que não forem suportados pelo driver de dispositivo do IBM Spectrum Protect. Se o driver de dispositivo de fita SCSI genérico do AIX for usado, a classe de dispositivo GENERICTAPE deverá ser configurada para o tipo de dispositivo que estiver especificado no comando **`DEFINE DEVCLASS`**.

Para os seguintes dispositivos de fita, é possível escolher se instalar o driver de dispositivo de fita do IBM Spectrum Protect ou o driver de dispositivo nativo para seu sistema operacional:

ECART
LTO (não da IBM)

Todas as bibliotecas conectadas ao SCSI que contiverem unidades de fita da lista devem usar o driver de alterador de mídia do IBM Spectrum Protect.

Os drivers de dispositivo de fita adquiridos de outros fornecedores de hardware podem ser usados se estiverem associados à classe de dispositivo GENERICTAPE. Drivers de dispositivo genéricos não são suportados em classes de dispositivos write-one, read-many (WORM).

Linux

É possível usar o driver de dispositivo Intermediário do IBM Spectrum Protect. IBM Spectrum Protect Os drivers de dispositivo intermediários requerem o driver de dispositivo SCSI genérico (sg) do Linux junto com o sistema operacional Linux para instalar os kernels.

Por exemplo, é possível instalar o driver de dispositivo Intermediário do IBM Spectrum Protect para os seguintes dispositivos de fita:

ECART
LTO (não da IBM)

Todas as bibliotecas conectadas por SCSI que contêm unidades de fita que não são rotuladas pela IBM na lista também devem usar o driver de dispositivo Intermediário do IBM Spectrum Protect.

Não é possível usar o driver de dispositivo de fita SCSI genérico (st) que é fornecido pelo sistema operacional Linux. Portanto, o tipo de dispositivo GENERICTAPE não é suportado para o comando **DEFINE DEVCLASS**.

Windows É possível selecionar um driver de dispositivo nativo certificado do Windows Hardware Qualification Lab em vez do driver de dispositivo do IBM Spectrum Protect. O driver de dispositivo nativo certificado pelo Windows Hardware Qualification Lab pode ser usado somente para dispositivos que têm um rótulo não IBM e para unidades de fita não IBM. Para o driver de dispositivo nativo certificado pelo Windows Hardware Qualification Lab, é possível selecionar o driver de dispositivo intermediário SCSI do IBM Spectrum Protect ou o driver de dispositivo de fita nativo do Windows. Se o driver de dispositivo intermediário SCSI for usado, a classe de dispositivo no comando **DEFINE DEVCLASS** não poderá ser GENERICTAPE. Se o driver de dispositivo nativo for usado, a classe de dispositivo deve ser GENERICTAPE.

Nomes de arquivos especiais para dispositivos de fita

Um nome de arquivo especial para um dispositivo de fita é necessário para que o servidor trabalhe com fita, alterador de mídia ou dispositivos de mídia removíveis.

AIX

Quando um dispositivo é configurado com sucesso, um nome de arquivo lógico é retornado. O Tabela 19 na página 75 especifica o nome do dispositivo, também chamado de nome do arquivo especial, que corresponde à unidade ou biblioteca. É possível usar o comando do sistema operacional **SMIT** para obter o nome do arquivo especial do dispositivo. Nos exemplos, *x* especifica um número inteiro, 0 ou superior.

Tabela 19. Exemplos de dispositivo

Dispositivo	Exemplo de dispositivo	Nome do arquivo lógico
Unidades de fita que podem ser usadas pelo driver de dispositivo do IBM Spectrum Protect	/dev/mt*x*	mt*x*
Unidades de fita que podem ser usadas pelo driver de dispositivo de fita do IBM	/dev/rmt*x*	rmt*x*
Unidades de fita que podem ser usadas pelo driver de dispositivo de fita genérico do IBM AIX	/dev/rmt*x*	rmt*x*
Dispositivos de biblioteca que podem ser usados pelo driver de dispositivo do IBM Spectrum Protect	/dev/lb*x*	lb*x*
Dispositivos de biblioteca que podem ser usados pelo driver de dispositivo de fita do IBM	/dev/smc*x*	smc*x*

Linux

Quando um dispositivo é configurado com sucesso, um nome de arquivo lógico é retornado. O Tabela 20 na página 76 especifica o nome do dispositivo, também chamado de nome do arquivo especial, que corresponde à unidade ou à biblioteca. Nos exemplos, *x* especifica um número inteiro, 0 ou superior.

Tabela 20. Exemplos de dispositivo

Dispositivo	Exemplo de dispositivo	Nome do arquivo lógico
Unidades de fita que podem ser usadas pelo driver de dispositivo intermediário do IBM Spectrum Protect	`/dev/tsmscsi/mtx`	`mtx`
Unidades de fita que podem ser usadas pelo driver de dispositivo lin_tape do IBM	`/dev/IBMtapex`	`IBMtapex`
Dispositivos de biblioteca que podem ser usados pelo driver de dispositivo intermediário do IBM Spectrum Protect	`/dev/tsmscsi/lbx`	`lbx`
Dispositivos de biblioteca que podem ser usados pelo driver de dispositivo lin_tape do IBM	`/dev/IBMchangerx`	`IBMchangerx`

Windows

Quando um dispositivo é configurado com sucesso, um nome de arquivo lógico é retornado. O Tabela 21 na página 76 especifica o nome do dispositivo, também chamado de nome do arquivo especial, que corresponde à unidade ou à biblioteca. Nos exemplos, *a*, *b*, *c*, *d* e *x* especificam um número inteiro, 0 ou superior, em que:

- *a* especifica o ID de destino.
- *b* especifica o LUN.
- *c* especifica o ID de barramento SCSI.
- *d* especifica o ID da porta.

Tabela 21. Exemplos de dispositivo

Dispositivo	Exemplo de dispositivo	Nome do dispositivo convertido
Unidades de fita que são suportadas pelo driver de dispositivo do IBM Spectrum Protect	mt*a.b.c.d*	mt*a.b.c.d*
Unidades de fita que são suportadas pelo driver de dispositivo intermediário do IBM Spectrum Protect	mt*a.b.c.d*	mt*a.b.c.d*
Unidades de fita que são suportadas pelo driver de dispositivo do IBM	Tape*x*	mt*a.b.c.d*
Dispositivos de biblioteca que são suportados pelo driver de dispositivo do IBM Spectrum Protect	lb*.a.b.c.d*	lb*a.b.c.d*
Dispositivos de biblioteca que são suportados pelo driver de dispositivo intermediário do IBM Spectrum Protect	lb*a.b.c.d*	lb*a.b.c.d*
Dispositivos de biblioteca que são suportados pelo driver de dispositivo do IBM	Changer*x*	lb*a.b.c.d*

Instalando e configurando drivers de dispositivo de fita

Antes de poder usar dispositivos de fita com o IBM Spectrum Protect, deve-se instalar o driver de dispositivo de fita correto.

O IBM Spectrum Protect suporta todos os dispositivos que forem suportados pelos drivers de dispositivo de fita IBM. No entanto, o IBM Spectrum Protect não suporta todos os níveis do sistema operacional que forem suportados pelos drivers de dispositivo de fita IBM.

Instalando e configurando os drivers de dispositivo IBM para dispositivos de fita IBM

Instale e configure um driver de dispositivo de fita IBM para usar um dispositivo de fita IBM.

Sobre Esta Tarefa

Para obter instruções sobre como instalar e configurar drivers de dispositivo de fita do IBM, consulte o IBM Tape Device Drivers: Guia de Instalação e do Usuário.

AIX Depois de concluir o procedimento de instalação no *IBM Tape Device Drivers Installation and User's Guide*, são emitidas mensagens diferentes, dependendo do driver de dispositivo que está sendo instalado. Se estiver instalando o driver de dispositivo para uma unidade de fita ou biblioteca IBM, as mensagens a seguir serão retornadas:

```
rmtx Disponível
```

ou

```
smcx Available
```

Observe o valor de *x*, que é designado pelo driver de dispositivo de fita IBM. Para determinar o nome do arquivo especial de seu dispositivo, emita um dos seguintes comandos:

- Para unidades de fita, `ls -l /dev/rmt*`
- Para bibliotecas de fitas, `ls -l /dev/smc*`

O nome do arquivo pode ter mais caracteres no final para indicar características operacionais diferentes, mas esses caracteres não são necessários para o IBM Spectrum Protect. Para drivers de dispositivo IBM, use o nome do arquivo base no parâmetro **DEVICE** do comando **DEFINE PATH** para designar um dispositivo para uma unidade (`/dev/rmtx`) ou uma biblioteca (`/dev/smcx`).

Depois de instalar o driver de dispositivo, é possível usar o System Management Interface Tool (SMIT) para configurar unidades de fita e bibliotecas de fitas não IBM. Execute as etapas a seguir:

1. Execute o programa SMIT.
2. Clique em **Dispositivos**.
3. Clique em **Dispositivos IBM Spectrum Protect**.
4. Clique em **Dispositivos conectados por SAN Fibre Channel**.
5. Clique em **Descobrir dispositivos suportados pelo IBM Spectrum Protect**. Espere a conclusão do processo de descoberta.
6. Volte para o menu **Dispositivos conectados por SAN Fibre Channel** e clique em **Listar atributos de um dispositivo descoberto**.

Linux Depois de concluir o procedimento de instalação no *IBM Tape Device Drivers Installation and User's Guide*, são emitidas mensagens diferentes, dependendo do driver de dispositivo que está sendo instalado. Se estiver instalando o driver de dispositivo para um dispositivo IBM LTO ou 3592 , as seguintes mensagens serão retornadas:

```
IBMtapex Available
```

ou

```
IBMChangerx Available
```

Observe o valor de *x*, que é designado pelo driver de dispositivo de fita IBM. Para determinar o nome do arquivo especial de seu dispositivo, emita um dos seguintes comandos:

- Para unidades de fita, `ls -l /dev/IBMtape*`

- Para bibliotecas de fitas, `ls -l /dev/IBMChange*`

O nome do arquivo pode ter mais caracteres no final para indicar características operacionais diferentes, mas esses caracteres não são necessários para o IBM Spectrum Protect. Para drivers de dispositivo IBM, use o nome do arquivo base no parâmetro **DEVICE** do comando **DEFINE PATH** para designar um dispositivo para uma unidade (`/dev/IBMtapex`) ou uma biblioteca (`/dev/IBMChangerx`).

Restrição: O tipo de dispositivo dessa classe não deve ser **GENERICTAPE**.

Windows Para sistemas operacionais Windows, o IBM Spectrum Protect fornece dois drivers de dispositivo:

Driver de dispositivo intermediário
Se o fabricante do dispositivo de fita fornecer um driver de dispositivo SCSI, instale o driver de dispositivo intermediário do IBM Spectrum Protect.

Driver de dispositivo SCSI para dispositivos de fita
Se o fabricante do dispositivo de fita não fornecer um driver de dispositivo SCSI, instale o driver de dispositivo SCSI do IBM Spectrum Protect para dispositivos de fita. O nome do arquivo do driver é `tsmscsi64.sys`.

Para obter instruções sobre como instalar e configurar drivers de dispositivo de fita IBM, consulte o *IBM Tape Device Drivers Installation and User's Guide*. Depois de instalar o driver de dispositivo de fita IBM, o servidor especifica um nome do arquivo especial, `Tape`*X*, para unidades de fita IBM ou `Changer`*Y*, para alteradores de mídia IBM. Para um driver de dispositivo SCSI do IBM Spectrum Protect ou um driver de dispositivo intermediário do IBM Spectrum Protect, é possível emitir o comando do sistema operacional Windows, **regedit**, para verificar o nome do arquivo especial e o driver de dispositivo. O servidor IBM Spectrum Protect também fornece um utilitário para verificar o dispositivo para o sistema operacional Windows. O utilitário, **tsmdlst**, é fornecido com o pacote do servidor. Para usar o utilitário, conclua as seguintes etapas:

1. Certifique-se de que a interface de programação de aplicativos (API) do adaptador de barramento de host esteja instalada.
2. Para obter informações sobre o dispositivo do sistema host, digite:

```
tsmdlst
```

Conceitos relacionados

Acesso de E/S de caminhos múltiplos com dispositivos de fita IBM
E/S de caminhos múltiplos é uma técnica que usa caminhos diferentes para acessar o mesmo dispositivo físico, por exemplo, por meio de diversos adaptadores de barramento de host (HBA) ou comutadores. O uso da técnica de caminhos múltiplos ajuda a assegurar que um ponto único de falha não ocorra.

Acesso de E/S de caminhos múltiplos com dispositivos de fita IBM

E/S de caminhos múltiplos é uma técnica que usa caminhos diferentes para acessar o mesmo dispositivo físico, por exemplo, por meio de diversos adaptadores de barramento de host (HBA) ou comutadores. O uso da técnica de caminhos múltiplos ajuda a assegurar que um ponto único de falha não ocorra.

O driver de dispositivo de fita IBM fornece suporte de caminhos múltiplos para que se um caminho falhar, o servidor pode usar um caminho diferente para acessar dados em um dispositivo de armazenamento. A falha e a transição para um caminho diferente não são detectadas pelo servidor em execução ou por um agente de armazenamento. O driver de dispositivo de fita IBM também usa E/S de caminhos múltiplos para fornecer balanceamento de carga dinâmico para desempenho de E/S aprimorado.

Para fornecer caminhos redundantes para dispositivos de fita IBM, conecte cada dispositivo a duas ou mais portas em um Adaptador de Barramento de Host Fibre Channel ou SAS multiporta (se estiver disponível em seu sistema operacional), ou a diferentes Adaptadores de Barramento de Host de Fibre Channel únicos. Se a E/S de caminhos múltiplos estiver ativada e um erro permanente ocorrer em um caminho, como um HBA ou cabo com mau funcionamento, drivers de dispositivo fornecerão failover de caminho automático para um caminho alternativo.

Após a ativação da E/S de caminhos múltiplos, o driver de dispositivo de fita IBM detecta todos os caminhos para um dispositivo no sistema host. Um caminho é designado como o caminho primário. Os

caminhos restantes são caminhos alternativos. O número máximo de caminhos alternativos para um dispositivo é 16. Para cada caminho, o driver de dispositivo de fita IBM cria um arquivo especial com um nome exclusivo. Um caminho deve existir no sistema antes que o driver possa criar um arquivo especial para o caminho. Se um caminho não existir, o driver não criará um arquivo especial. Ao usar o comando **DEFINE PATH** para especificar o caminho para um destino, especifique o arquivo que está associado ao caminho primário como o valor do parâmetro **DEVICE**.

AIX

No AIX, a E/S de caminhos múltiplos não é ativada automaticamente quando o driver de dispositivo de fita IBM é instalado. Deve-se configurá-la para cada dispositivo lógico após a instalação. A E/S de caminhos múltiplos permanece ativada até que o dispositivo seja excluído ou o suporte seja desconfigurado. Para obter instruções de configuração, consulte o *IBM Tape Device Drivers Installation and User's Guide*.

Para obter os nomes de arquivos especiais, use o comando **ls -l**, por exemplo, **ls -l /dev/rmt***. Os caminhos primários e caminhos alternativos são identificados por **PRI** e **ALT**, conforme visto no exemplo a seguir:

```
rmt0 Available 20-60-01-PRI IBM 3590 Tape Drive and Medium Changer (FCP)
rmt1 Available 30-68-01-ALT IBM 3590 Tape Drive and Medium Changer (FCP)
```

Nesse exemplo, os seguintes caminhos estão associados à unidade de fita IBM 3590:

- 20-60-01-PRI
- 30-68-01-ALT

O nome do arquivo especial associado ao caminho primário é /dev/rmt0. Especifique /dev/rmt0 como o valor do parâmetro **DEVICE** no comando **DEFINE PATH**.

Para exibir detalhes relacionados ao caminho sobre uma unidade de fita específica, também é possível utilizar o comando **itdt -f /dev/rmtx path**, em que *x* é o número da unidade de fita configurada. Para exibir detalhes relacionados ao caminho sobre um alterador de mídia específico, use o comando **itdt -f /dev/smcy path**, em que *y* é o número do alterador de mídia configurado.

Linux

No Linux, a E/S de caminhos múltiplos para alteradores de mídia e unidades de fita não é ativada automaticamente quando o driver de dispositivo é instalado. Para obter instruções sobre como configurar a E/S de caminhos múltiplos, consulte o *IBM Tape Device Drivers Installation and User's Guide*.

Quando uma E/S de caminhos múltiplos é ativada para um dispositivo lógico, ela permanece ativada até que o dispositivo seja excluído ou o suporte seja desconfigurado.

Para exibir os nomes do arquivo especial para unidades de fita e alteradores de mídia IBM, use o **ls -l /dev/IBMx**, em que *x* é o número do índice do dispositivo. Também é possível inserir o comando **cat /proc/scsi/IBMtape** para unidades de fita. Conforme mostrado no arquivo IBMtape, os caminhos primários e caminhos alternativos são identificados como Primários ou Alternativos:

```
Number     Model       SN              HBA             FO Path
 0         03592       IBM1234567      qla2xxx         Primary
 1         03592       IBM1234567      qla2xxx         Alternate
```

O nome do arquivo especial associado ao caminho primário para esta unidade de fita é /dev/IBMtape0. Especifique /dev/IBMTape0 como o valor do parâmetro **DEVICE** no comando **DEFINE PATH** para esse dispositivo.

Para obter os nomes dos arquivos especiais associados aos caminhos primários para todos os alteradores de mídia configurados no sistema, emita o comando **cat /proc/scsi/IBMchanger**. O exemplo a seguir é obtido a partir do arquivo IBMchanger:

```
Number     Model          SN              HBA           FO Path
 3         03584L22       IBM1002345      qla2xxx       Primary
 4         03584L22       IBM1002345      qla2xxx       Alternate
```

O nome do arquivo especial associado ao caminho primário para esse alterador de mídia é /dev/IBMchanger3. Especifique /dev/IBMchanger3 como o valor do parâmetro **DEVICE** no comando **DEFINE PATH** para esse dispositivo.

Para exibir detalhes relacionados ao caminho sobre uma unidade de fita específica no sistema, use o comando **itdt -f /dev/IBMtapex path**, em que *x* é o número de um dispositivo de fita configurado. Para exibir detalhes relacionados ao caminho sobre um alterador de mídia específico no sistema, use o comando **itdt -f /dev/IBMchangerx path**, em que *x* é o número de um alterador de mídia configurado.

Windows No Windows, a E/S de caminhos múltiplos para alteradores de mídia e unidades de fita não é ativada automaticamente quando o driver de dispositivo é instalado. Para obter instruções sobre como configurar a E/S de caminhos múltiplos, consulte o *IBM Tape Device Drivers Installation and User's Guide*. Se a E/S de caminhos múltiplos estiver configurada, um dispositivo terá dois nomes de dispositivo correspondentes com locais diferentes. Para obter informações detalhadas sobre o caminho primário e o caminho alternativo, execute o IBM Tape Diagnostic Tool com a função **qrypath**. A saída é semelhante ao seguinte exemplo:

```
C:\Users\Administrator\Downloads\ITDT> .\itdt.exe qrypath -f \\.\Tape0
Querying SCSI paths...
Total paths configured.......... 2

Caminho Alternativo
Logical Device................. Tape0
Serial Number.................. 0000078F7612
SCSI Host ID................... 8
SCSI Channel................... 0
Target ID...................... 3
Logical Unit................... 0
Path Enabled................... Sim

Caminho Primário
Logical Device................. Tape0
Serial Number.................. 0000078F7612
SCSI Host ID................... 8
SCSI Channel................... 0
Target ID...................... 1
Logical Unit................... 0
Path Enabled................... Sim


Exit with code: 0
```

AIX Configurando drivers de dispositivo de fita em sistemas AIX

Revise as instruções para instalar e configurar drivers de dispositivo de fita não IBM em sistemas AIX.

Sobre Esta Tarefa

Para obter instruções sobre como instalar e configurar drivers de dispositivo de fita IBM, consulte o *IBM Tape Device Drivers Installation and User's Guide*.

AIX Dispositivos SCSI e Fibre Channel

Os menus e prompts de definição de dispositivo do IBM Spectrum Protect no SMIT permitem o gerenciamento de dispositivos conectados ao SCSI e ao Fibre Channel (FC).

O menu principal do IBM Spectrum Protect tem duas opções:

Dispositivos conectados ao SCSI
Utilize esta opção para configurar dispositivos SCSI que estão conectados a um adaptador SCSI no host.

Dispositivos conectados à rede de área do sistema (SAN) do Fibre Channel

Use essa opção para configurar dispositivos que estiverem conectados a um adaptador FC no host. Escolha um dos seguintes atributos:

Listar os atributos de um dispositivo descoberto

Lista atributos de um dispositivo que é conhecido para o banco de dados ODM atual.

- ID da Porta FC:

  O ID(N(L)_Port ou F(L)_Port) da porta FC de 24 bits. Este é o identificador de endereço que é exclusivo dentro da topologia associada na qual o dispositivo está conectado. Em ambientes comutadores ou de malha, ele pode ser determinado pelo comutador, com o máximo 2 bytes, que são diferentes de zero. Em um Loop arbitrado privado, é o Endereço físico de loop arbitrado (AL_PA), com o máximo de 2 bytes sendo zero. Consulte seus fornecedores FC para descobrir como um AL_PA ou um ID da porta é designado.

- ID do LUN mapeado:

  uma caixa de ponte de FC para SCSI, também chamada de conversor, roteador ou gateway. Consulte seus fornecedores de ponte sobre como as LUNs são mapeadas. Não se deve mudar IDs de LUN mapeados.

- Nome do WW:

  O nome mundial da porta à qual o dispositivo é conectado. É o identificador exclusivo de 64 bits que é designado pelos fornecedores de componentes FC, como pontes ou dispositivos FC nativos. Consulte seus fornecedores FC para descobrir o WWN de uma porta.

- ID do Produto:

  o ID do produto de um dispositivo. Consulte seus fornecedores de dispositivo para determinar o ID do produto.

Descobrir os dispositivos suportados pelo IBM Spectrum Protect

Essa opção descobre dispositivos em um SAN FC que são suportados pelo IBM Spectrum Protect e os tornam disponíveis. Se um dispositivo for incluído ou removido de um ambiente SAN existente, redescubra os dispositivos selecionando essa opção. Os dispositivos devem ser descobertos primeiro para que os valores atuais dos atributos de dispositivo sejam mostrados na opção `Atributos de lista de um dispositivo descoberto`. Dispositivos suportados em SAN FC são unidades de fita e alteradores de mídia. O driver de dispositivo IBM Spectrum Protect ignora todos os outros tipos de dispositivo, como disco.

Remova todos os dispositivos definidos

Essa opção remove todos os dispositivos IBM Spectrum Protect conectados ao SAN do FC cujo estado é `DEFINED` no banco de dados ODM. Se necessário, redescubra os dispositivos selecionando a opção `Discover Devices Supported by IBM Spectrum Protect` após a remoção de todos os dispositivos definidos.

Remover um dispositivo

Esta opção remove um único dispositivo IBM Spectrum Protect conectado ao SAN do FC cujo estado é `DEFINED` no banco de dados ODM. Se necessário, redescubra o dispositivo selecionando a opção `Discover Devices Supported by IBM Spectrum Protect` após a remoção de um dispositivo definido.

AIX Configurando drivers de dispositivo IBM Spectrum Protect para alteradores de mídia

Use o procedimento a seguir para configurar os drivers de dispositivo do IBM Spectrum Protect para alteradores de mídia para bibliotecas não IBM.

Procedimento

Execute o programa SMIT para configurar o driver de dispositivo para cada autochanger ou robô:

1. Selecione **Dispositivos**.
2. Selecione **IBM Spectrum ProtectDevices**.
3. Selecione **Library/MediumChanger (Biblioteca/MediumChanger)**.

4. Selecione **Add a Library/MediumChanger**.
5. Selecione o IBM Spectrum Protect-SCSI-LB para qualquer biblioteca suportada do IBM Spectrum Protect.
6. Selecione a placa principal à qual o dispositivo está sendo conectado. Este número é listado no formato: 00-0X, em que X é a localização do número do slot da placa adaptadora SCSI.
7. Quando solicitado, insira o endereço CONNECTION do dispositivo que estiver instalando. O endereço de conexão é um número de dois dígitos. O primeiro dígito é o ID SCSI (valor gravado na planilha). O segundo dígito é o número da unidade lógica (LUN) SCSI do dispositivo, que geralmente é zero, a menos que seja indicado de outra forma. O ID e o LUN do SCSI devem ser separados por vírgula (,). Por exemplo, um endereço de conexão de `4,0` tem um ID=4 e um LUN=0 SCSI.
8. Clique em **EXECUTAR**.

   Você recebe uma mensagem (nome do arquivo lógico) do formulário `lbX Available`. Observe o valor de X, que é um número que é designado automaticamente pelo sistema. Use estas informações para preencher o campo **Nome do dispositivo** na planilha.

   Por exemplo, se a mensagem for `lb0 Available`, o campo **Nome do dispositivo** será `/dev/lb0` na planilha. Utilize sempre o prefixo `/dev/` com o nome fornecido pelo SMIT.

AIX Configurando os drivers de dispositivos do IBM Spectrum Protect para unidades de fita

Use o procedimento a seguir para configurar os drivers de dispositivo do IBM Spectrum Protect para alteradores de mídia para bibliotecas adquiridas pelo fornecedor.

Procedimento

Importante: O IBM Spectrum Protect não pode substituir fitas *tar* ou *dd*, mas *tar* ou *dd* pode substituir fitas do IBM Spectrum Protect.

Restrição: As unidades de fita podem ser compartilhadas somente quando a unidade não estiver definida ou o servidor não estiver iniciado. O comando **MKSYSB** não funciona quando o IBM Spectrum Protect e o AIX compartilham a mesma unidade ou unidades. Para usar o driver de dispositivo de fita nativo do sistema operacional com uma unidade SCSI, o dispositivo deverá primeiro ser configurado para o AIX e, em seguida, configurado para o IBM Spectrum Protect. Consulte a documentação do AIX referente a estes drivers de dispositivos nativos.

Execute o programa SMIT para configurar o driver de dispositivo para cada unidade (inclusive unidades de bibliotecas), como a seguir:

1. Selecione **Dispositivos**.
2. Selecione **IBM Spectrum ProtectDevices**.
3. Selecione **Unidade de fita**.
4. Selecione **Incluir uma unidade de fita**.
5. Selecione o IBM Spectrum Protect-SCSI-MT para qualquer unidade de fita suportada.
6. Selecione a placa à qual o dispositivo está sendo conectado. Este número é listado no formato: 00-0X, em que X é a localização do número do slot da placa adaptadora SCSI.
7. Quando solicitado, digite o endereço de CONEXÃO do dispositivo que está instalando. O endereço de conexão é um número de dois dígitos. O primeiro dígito é o ID SCSI (valor gravado na planilha). O segundo dígito é o número da unidade lógica (LUN) SCSI do dispositivo, que geralmente é zero, a menos que seja indicado de outra forma. O ID e o LUN do SCSI devem ser separados por vírgula (,). Por exemplo, um endereço de conexão de `4,0` tem um ID=4 e um LUN=0 SCSI.
8. Clique em **EXECUTAR**. Você recebe uma mensagem:

   Se estiver configurando o driver de dispositivo para um dispositivo de fita (diferente de uma unidade de fita IBM), você receberá uma mensagem (nome do arquivo lógico) no formato `mtX Available`. Observe o valor de X, que é um número que é designado automaticamente pelo sistema. Use estas informações para preencher o campo **Nome do dispositivo** na planilha.

   Por exemplo, se a mensagem for `mt0 Available`, o campo **Nome do dispositivo** será `/dev/mt0` na planilha. Utilize sempre o prefixo `/dev/` com o nome fornecido pelo SMIT.

AIX Configurando dispositivos conectados à SAN Fibre Channel

Para configurar um dispositivo conectado à SAN Fibre Channel, conclua o procedimento.

Procedimento

1. Execute o programa SMIT.
2. Selecione **Dispositivos**.
3. Selecione **IBM Spectrum ProtectDevices**.
4. Selecione **Dispositivos conectados à SAN Fibre Channel**.
5. Selecione **Descobrir dispositivos suportados pelo IBM Spectrum Protect**. O processo de descoberta pode levar algum tempo.
6. Volte para o menu **Fibre Channel** e selecione **Listar atributos de um dispositivo descoberto**.
7. Observe o identificador de dispositivo de três caracteres que é usado ao definir um caminho para o dispositivo IBM Spectrum Protect.
   Por exemplo, se uma unidade de fita tiver o identificador `mt2`, especifique `/dev/mt2` como o nome do dispositivo.

Linux Configurando drivers de dispositivo de fita em sistemas Linux

Revise os tópicos a seguir ao instalar e configurar drivers de dispositivo de fita em sistemas Linux.

Linux Configurando drivers intermediários do IBM Spectrum Protect para dispositivos de fita e bibliotecas

Para usar o driver do IBM Spectrum Protect Linux Passthru, deve-se concluir as etapas a seguir.

Procedimento

1. Verifique se o dispositivo está conectado ao sistema e se está ligado e ativo.
2. Verifique se o dispositivo está corretamente detectado pelo seu sistema emitindo este comando:

   ```
   cat /proc/scsi/scsi
   ```

3. Certifique-se de que o pacote de drivers de dispositivo do IBM Spectrum Protect (`tsmscsi`) e o pacote do servidor de armazenamento estejam instalados.
4. Existem dois métodos de configuração de driver disponíveis no pacote de drivers de dispositivo do IBM Spectrum Protect: `autoconf` e `tsmscsi`. Esses dois métodos concluem as tarefas a seguir:
   - Carregue o driver genérico SCSI do Linux (sg) para o kernel.
   - Crie arquivos especiais necessários para o driver Passthru.
   - Crie arquivos de informações de dispositivo para dispositivos de fita (`/dev/tsmscsi/mtinfo`) e bibliotecas (`/dev/tsmscsi/lbinfo`).
5. Execute o método de configuração preferencial (`autoconf` ou `tsmscsi`) para o driver intermediário do IBM Spectrum Protect.
   - Para executar o método de configuração `autoconf`, emita o seguinte comando:

     ```
     autoconf
     ```

   - Para executar o método de configuração `tsmscsi`, conclua as seguintes etapas:
     a. Copie os dois arquivos de configuração de amostra que estão no diretório de instalação a partir de *mt.conf.smp* e *lb.conf.smp* para *mt.conf* e *lb.conf*, respectivamente.
     b. Editar o `mt.conf` e `lb.conf`. Inclua uma sub-rotina (conforme mostrado no exemplo no início do arquivo) para cada combinação de destino, ID e LUN SCSI. Cada combinação de entradas de destino SCSI, ID e LUN correspondem a uma unidade de fita ou biblioteca que deseja configurar. Certifique-se de que os arquivos atendam a estes requisitos:
        – Remova o exemplo que está no início dos arquivos.

- Deve haver uma nova linha entre cada sub-rotina.
- Deve haver uma nova linha depois da última sub-rotina.
- Assegure-se de que não haja sinais de número (#) em qualquer arquivo.

c. Execute o script `tsmscsi` no diretório de instalação do driver de dispositivo.

6. Verifique se o dispositivo está configurado corretamente visualizando os arquivos de texto para dispositivos de fita (`/dev/tsmscsi/mtinfo`) e bibliotecas (`/dev/tsmscsi/lbinfo`).
7. Determine os nomes de arquivos especiais para as unidades de fita e bibliotecas:
   - Para determinar os nomes para dispositivos de fita, emita o comando a seguir:

     ```
     > ls  /dev/tsmscsi/mt*
     ```

   - Para determinar os nomes para bibliotecas, emita o comando a seguir:

     ```
     > ls  /dev/tsmscsi/lb*
     ```

   Essas informações ajudam a identificar quais dos nomes de arquivo especiais `/dev/tsmscsi/mtx` e `/dev/tsmscsi/lbx` deverão ser fornecidos para o servidor quando emitir um comando **DEFINE PATH**.

O que Fazer Depois

Se você reiniciar o sistema host, deverá executar novamente o script `autoconf` ou `tsmscsi` para reconfigurar dispositivos do IBM Spectrum Protect. Se você reiniciar a instância do servidor do IBM Spectrum Protect, não é preciso reconfigurar dispositivos. Em geral, o driver genérico SCSI do Linux é pré-instalado no kernel. Para verificar se o driver está no kernel, emita o comando a seguir:

```
> lsmod | grep sg
```

Se o driver não estiver no kernel, emita o comando **modprobe sg** para carregar o driver sg no kernel.

Linux Instalando drivers de dispositivo zSeries Linux Fibre Channel (zfcp)

O driver de dispositivo do adaptador Fibre Channel do zSeries Linux (zfcp) é um driver de adaptador especial no sistema IBM zSeries.

Sobre Esta Tarefa

Os drivers de dispositivo de fita IBM Spectrum Protect e IBM podem ser executados em plataformas zSeries com sistemas operacionais Linux em ambientes de 64 bits, e suportam a maioria dos dispositivos de fita original equipment manufacturer (OEM) e IBM com interfaces Fibre Channel.

Para obter informações adicionais sobre o driver zfcp, consulte o IBM Redpaper, *Getting Started with zSeries Fibre Channel Protocol*, que está disponível em IBM Redbooks.

Procedimento

1. Carregue o módulo qdio.
2. Instale o driver zfcp.
3. Mapeie o Fibre Channel Protocol (FCP) e configure o driver zfcp.
4. Instale e configure o driver de dispositivo de fita IBM.

Linux Informações sobre dispositivos SCSI do seu sistema

Informações sobre os dispositivos vistos por seu sistema estão disponíveis no arquivo */proc/scsi/scsi.* Este arquivo contém uma lista de cada dispositivo SCSI detectado.

As informações sobre o dispositivo a seguir estão disponíveis: o número do host, número do canal, ID do SCSI, número da Unidade Lógica, fornecedor, nível de firmware, tipo de dispositivo e o modo SCSI. Por exemplo, se um sistema contiver algumas bibliotecas StorageTek e IBM, um SAN Gateway e algumas unidades Quantum DLT, o arquivo */proc/scsi/scsi* será semelhante a este:

```
Attached devices:
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor:  STK    Model: 9738     Rev: 2003
  Type:  Medium Changer        ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor:  PATHLIGHT Model: SAN Gateway     Rev: 32aC
  Type: Unknown          ANSI SCSI revision: 03
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor:  QUANTUM  Model: DLT7000     Rev: 2560
  Type:  Sequential-Access         ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 04
  Vendor: IBM     Model: 7337     Rev: 1.63
  Type:  Medium Changer        ANSI SCSI revision: 02
```

Linux Evitando que rótulos de fita sejam sobrescritos

O driver de dispositivo IBM Spectrum Protect Passthru usa o driver de dispositivo genérico SCSI do Linux (sg) para controlar e operar dispositivos de fita que estiverem conectados no sistema. Se o driver de dispositivo de fita SCSI genérico do Linux for carregado no kernel e configurar dispositivos de fita conectados, poderão surgir conflitos sobre como um dispositivo é gerenciado, porque tanto o driver sg genérico quanto o driver st podem controlar o mesmo dispositivo.

Sobre Esta Tarefa

Se o driver st controlar os dispositivos que são usados pelo IBM Spectrum Protect, os rótulo de fita internos do IBM Spectrum Protect poderão ser sobrescritos e os dados poderão ser perdidos. Se um aplicativo usar o driver st para controlar dispositivos e a opção não rebobinar não for especificada, as fitas serão rebobinadas automaticamente após a conclusão de uma operação. A operação de rebobinamento automático reposiciona o cabeçote no início da fita. Se a fita permanecer carregada na unidade, a próxima operação de gravação não IBM Spectrum Protect sobrescreverá o rótulo da fita IBM Spectrum Protect, por conta de o rótulo estar no início da fita.

Para evitar que os rótulos IBM Spectrum Protect sejam sobrescritos, podendo resultar em perda de dados, assegure-se de que apenas o driver do IBM Spectrum Protect Passthru controle dispositivos que sejam usados pelo IBM Spectrum Protect. Remova o driver st do kernel ou, se o driver for usado por alguns aplicativos no sistema, exclua os arquivos especiais que corresponderem aos dispositivos do IBM Spectrum Protect, para que o driver st não possa mais controlá-los.

Se estiver usando o driver de dispositivo de fita IBM para controlar dispositivos em seu sistema, talvez ocorrerão os mesmos problemas com conflitos de controle de driver de dispositivo. Revise a documentação de sua fita IBM para determinar como resolver esse problema e evitar perda de dados.

Remova o driver st

Se nenhum outro aplicativo no sistema usar dispositivo st, remova o driver st do kernel. Emita o seguinte comando para descarregar o driver st:

```
rmmod st
```

Exclua arquivos especiais de dispositivo que corresponderem aos dispositivos IBM Spectrum Protect

Se houver aplicativos que requerem o uso do driver st, exclua os arquivos especiais que corresponderem aos dispositivos IBM Spectrum Protect. Esses arquivos especiais são gerados pelo driver st. Quando eles são eliminados, o driver st não pode mais controlar os dispositivos IBM Spectrum Protect correspondentes. Nomes de arquivo especiais de dispositivo para unidades de fita aparecem no diretório `/dev/`. Os nomes têm o formato `/dev/[n]st[0-1024][l][m][a]`.

Liste os nomes de arquivos especiais de unidade st e os nomes de arquivos especiais de dispositivos IBM Spectrum Protect usando o comando ls. Com base na saída das sequências de dispositivo, é possível localizar dispositivos na lista de dispositivos st que corresponderem aqueles na lista de dispositivos IBM Spectrum Protect. Em seguida, o comando rm pode ser utilizado para excluir dispositivos st.

Emita os seguintes comandos para listar os dispositivos st e IBM Spectrum Protect:

```
ls -l /dev/*st*
ls -l /dev/tsmscsi/mt*
```

Exclua os dispositivos st usando o comando `rm`:

```
rm /dev/*st*
```

Windows Configurando drivers de dispositivo de fita em sistemas Windows

Revise as instruções para instalar e configurar drivers para dispositivos de fita e bibliotecas em sistemas Windows.

Windows Preparando para usar o driver intermediário do IBM Spectrum Protect para dispositivos de fita e bibliotecas

Para usar o driver de dispositivo intermediário do IBM Spectrum Protect Windows para dispositivos de fita e bibliotecas, deve-se instalar o driver e obter os nomes dos dispositivos para o servidor usar.

Antes de Iniciar

1. Determine se o fabricante do dispositivo de fita ou biblioteca de fitas fornece um driver de dispositivo.
2. Se o fabricante fornecer um pacote de driver de dispositivo, faça download do pacote e instale-o.
3. Configure o driver de dispositivo SCSI seguindo as instruções do fabricante.

Procedimento

1. Instale o driver de dispositivo intermediário do IBM Spectrum Protect.
2. Obtenha os nomes do dispositivo que o servidor deve usar executando uma das seguintes ações:
   - No servidor, execute o comando **QUERY SAN**. A saída mostra todos os nomes de dispositivos e seus números de série de dispositivo associados.
   - No diretório do servidor, execute o utilitário **tsmdlst.exe**. A saída mostra todos os nomes de dispositivos, seus números de série associados e locais de dispositivo associados.
   - No prompt de comandos do sistema Windows, execute o comando **regedit**. Na saída, obtenha os nomes do arquivo de dispositivo com base nas localizações de dispositivo. A localização consiste no ID da porta, ID do barramento SCSI, ID de LUN e ID de destino SCSI. O nome do arquivo de dispositivo do IBM Spectrum Protect tem um formato de mt*A*.*B*.*C*.*C* para unidades de fita e lb*A*.*B*.*C*.*D* para bibliotecas de fitas, em que:
     - *A* é o ID de destino SCSI.
     - *B* é o ID de LUN.
     - *C* é o ID de barramento SCSI.
     - *D* é o ID da porta.

Windows Configurando o driver SCSI do IBM Spectrum Protect para dispositivos de fita e bibliotecas

Se o fabricante de uma unidade de fita ou biblioteca de fitas não fornecer um driver de dispositivo SCSI, você deve instalar o driver de dispositivo SCSI do IBM Spectrum Protect.

Sobre Esta Tarefa

O nome do arquivo do driver de dispositivo SCSI do IBM Spectrum Protect é `tsmscsi64.sys`.

Procedimento

1. Localize o dispositivo no console do Gerenciador de Dispositivos (`devmgmt.msc`) e selecione-o. As unidades de fita estão listadas em **Unidades de fita**, e os alteradores de mídia estão em **Alteradores de mídia**.
2. Configure o dispositivo para uso pelo driver de dispositivo `tsmscsi64.sys`:
   a. Clique com o botão direito no dispositivo e clique em **Atualizar Software de driver**.
   b. Clique em **Procurar em meu computador o driver de software**.

3. Clique em **Deixe-me selecionar de uma lista de drivers de dispositivo em meu computador**.
4. Clique em **Avançar**.
5. Selecione a opção apropriada:
   a. Para uma unidade de fita, selecione **IBM Spectrum Protect para Unidades de Fita**.
   b. Para um alterador de mídia, selecione **IBM Spectrum Protect para Alteradores de Mídia**.
6. Clique em **Avançar**.
7. Clique em **Concluir**.
8. Verifique se o dispositivo foi configurado corretamente para o driver de dispositivo `tsmscsi64`:
   a. Clique com o botão direito no dispositivo e clique em **Propriedades**.
   b. Clique na guia **Driver** e em **Detalhes do driver**. A janela **Detalhes do driver** mostra o driver de dispositivo que está controlando o dispositivo.

Configurando bibliotecas para uso por um servidor

Para usar uma biblioteca ou bibliotecas para armazenamento para um servidor IBM Spectrum Protect, deve-se primeiro configurar os dispositivos no sistema do servidor.

Antes de Iniciar

1. Conecte dispositivos ao hardware do servidor. Siga as instruções em "Conectando um dispositivo de biblioteca automatizada ao seu sistema" na página 73.
2. Selecione os drivers de dispositivo de fita. Siga as instruções em "Selecionando um driver de dispositivo de fita" na página 73.
3. Instale e configure os drivers de dispositivo de fita. Siga as instruções em "Instalando e configurando drivers de dispositivo de fita" na página 76.
4. Determine os nomes dos dispositivos que são necessários para definir a biblioteca para o servidor. Siga as instruções em "Nomes de arquivos especiais para dispositivos de fita" na página 75.

Procedimento

1. Defina a biblioteca e o caminho do servidor para a biblioteca. Siga as instruções em "Definindo bibliotecas" na página 89.
2. Defina as unidades na biblioteca. Siga as instruções em "Definindo unidades" na página 90.

   Para bibliotecas SCSI, é possível usar o comando **PERFORM LIBACTION** para definir unidades e caminhos para uma biblioteca em uma etapa, em vez de concluir as duas etapas "2" na página 87 e "3" na página 87. Para usar o comando **PERFORM LIBACTION** para definir unidades e caminhos para uma biblioteca, a opção SANDISCOVERY deve ser suportada e ativada.
3. Defina um caminho do servidor para cada unidade usando o comando **DEFINE PATH**.
4. Defina uma classe de dispositivo. Siga as instruções em "Definindo classes de dispositivo de fita" na página 91.

   As classes de dispositivo especificam os formatos de gravação para unidades e as classificam de acordo com o tipo. Use o valor padrão, **FORMAT=DRIVE** como o formato de gravação apenas se todas as unidades que estiverem associadas à classe de dispositivo puderem ler e gravar em toda a mídia.

   Por exemplo, se você tiver uma combinação de unidades Ultrium Geração 3 e Ultrium Geração 4, mas tiver somente uma mídia Ultrium Geração 3. É possível especificar **FORMAT=DRIVE**, porque tanto as unidades da Geração 4 quanto as unidades da Geração 3 podem ler e gravar na mídia da Geração 3.
5. Defina um conjunto de armazenamentos usando o comando **DEFINE STGPOOL**.

   Considere as seguintes opções principais para definir conjuntos de armazenamentos:

- Os volumes utilizáveis são volumes nulos disponíveis para uso. Se você especificar um valor para o número máximo de volumes utilizáveis no conjunto de armazenamentos, o servidor poderá escolher entre os volumes utilizáveis disponíveis na biblioteca.

  Se você não permitir volumes utilizáveis, a etapa extra de definir explicitamente cada volume a ser usado no conjunto de armazenamentos deverá ser concluída. Além disso, especifique o parâmetro **MAXSCRATCH=0** ao definir o conjunto de armazenamentos para que os volumes utilizáveis não sejam usados.
- A configuração padrão para conjuntos de armazenamentos primários é a disposição por grupo. O padrão para conjuntos de armazenamentos de cópia e conjuntos de dados ativos é a desativação da disposição. O servidor usa a *disposição* para manter todos os arquivos que pertencerem a um grupo de nós clientes, um único nó cliente, um espaço de arquivo do cliente ou um grupo de espaços no arquivo do cliente em um número mínimo de volumes. Se a disposição estiver desativada para um conjunto de armazenamentos e os clientes começarem a armazenar dados, não será possível mudar os dados facilmente no conjunto para que eles sejam dispostos.

6. Efetue check-in e rotule os volumes da biblioteca. Siga as instruções em "Efetuando check-in de volumes em uma biblioteca automatizada" na página 179 e "Etiquetando volumes de fita" na página 177.

   Assegure-se de que volumes suficientes na biblioteca estejam disponíveis para o servidor. Mantenha volumes suficientes rotulados em mãos para que não se esgotem durante uma operação, como um backup de cliente. Rotule volumes utilizáveis adicionais para quaisquer operações de recuperação em potencial que possam ocorrer posteriormente.

   Os procedimentos para check-in e rotulagem de volumes são os mesmos, independentemente se a biblioteca contiver unidades de um único tipo de dispositivo ou unidades de múltiplos tipos de dispositivos. É possível usar o comando **CHECKIN LIBVOLUME** para efetuar check-in de volumes que já estiverem rotulados. Ou então, se desejar rotular e efetuar check-in de volumes em uma etapa, emita o comando **LABEL LIBVOLUME**.

   Bibliotecas com múltiplos tipos de dispositivo: Se sua biblioteca possuir unidades de múltiplos tipos de dispositivos e você definiu duas bibliotecas para o servidor do IBM Spectrum Protect, as duas bibliotecas definidas representarão uma biblioteca física. Deve-se efetuar check-in de volumes de fita separadamente para cada biblioteca definida. Certifique-se de efetuar check-in de volumes para a biblioteca do IBM Spectrum Protect.

O que Fazer Depois

Verifique as definições do seu dispositivo para assegurar que tudo esteja configurado corretamente. Use um comando **QUERY** para revisar informações sobre cada objeto de armazenamento.

Ao revisar os resultados do comando **QUERY DRIVE**, verifique se o tipo de dispositivo para a unidade é o que você espera. Se um caminho não for definido, o tipo de dispositivo da unidade será listado como UNKNOWN e, se o caminho errado for utilizado, GENERIC_TAPE ou outro tipo de dispositivo será mostrado. Esta etapa é importante, especialmente quando estiver usando mídia combinada.

Opcionalmente, configure o compartilhamento de biblioteca. Siga as instruções em "Configurando o compartilhamento de biblioteca" na página 98.

Informações relacionadas

CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)

DEFINE STGPOOL (definir um volume em um conjunto de armazenamentos)

LABEL LIBVOLUME (Rotular um volume de biblioteca)

PERFORM LIBACTION (Definir ou Excluir Todas as Unidades e os Caminhos para uma Biblioteca)

Definindo dispositivos de fita

Antes de fazer backup ou migrar dados para a fita, deve-se definir um dispositivo de fita para o servidor.

Definindo bibliotecas e unidades

Uma biblioteca de fitas pode incluir uma ou mais unidades de fita. Saiba como definir bibliotecas, unidades e caminhos para o servidor IBM Spectrum Protect.

Definindo bibliotecas

Antes de poder usar uma unidade, deve-se definir a biblioteca à qual a unidade pertence.

Procedimento

1. Define a biblioteca usando o comando **DEFINE LIBRARY**.

   Por exemplo, se você tiver uma biblioteca de fitas IBM TS3500, é possível definir uma biblioteca chamada ROBOTMOUNT usando o seguinte comando:

   ```
   define library robotmount libtype=scsi
   ```

   Se precisar do compartilhamento de bibliotecas ou da movimentação de dados sem LAN, consulte as seguintes informações:

   - “Configurando o compartilhamento de biblioteca” na página 98
   - “Configurando a Movimentação de Dados sem LAN” na página 117
2. Defina um caminho do servidor para a biblioteca usando o comando **DEFINE PATH**. Ao especificar o parâmetro **DEVICE**, insira o nome do arquivo especial do dispositivo. Esse nome é requerido pelo servidor para se comunicar com unidades de fita, alterador de mídia e dispositivos de mídia removíveis. Para obter informações adicionais sobre nomes de arquivos especiais do dispositivo, consulte “Nomes de arquivos especiais para dispositivos de fita” na página 75.

   AIX
   ```
   define path server1 robotmount srctype=server desttype=library
   device=/dev/lb0
   ```

   Linux
   ```
   define path server1 robotmount srctype=server desttype=library
   device=/dev/tsmscsi/lb0
   ```

   Windows
   ```
   define path server1 robotmount srctype=server desttype=library
   device=lb0.0.1.0
   ```

Informações relacionadas

DEFINE LIBRARY (Definir uma biblioteca)
DEFINE PATH (Definir um caminho)

Definindo bibliotecas SCSI em uma SAN

Para um tipo de biblioteca SCSI em uma SAN, o servidor pode rastrear o número de série da biblioteca. Com o número de série, o servidor pode confirmar a identidade do dispositivo quando você define o caminho ou quando o servidor usa o dispositivo.

Sobre Esta Tarefa

Se preferir, será possível especificar o número de série ao definir a biblioteca para o servidor. Por conveniência, o padrão é permitir que o servidor obtenha o número de série da biblioteca ao definir o caminho.

Se especificar o número de série, o servidor confirmará que o número de série está correto ao definir o caminho para a biblioteca. Ao definir o caminho, é possível configurar o parâmetro **AUTODETECT=YES** para permitir que o servidor corrija o número de série se o número detectado não corresponder ao que foi inserido ao definir a biblioteca. Como uma melhor prática, especifique o parâmetro **AUTODETECT=YES** para atualizar automaticamente o número de série para a unidade no banco de dados quando o caminho está definido.

Dependendo dos recursos da biblioteca, o servidor pode não conseguir detectar automaticamente o número de série. Nem todos os dispositivos são capazes de retornar um número de série quando

solicitado por um aplicativo, como o servidor. Neste caso, o servidor não registra um número de série para o dispositivo e é incapaz de confirmar a identidade do dispositivo quando você define o caminho ou quando o servidor usa o dispositivo. Para obter informações adicionais, consulte "Impactos de mudanças de dispositivo na SAN" na página 127.

Definindo unidades

Para informar o servidor sobre uma unidade que pode ser usada para acessar volumes de armazenamento, emita o comando **DEFINE DRIVE**, seguido pelo comando **DEFINE PATH**.

Antes de Iniciar

Um *objeto da unidade* representa um mecanismo de unidade em uma biblioteca que utiliza mídia removível. Para dispositivos com múltiplas unidades, incluindo bibliotecas automatizadas, deve-se definir cada unidade separadamente e associá-la a uma biblioteca. As definições de unidade podem incluir informações, como o endereço do elemento para unidades em SCSI, a frequência com que uma unidade de fita é limpa e se a unidade está on-line.

O IBM Spectrum Protect suporta unidades de fita que podem ser independentes ou que podem ser parte de uma biblioteca automatizada. O método preferencial é configurar a solução de fita usando bibliotecas automatizadas.

Sobre Esta Tarefa

Ao emitir o comando **DEFINE DRIVE**, deve-se fornecer algumas ou todas as informações a seguir:

Nome da Biblioteca
O nome da biblioteca na qual a unidade está localizada.

Nome da unidade
O nome que é designado à unidade.

Número de série
O número de série da unidade. O parâmetro de número de série se aplica apenas a unidades em SCSI. Com o número de série, o servidor pode confirmar a identidade do dispositivo quando você define o caminho ou quando o servidor usa o dispositivo.

Se preferir, será possível especificar o número de série. O padrão é permitir que o próprio servidor obtenha o número de série da unidade no momento em que o caminho é definido. Se especificar o número de série, o servidor confirmará que o número de série está correto ao definir o caminho para a unidade. Ao definir o caminho, é possível configurar o parâmetro **AUTODETECT=YES** para permitir que o servidor corrija o número de série, se o número que ele detectar não corresponder ao que foi inserido ao definir a unidade. Como uma melhor prática, especifique o parâmetro **AUTODETECT=YES** para atualizar automaticamente o número de série para a unidade no banco de dados quando o caminho está definido.

Dependendo dos recursos da unidade, o servidor pode não conseguir detectar automaticamente o número de série. Neste caso, o servidor não registra um número de série para o dispositivo e é incapaz de confirmar a identidade do dispositivo quando você define o caminho ou quando o servidor usa o dispositivo. Consulte "Impactos de mudanças de dispositivo na SAN" na página 127.

Endereço do elemento
O endereço do elemento da unidade. O parâmetro **ELEMENT** se aplica apenas a unidades em bibliotecas SCSI. O endereço do elemento é um número que indica a localização física de uma unidade dentro de uma biblioteca automatizada. O servidor precisa do endereço do elemento para conectar o local físico da unidade ao endereço SCSI da unidade. O servidor pode obter o endereço do elemento da unidade ao definir o caminho, ou é possível especificar o número do elemento ao definir a unidade. Como uma melhor prática, especifique o parâmetro **ELEMENT=AUTODETECT** para o servidor para detectar automaticamente o número do elemento quando o caminho para a unidade estiver definido.

Dependendo dos recursos da biblioteca, o servidor pode não conseguir detectar automaticamente o endereço do elemento. Neste caso, deve-se fornecer o endereço do elemento ao definir a unidade,

caso a biblioteca tenha mais de uma unidade. Para obter o endereço do elemento, acesse o IBM Support Portal for IBM Spectrum Protect.

Dica: Os drivers de dispositivo de fita IBM e o drivers de dispositivo de fita não IBM geram diferentes arquivos de dispositivo e formatos:

- Para IBM, os nomes de dispositivos começam com `rmt` seguidos por um número inteiro, por exemplo, `/dev/rmt0`.
- Para drivers de dispositivo de fita IBM Spectrum Protect, os nomes de dispositivos de fita começam com `mt` seguido por um número inteiro, por exemplo, `/dev/mt0`.

Você deve usar o arquivo de dispositivo correto ao definir um caminho.

Procedimento

1. Designe uma unidade a uma biblioteca emitindo o comando **DEFINE DRIVE**.
2. Para tornar a unidade utilizável pelo servidor, emita o comando **DEFINE PATH**.

   Para obter exemplos sobre como configurar bibliotecas, caminhos e unidades, consulte Exemplo: configure uma biblioteca SCSI ou Virtual Tape Library com um tipo de dispositivo de unidade único e Exemplo: configure uma biblioteca SCSI ou Virtual Tape Library com múltiplos tipos de dispositivo da unidade.

Definindo classes de dispositivo de fita

Uma classe de dispositivo define um conjunto de características que são usadas por um conjunto de volumes que podem ser criados em um conjunto de armazenamentos. Você deve definir uma classe de dispositivo para um dispositivo de fita para assegurar que o servidor possa usar o dispositivo.

Antes de Iniciar

Deve-se definir as bibliotecas e as unidades para o servidor antes de definir as classes de dispositivo.

Sobre Esta Tarefa

Para obter uma lista de dispositivos suportados e formatos de classes de dispositivo válidas, consulte o website IBM Spectrum Protect Dispositivos suportados para seu sistema operacional:

- AIX Windows Dispositivos Suportados para AIX e Windows
- Linux Dispositivos Suportados para Linux

É possível definir múltiplas classes de dispositivo para cada tipo de dispositivo. Por exemplo, talvez você queira especificar diferentes atributos para conjuntos de armazenamentos diferentes que usarem o mesmo tipo de unidade de fita. Podem ser requeridas variações que não são específicas para o dispositivo, mas sim, para o modo com que deseja usar o dispositivo (por exemplo, a retenção de montagem ou limite de montagem).

Diretrizes:

- Uma classe de dispositivo pode ser associada a vários conjuntos de armazenamentos, mas cada conjunto de armazenamentos é associado apenas a uma classe de dispositivo.
- Bibliotecas SCSI podem incluir unidades de fita de mais de um tipo de dispositivo. Ao definir a classe de dispositivo nesse ambiente, deve-se declarar um valor para o parâmetro **FORMAT**.

  Para obter informações adicionais, consulte “Tipos de dispositivos combinados em bibliotecas” na página 18.

Procedimento

Para definir uma classe de dispositivo, use o comando **DEFINE DEVCLASS** com o parâmetro **DEVTYPE**, que designa um tipo de dispositivo para a classe de dispositivo.

Resultados

Se você incluir a opção DEVCONFIG no arquivo dsmserv.opt, os arquivos que forem especificados com essa opção serão atualizados automaticamente com os resultados dos comandos **DEFINE DEVCLASS**, **UPDATE DEVCLASS** e **DELETE DEVCLASS**.

Informações relacionadas

DEFINE DEVCLASS (Definir uma Classe de Dispositivo)

QUERY DEVCLASS (Exibir Informações Sobre Uma ou Mais Classes de Dispositivo)

UPDATE DEVCLASS (atualizar uma classe de dispositivo)

Definindo classes de dispositivo LTO

Para evitar problemas ao combinar diferentes gerações de unidades e mídia LTO em uma única biblioteca, revise as restrições. Além disso, revise as restrições para a criptografia de unidade LTO.

Combinando unidades e mídia LTO em uma biblioteca

Ao combinar diferentes gerações de unidades e mídia LTO, você deve considerar os recursos de leitura/gravação de cada geração. O método preferencial é configurar uma classe de dispositivo diferente para cada geração de mídia.

Sobre Esta Tarefa

Se estiver considerando a combinação de diferentes gerações de mídia e unidades LTO, revise as seguintes restrições:

Tabela 22. Recursos de leitura/gravação para diferentes gerações de unidades LTO

Unidades	Mídia de geração 1	Mídia de geração 2	Mídia de geração 3	Mídia de geração 4	Mídia de geração 5	Mídia de geração 6	Mídia de Geração 7	Mídia de geração M8	Mídia de geração 8
Geração 1	Acesso de leitura/ gravação	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D
Geração 2	Acesso de leitura/ gravação	Acesso de leitura/ gravação	N/D	N/D	N/D	N/D	N/D	N/D	N/D
Geração 3	Acesso somente leitura	Acesso de leitura/ gravação	Acesso de leitura/ gravação	N/D	N/D	N/D	N/D	N/D	N/D
Geração 4	N/D	Acesso somente leitura	Acesso de leitura/ gravação	Acesso de leitura/ gravação	N/D	N/D	N/D	N/D	N/D
Geração 5	N/D	N/D	Acesso somente leitura	Acesso de leitura/ gravação	Acesso de leitura/ gravação	N/D	N/D	N/D	N/D
Geração 6	N/D	N/D	N/D	Acesso somente leitura	Acesso de leitura/ gravação	Acesso de leitura/ gravação	N/D	N/D	N/D
Geração 7	N/D	N/D	N/D	N/D	Acesso de Leitura	Acesso de leitura/ gravação	Acesso de leitura/ gravação	N/D	N/D
Geração 8	N/D	N/D	N/D	N/D	N/D	N/D	Acesso de leitura/ gravação	Acesso de leitura/ gravação	Acesso de leitura/ gravação

Exemplo

Se estiver combinando diferentes tipos de unidades e mídia, configure classes de dispositivo diferentes: uma para cada tipo de mídia. Para especificar o tipo de mídia, use o parâmetro **FORMAT** em cada uma das definições de classe de dispositivo. (Não especifique FORMAT=DRIVE). Por exemplo, se estiver combinando unidades Ultrium Geração 5 e Ultrium Geração 6, especifique FORMAT=ULTRIUM5C (ou

ULTRIUM5) para a classe de dispositivo Ultrium Geração 5 e FORMAT=ULTRIUM6C (ou ULTRIUM6) para a classe de dispositivo Ultrium Geração 6.

Nesse exemplo, ambas as classes de dispositivo podem apontar para a mesma biblioteca com unidades Ultrium Geração 5 e Ultrium Geração 6. As unidades são compartilhadas entre os dois conjuntos de armazenamentos. Um conjunto de armazenamentos usa a primeira classe de dispositivo e a mídia Ultrium Geração 5 exclusivamente. O outro conjunto de armazenamentos usa a segunda classe de dispositivo e a mídia Ultrium Geração 6 exclusivamente. Como os dois conjuntos de armazenamentos compartilham uma única biblioteca, a mídia Ultrium Geração 5 pode ser montada em unidades Ultrium Geração 6 conforme se tornam disponíveis durante o processamento de ponto de montagem.

Se você combinar gerações de mídia somente leitura mais antigas com mídia de leitura/gravação mais recente em uma única biblioteca, deve marcar a mídia somente leitura como somente leitura e efetuar check-out de toda a mídia utilizável somente leitura. Por exemplo, se estiver combinando unidades e mídia Ultrium Geração 4 com Ultrium Geração 6 em uma única biblioteca, você deverá marcar a mídia Geração 4 como somente leitura. Além disso, você deve efetuar check-out de todos os volumes utilizáveis Geração 4.

Limites de montagem em ambientes de mídia combinada de LTO

Em uma biblioteca de mídia combinada, em que múltiplas classes de dispositivos apontam para a mesma biblioteca, unidades compatíveis são compartilhadas entre conjuntos de armazenamentos. Assegure-se de configurar um valor apropriado para o parâmetro **MOUNTLIMIT** em cada uma das classes de dispositivo.

Por exemplo, em uma biblioteca de mídia combinada que contém unidades e mídia Ultrium Geração 1 e Ultrium Geração 2, a mídia Ultrium Geração 1 pode ser montada em unidades Ultrium Geração 2.

Considere o exemplo de uma biblioteca combinada que consiste nas seguintes unidades e mídia:

- Quatro unidades LTO Ultrium Geração 1 e mídia LTO Ultrium Geração 1
- Quatro unidades LTO Ultrium Geração 2 e mídia LTO Ultrium Geração 2

Você criou as classes de dispositivo a seguir:

- Classe de dispositivo LTO Ultrium Geração 1 LTO1CLASS especificando FORMAT=ULTRIUM1C
- Classe de dispositivo LTO Ultrium Geração 2 LTO2CLASS especificando FORMAT=ULTRIUM2C

Você também criou os conjuntos de armazenamentos a seguir:

- Conjunto de armazenamentos LTO Ultrium Geração 1 LTO1POOL com base na classe de dispositivo LTO1CLASS
- Conjunto de armazenamentos LTO Ultrium Geração 2 LTO2POOL com base na classe de dispositivo LTO2CLASS

O número de pontos de montagem disponíveis para uso por cada conjunto de armazenamentos é especificado na classe de dispositivo usando o parâmetro **MOUNTLIMIT**. O parâmetro **MOUNTLIMIT** na classe de dispositivo LTO2CLASS deve ser configurado para 4 para corresponder ao número de unidades disponíveis que podem montar somente mídia LTO7. O parâmetro **MOUNTLIMIT** na classe de dispositivo LTO1CLASS deve ser configurado para um valor que seja maior que o número de unidades disponíveis (5 ou possivelmente 6) para ajustar ao fato de que a mídia Ultrium Geração 1 mídia pode ser montada em unidades Ultrium Geração 7. O valor ideal para **MOUNTLIMIT** depende da carga de trabalho e dos padrões de acesso do conjunto de armazenamentos.

Monitore e ajuste a configuração **MOUNTLIMIT** para adequar-se às cargas de trabalho que mudam constantemente. Se o **MOUNTLIMIT** para LTO1POOL for configurado muito alto, as solicitações de montagem para o LTO2POOL poderão ser atrasadas ou falhar porque as unidades Ultrium Geração 2 são usadas para satisfazer as solicitações de montagem do Ultrium Geração 1. No pior cenário, a concorrência demasiada para unidades Ultrium Geração 2 pode fazer com que montagens de mídia Geração 2 falhem com a mensagem a seguir:

```
ANR8447E No drives are currently available in the library.
```

Se o valor **MOUNTLIMIT** para LTO1POOL não for configurado alto o suficiente, as solicitações de montagem que podem ser satisfeitas por unidades LTO Ultrium Geração 2 serão atrasadas.

Restrição: As restrições de aplicam ao combinar unidades Ultrium Geração 1 com Ultrium Geração 2 ou Geração 3 devido a como os pontos de montagem são alocados. Por exemplo, os processos que requerem múltiplos pontos de montagem que incluem volumes Ultrium Geração 1 e Ultrium Geração 2 podem tentar reservar somente unidades Ultrium Geração 2, mesmo quando uma montagem pode ser satisfeita por uma unidade Ultrium Geração 6 disponível. Os processos que se comportam dessa maneira incluem os comandos **MOVE DATA** e **BACKUP STGPOOL**. Esses processos esperam até que o número necessário de pontos de montagem possa ser satisfeito com unidades Ultrium Geração 2.

Informações relacionadas

BACKUP STGPOOL (fazer backup dos dados do conjunto de armazenamentos primários para o conjunto de armazenamentos de cópia)

DEFINE DEVCLASS (Definir uma Classe de Dispositivo)

MOVE DATA (Mover Arquivos em um Volume do Conjunto de Armazenamento)

Ativando e desativando a criptografia de unidade para unidades de fita LTO Geração 4 ou mais recente

O IBM Spectrum Protect suporta os três tipos de criptografia de unidade que estão disponíveis com unidades LTO Geração 4 ou mais recente: Aplicativo, Sistema e Biblioteca. Esses métodos são definidos por meio do hardware.

Sobre Esta Tarefa

O parâmetro **DRIVEENCRYPTION** no comando **DEFINE DEVCLASS** especifica se a criptografia de unidade é permitida para formatos IBM e HP LTO Geração 4 ou mais recente, Ultrium 4 e Ultrium 4C. Este parâmetro assegura a compatibilidade do IBM Spectrum Protect com configurações de criptografia de hardware para volumes nulos. Não é possível usar esse parâmetro para volumes do conjunto de armazenamentos que estão cheios ou sendo preenchidos.

O IBM Spectrum Protect suporta o método de Aplicativo de criptografia com unidades IBM e HP LTO-4 ou mais recente. Somente o IBM LTO-4 ou mais recente suporta os métodos de Sistema e de Biblioteca. O método de criptografia da Biblioteca pode ser usado apenas se o hardware do seu sistema (por exemplo, IBM TS3500) suportá-lo.

Restrição: Não é possível usar criptografia de unidade com mídia write-once, read-many (WORM).

O método do aplicativo é definido por meio do hardware. Para usar o método do aplicativo, em que o IBM Spectrum Protect gera e gerencia chaves de criptografia, configure o parâmetro **DRIVEENCRYPTION** como ON. Esta ação permite a criptografia de dados para volumes nulos. Se o parâmetro for configurado como ON e o hardware estiver configurado para outro método de criptografia, as operações de backup falharão.

Procedimento

O exemplo simplificado a seguir mostra as etapas que você executaria para ativar e desativar a criptografia de dados para volumes nulos em um conjunto de armazenamentos:

1. Defina uma biblioteca emitindo o comando **DEFINE LIBRARY**:

   ```
   define library 3584 libtype=SCSI
   ```

2. Defina uma classe de dispositivo, LTO_ENCRYPT, emitindo o comando **DEFINE DEVCLASS** e especificando IBM Spectrum Protect como o gerenciador de chave:

   ```
   define devclass lto_encrypt library=3584 devtype=lto driveencryption=on
   ```

3. Defina um conjunto de armazenamentos emitindo o comando **DEFINE STGPOOL**:

   ```
   define stgpool lto_encrypt_pool lto_encrypt
   ```

4. Para desativar a criptografia em novos volumes, configure o parâmetro **DRIVEENCRYPTION** como 0FF. O valor padrão é ALLOW. A criptografia de unidade para volumes nulos será permitida se outro método de criptografia for ativado.

Conceitos relacionados

Métodos de criptografia de fita

A decisão sobre o método de criptografia a ser usado depende de como você deseja gerenciar seus dados.

Definindo classes de dispositivo 3592

As definições de classe de dispositivo para dispositivos 3592, TS1130, TS1140, TS1150 e mais recente incluem parâmetros para velocidades mais rápidas de acesso ao volume e criptografia de unidade. Para evitar problemas ao combinar diferentes gerações de unidades 3592 e TS1130 e mais recente em uma biblioteca, revise as diretrizes.

Combinando gerações de unidades e mídia 3592 em uma única biblioteca

Para obter um desempenho ideal, não combine gerações de mídia 3592 em uma única biblioteca. Problemas de mídia podem resultar quando gerações de unidades diferentes são combinadas. Por exemplo, o IBM Spectrum Protect pode não ser capaz de ler o rótulo de um volume.

Sobre Esta Tarefa

A tabela a seguir mostra a interoperabilidade de leitura/gravação para gerações de unidades.

Unidades	Formato da Geração 1	Formato da Geração 2	Formato da Geração 3	Formato da Geração 4	Formato da Geração 5
Geração 1	Acesso de leitura/ gravação	N/D	N/D	N/D	N/D
Geração 2	Acesso de leitura/ gravação	Acesso de leitura/ gravação	N/D	N/D	N/D
Geração 3	Acesso somente leitura	Acesso de leitura/ gravação	Acesso de leitura/ gravação	N/D	N/D
Geração 4	N/D	Somente leitura	Acesso de leitura/ gravação	Acesso de leitura/ gravação	N/D
Geração 5	N/D	N/D	Acesso de Leitura	Acesso de leitura/ gravação	Acesso de leitura/ gravação

Se você precisar combinar gerações de unidades em uma biblioteca, revise o exemplo e restrições para ajudar a evitar problemas.

Tabela 23. Combinando gerações de unidades	
Tipo de biblioteca	**Exemplo e restrições**
SCSI	Defina um novo conjunto de armazenamentos e classe de dispositivo para a geração de unidade mais recente. Por exemplo, suponha que você tenha um conjunto de armazenamentos e uma classe de dispositivo para 3592-2. O conjunto de armazenamentos contém todas as mídias que foram gravadas no formato da Geração 2. Suponha que o valor do parâmetro **FORMAT** na definição da classe de dispositivo seja configurado como 3952-2 (não **DRIVE**). Você inclui as unidades da Geração 3 na biblioteca. Execute as etapas a seguir: 1. Na nova definição de classe de dispositivo para as unidades da Geração 3, configure o valor do parâmetro **FORMAT** para 3592-3 ou 3592-3C. Não especifique **DRIVE**. 2. Na definição do conjunto de armazenamentos que está associado a unidades de Geração 2, atualize o parâmetro **MAXSCRATCH** para 0, por exemplo: `update stgpool genpool2 maxscratch=0` Este método permite que ambas as gerações usem seus formatos ideias e minimiza problemas de mídia em potencial que possam resultar da combinação de gerações. No entanto, ele não resolve todos os problemas de mídia. Por exemplo, ele pode resultar em uma concorrência para pontos de montagem e falhas de montagem. (Para saber mais sobre a competição de ponto de montagem no contexto de unidades e mídia 3592, consulte “Definindo classes de dispositivo 3592” na página 95.) **Restrição:** A lista a seguir descreve as restrições de mídia: • **CHECKIN LIBVOL**: o problema do uso da opção CHECKLABEL=YES. Se o rótulo for gravado em um formato da Geração 3 ou mais recente, e você especificar a opção CHECKLABEL=YES, as unidades de gerações anteriores falharão usando esse comando. Para evitar este problema, especifique CHECKLABEL=BARCODE. • **LABEL LIBVOL**: Quando o servidor tenta usar unidades de uma geração anterior para ler o rótulo gravado no formato de Geração 3 ou mais recente, o comando **LABEL LIBVOL** falha, a menos que OVERWRITE=YES esteja especificado. Verifique se a mídia que está sendo rotulada com OVERWRITE=YES não tenha nenhum dado ativo. • **CHECKOUT LIBVOL**: Quando o IBM Spectrum Protect verifica o rótulo (CHECKLABEL=YES) como um formato da Geração 3 ou mais recente, e as unidades de leitura de gerações anteriores, o comando falhará. Para evitar esse problema, especifique CHECKLABEL=NO.

Informações relacionadas

CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)

CHECKOUT LIBVOLUME (Verificar um Volume de Armazenamento Fora de uma Biblioteca)

LABEL LIBVOLUME (Rotular um volume de biblioteca)

UPDATE STGPOOL (Atualizar um conjunto de armazenamentos)

Controlando a velocidade de acesso a dados para volumes 3592

É possível otimizar a capacidade de armazenamento e melhorar a velocidade de acesso a dados ao criar volumes. Ao particionar dados em conjuntos de armazenamentos que possuem volumes, é possível especificar a porcentagem de capacidade de escala para fornecer capacidade de armazenamento máxima ou para fornecer acesso rápido ao volume.

Sobre Esta Tarefa

Para reduzir a capacidade de mídia, especifique o parâmetro **SCALECAPACITY** quando definir a classe de dispositivo usando o comando **DEFINE DEVCLASS** ou quando atualizar a classe de dispositivo usando o comando **UPDATE DEVCLASS**.

Especifique um valor de porcentagem de 20, 90 ou 100. Um valor de 20% fornece tempo de acesso mais rápido e 100% fornece a maior capacidade de armazenamento. Por exemplo, se você especificar uma capacidade de escala de 20 para uma classe de dispositivo 3592 sem compactação, um volume 3592 nessa classe de dispositivo armazenará 20% de sua capacidade total de 300 GB ou cerca de 60 GB.

A capacidade de escala entra em vigor apenas quando os dados são gravados pela primeira vez em um volume. As atualizações para a classe de dispositivo para capacidade de escala não afetam os volumes que já tiverem dados gravados neles até que o volume seja retornado para o status inicial.

Informações relacionadas

DEFINE DEVCLASS (Definir uma Classe de Dispositivo)

UPDATE DEVCLASS (atualizar uma classe de dispositivo)

Ativando e desativando a criptografia de unidade 3592 Geração 2 e mais recente

Com o IBM Spectrum Protect, é possível usar os seguintes tipos de criptografia de unidade com unidades que são 3592 Geração 2 e mais recente: Aplicativo, Sistema e Biblioteca. Esses métodos são definidos por meio do hardware.

Sobre Esta Tarefa

O parâmetro **DRIVEENCRYPTION** no comando **DEFINE DEVCLASS** especifica se a criptografia de unidade é permitida para unidades que são 3592 Geração 2 e mais recente. Use este parâmetro para assegurar a compatibilidade do IBM Spectrum Protect com configurações de criptografia de hardware para volumes nulos. Não é possível usar esse parâmetro para volumes do conjunto de armazenamentos que estão cheios ou sendo preenchidos.

- Para usar o método do aplicativo, em que o IBM Spectrum Protect gera e gerencia chaves de criptografia, configure o parâmetro **DRIVEENCRYPTION** como ON. Isso permite a criptografia de dados para volumes nulos. Se o parâmetro for configurado como ON e se o hardware estiver configurado para outro método de criptografia, as operações de backup falharão.
- Para usar os métodos de criptografia Biblioteca ou Sistema, configure o parâmetro como **ALLOW**. Isso especifica que IBM Spectrum Protect não é o gerenciador de chave para a criptografia de unidade, mas permite que o hardware criptografe os dados do volume por meio de um dos outros métodos. Especificar este parâmetro não criptografa os volumes automaticamente. Os dados podem ser criptografados apenas especificando o parâmetro **ALLOW** e configurando o hardware para usar um desses métodos.

O parâmetro **DRIVEENCRYPTION** é opcional. O valor padrão é permitir os métodos de criptografia Biblioteca ou Sistema.

Procedimento

O seguinte exemplo simplificado mostra como criptografar dados para volumes nulos em um conjunto de armazenamentos, usando o IBM Spectrum Protect como o gerenciador de chave:

1. Defina uma biblioteca emitindo o comando **DEFINE LIBRARY**.
   Por exemplo, emita o seguinte comando:

   ```
   define library 3584 libtype=SCSI
   ```

2. Defina uma classe de dispositivo, 3592_ENCRYPT, emitindo o comando **DEFINE DEVCLASS** e especificando o valor ON para o parâmetro **DRIVEENCRYPTION**.
   Por exemplo, emita o seguinte comando:

   ```
   define devclass 3592_encrypt library=3584 devtype=3592 driveencryption=on
   ```

3. Defina um storage pool.

Por exemplo, emita o seguinte comando:

```
define stgpool 3592_encrypt_pool 3592_encrypt
```

O que Fazer Depois

Para desativar qualquer método de criptografia em novos volumes, configure o parâmetro **DRIVEENCRYPTION** como 0FF. Se o hardware estiver configurado para criptografar dados por meio do método biblioteca ou do sistema e o **DRIVEENCRYPTION** estiver configurado como 0FF, as operações de backup falharão.

Configurando o compartilhamento de biblioteca

Múltiplos servidores do IBM Spectrum Protect podem compartilhar dispositivos de armazenamento usando uma rede de área de armazenamento (SAN). Configure um servidor como o gerenciador de biblioteca e os outros servidores como clientes de biblioteca.

Antes de Iniciar

Assegure-se de que seus sistemas atendam aos requisitos de licenciamento para compartilhamento de biblioteca. Uma autorização para IBM Spectrum Protect for SAN é necessária para cada servidor do IBM Spectrum Protect que estiver configurado como um cliente de biblioteca ou como um gerenciador de biblioteca em um ambiente SAN.

Sobre Esta Tarefa

Com a movimentação de dados sem a LAN, os sistemas do cliente do IBM Spectrum Protect podem acessar diretamente dispositivos de armazenamento que estiverem definidos para um servidor do IBM Spectrum Protect. Os agentes de armazenamento são instalados e configurados nos sistemas do cliente para executar a movimentação de dados.

Para configurar o compartilhamento de biblioteca, deve-se definir um servidor do IBM Spectrum Protect como o gerenciador de biblioteca para sua configuração de biblioteca compartilhada. Em seguida, defina outros servidores IBM Spectrum Protect como clientes de biblioteca, que se comunicam e solicitam recursos de armazenamento do gerenciador de biblioteca. O servidor do gerenciador de biblioteca deve estar na mesma versão ou em uma versão mais recente que o servidor ou servidores que estiverem definidos como clientes de biblioteca.

Procedimento

Para concluir as etapas a seguir para compartilhar recursos da biblioteca em uma SAN entre servidores do IBM Spectrum Protect, conclua as etapas a seguir:

1. Configure as comunicações entre servidores.

   Para compartilhar um dispositivo de armazenamento em uma SAN, defina os servidores entre si usando a função de definição cruzada. Cada servidor deve ter um nome exclusivo.
2. Defina uma biblioteca compartilhada e configure dispositivos de fita nos sistemas do servidor.

   Use o procedimento que está descrito em “Configurando bibliotecas para uso por um servidor” na página 87 para definir uma biblioteca para uso no ambiente compartilhado. Modifique o procedimento para definir a biblioteca como compartilhada, especificando o parâmetro **SHARED=YES** para o comando **DEFINE LIBRARY**.
3. Defina o servidor do gerenciador de bibliotecas.
4. Defina a biblioteca compartilhada no servidor que é o cliente de biblioteca.
5. No servidor do gerenciador de bibliotecas, defina os caminhos do cliente de biblioteca para cada unidade que o cliente de biblioteca possa acessar.

   O nome do dispositivo deve refletir o caminho no qual o sistema do cliente de biblioteca reconhece o dispositivo de fita. Um caminho do gerenciador de biblioteca para cada unidade de fita deve ser definido para que o cliente da biblioteca use a unidade.

Para evitar problemas, certifique-se de que todas as definições de caminho da unidade que são especificadas para o gerenciador de biblioteca também sejam especificadas para cada cliente de biblioteca.

Por exemplo, se o gerenciador de biblioteca definir três unidades de fita, o cliente de biblioteca também deverá definir três unidades de fita. Para limitar o número de unidades de fita que um cliente de biblioteca pode usar em um momento, use o parâmetro **MOUNTLIMIT** da classe de dispositivo no cliente de biblioteca.

6. Defina classes de dispositivo para a biblioteca compartilhada.

   O método preferencial é tornar os nomes de classe de dispositivo iguais em ambos os servidores para evitar confusão quando definir múltiplas classes de dispositivo com o mesmo tipo de dispositivo e parâmetros de biblioteca. Algumas operações, como backup de banco de dados, usam o nome da classe de dispositivo para identificar os dados para backup.

   Os parâmetros de classe de dispositivo que estiverem especificados no gerenciador de biblioteca substituem os parâmetros que estiverem especificados para o cliente de biblioteca. Se os nomes de classe de dispositivo forem diferentes, o gerenciador de biblioteca utilizará os parâmetros que estiverem especificados em uma classe de dispositivo que corresponderem ao tipo de dispositivo que estiver especificado para o cliente de biblioteca.
7. Defina um conjunto de armazenamentos para a biblioteca compartilhada.
8. Repita as etapas para configurar outro servidor como um cliente de biblioteca.

Informações relacionadas

DEFINE DEVCLASS (Definir uma Classe de Dispositivo)
DEFINE LIBRARY (Definir uma biblioteca)
DEFINE STGPOOL (definir um volume em um conjunto de armazenamentos)

Linux AIX Exemplo: compartilhamento de exemplo para servidores AIX e Linux

Para saber como configurar um ambiente de compartilhamento de biblioteca SCSI para servidores que são executados em sistemas AIX ou Linux, revise o procedimento de amostra.

Sobre Esta Tarefa

Neste exemplo, um servidor do gerenciador de bibliotecas chamado ASTRO e um cliente de biblioteca chamado JUDY são configurados. Para ajudar a esclarecer o local em que cada etapa é executada, os comandos são precedidos pelo nome do servidor no qual o comando é emitido. A maioria dos comandos é emitida no cliente de biblioteca.

Para bibliotecas SCSI, defina a biblioteca especificando o parâmetro **libtype=scsi**.

Procedimento

1. Para configurar ASTRO como o servidor do gerenciador de bibliotecas, defina uma biblioteca SCSI compartilhada denominada SANGROUP.

   Por exemplo:

   ```
   astro> define library sangroup libtype=scsi shared=yes
   ```

   Em seguida, conclua o restante das etapas conforme descrito em Exemplo: configure uma biblioteca SCSI ou Virtual Tape Library com um tipo de dispositivo de unidade único para configurar a biblioteca.

   Dica: É possível usar o comando **PERFORM LIBACTION** para definir unidades e caminhos para uma biblioteca em uma etapa.
2. Defina ASTRO como o servidor gerenciador de biblioteca emitindo o comando **DEFINE SERVER**.

   ```
   judy> define server astro serverpassword=secret hladdress=192.0.2.24
    lladdress=1777 crossdefine=yes
   ```

3. Defina o SANGROUP de biblioteca compartilhada emitindo o comando **DEFINE LIBRARY**. Deve-se usar o nome do servidor do gerenciador de biblioteca no parâmetro **PRIMARYLIBMANAGER** e usar LIBTYPE=SHARED.

```
judy> define library sangroup libtype=shared primarylibmanager=astro
```

   Assegure-se de que o nome da biblioteca seja igual ao nome da biblioteca no gerenciador de biblioteca.
4. Defina caminhos do gerenciador de biblioteca, ASTRO, para duas unidades na biblioteca compartilhada emitindo o comando **DEFINE PATH**.

```
AIX astro> define path judy drivea srctype=server desttype=drive
 library=sangroup device=/dev/rmt6
astro> define path judy driveb srctype=server desttype=drive
 library=sangroup device=/dev/rmt7
```

```
Linux astro> define path judy drivea srctype=server desttype=drive
 library=sangroup device=/dev/IBMtape6
astro> define path judy driveb srctype=server desttype=drive
 library=sangroup device=/dev/IBMtape7
```

5. Defina todas as classes de dispositivo que estiverem associadas à biblioteca compartilhada.

```
AIX judy> define devclass tape library=sangroup devtype=lto
```

```
Linux judy> define devclass tape library=sangroup devtype=lto
```

   Os parâmetros a seguir para a definição de classe de dispositivo devem ser os mesmos no cliente de biblioteca e no gerenciador de biblioteca:

   - **BIBLIOTECA**
   - **DRIVEENCRYPTION**
   - **WORM**
   - **FORMAT**
6. Defina um conjunto de armazenamentos que é chamado BACKTAPE para uso da biblioteca compartilhada. Emita o comando **DEFINE STGPOOL**.

```
judy> define stgpool backtape tape maxscratch=50
```

O que Fazer Depois

Repita o procedimento para definir mais clientes de biblioteca para seu gerenciador de biblioteca.

Informações relacionadas

DEFINE DEVCLASS (Definir uma Classe de Dispositivo)

DEFINE DRIVE (Definir uma Unidade para uma Biblioteca)

DEFINE LIBRARY (Definir uma biblioteca)

DEFINE PATH (Definir um caminho)

DEFINE STGPOOL (definir um volume em um conjunto de armazenamentos)

Windows Exemplo: compartilhamento de biblioteca para servidores Windows

Para saber como configurar um ambiente de compartilhamento de bibliotecas para servidores que são executados em sistemas Windows, revise o procedimento de amostra.

Sobre Esta Tarefa

Neste exemplo, um servidor do gerenciador de bibliotecas chamado ASTRO e um cliente de biblioteca chamado JUDY são configurados.

Para bibliotecas SCSI, defina a biblioteca especificando o parâmetro **libtype=scsi**.

Windows Configurando o servidor do gerenciador de bibliotecas

Deve-se configurar o servidor do gerenciador de bibliotecas para configurar os servidores do IBM Spectrum Protect para compartilhar dispositivos conectados ao SAN.

Procedimento

O procedimento a seguir é um exemplo de como configurar um servidor do IBM Spectrum Protect que é denominado ASTRO como um gerenciador de biblioteca:

1. Assegure-se de que o servidor do gerenciador de bibliotecas esteja em execução:
   a) Inicie o Console de Gerenciamento de Serviços do Windows (services.msc).
   b) Selecione o serviço. Por exemplo, TSM `Server1`.
   c) Se o serviço não estiver em execução, clique com o botão direito no nome do serviço e clique em **Iniciar**.
2. Obtenha as informações da biblioteca e da unidade para o dispositivo de biblioteca compartilhada:
   a) Execute o utilitário `tsmdlst.exe`. O utilitário está no diretório `\Program Files\Tivoli\TSM \server`.
3. Defina uma biblioteca cujo tipo de biblioteca seja SCSI.

   Por exemplo:

   ```
   define library sangroup libtype=scsi shared=yes
   ```

   Este exemplo usa o padrão para o número de série da biblioteca, que é fazer com que o próprio servidor obtenha o número de série da biblioteca no momento em que o caminho é definido. Dependendo dos recursos da biblioteca, o servidor pode não conseguir detectar automaticamente o número de série. Neste caso, o servidor não registra um número de série para o dispositivo e é incapaz de confirmar a identidade do dispositivo quando você define o caminho ou quando o servidor usa o dispositivo.
4. Defina o caminho do servidor para a biblioteca.

   ```
   define path astro sangroup srctype=server desttype=library
    device=lb0.0.0.2
   ```

   Se você não incluiu o número de série quando definiu a biblioteca, o servidor agora consultará a biblioteca para obter esta informação. Se você incluiu o número de série quando definiu a biblioteca, o servidor verificará que você definiu e emitirá uma mensagem se houver uma incompatibilidade.
5. Defina as unidades na biblioteca.

   ```
   define drive sangroup drivea
   define drive sangroup driveb
   ```

   Este exemplo usa o padrão para o número de série da unidade, que é fazer com que o servidor obtenha o próprio número de série da unidade no momento em que o caminho é definido. Dependendo dos recursos da unidade, o servidor pode não conseguir detectar automaticamente o número de série. Neste caso, o servidor não registra um número de série para o dispositivo e é incapaz de confirmar a identidade do dispositivo quando você define o caminho ou quando o servidor usa o dispositivo.

   Este exemplo também utiliza o padrão para o endereço do elemento da unidade, que é fazer com que o próprio servidor obtenha o número do elemento da unidade no momento em que o caminho é definido.

   O endereço do elemento é um número que indica a localização física de uma unidade dentro de uma biblioteca automatizada. O servidor precisa do endereço do elemento para conectar o local físico da unidade ao endereço SCSI da unidade. É possível fazer com que o próprio servidor obtenha o número do elemento da unidade no momento em que o caminho é definido ou especificar o número do elemento quando definir a unidade.

Dependendo dos recursos da biblioteca, o servidor pode não conseguir detectar automaticamente o endereço do elemento. Neste caso, deve-se fornecer o endereço do elemento ao definir a unidade. Os números de elemento para muitas bibliotecas estão disponíveis em IBM Support Portal for IBM Spectrum Protect.

6. Defina o caminho do servidor para cada uma das unidades.

```
define path astro drivea srctype=server desttype=drive library=sangroup
 device=mt0.1.0.2
define path astro driveb srctype=server desttype=drive library=sangroup
 device=mt0.2.0.2
```

Se você não incluiu o número de série ou o endereço do elemento quando definiu a unidade, o servidor agora consultará a unidade ou a biblioteca para obter esta informação.

7. Defina pelo menos uma classe de dispositivo.

```
define devclass tape devtype=dlt library=sangroup
```

8. Efetue check-in do inventário de biblioteca. O exemplo a seguir efetua check-in de todos os volumes no inventário de biblioteca como volumes utilizáveis. O servidor utiliza o nome na etiqueta de código de barras como o nome do volume.

```
checkin libvolume sangroup search=yes status=scratch
 checklabel=barcode
```

9. Configure um conjunto de armazenamentos para a biblioteca compartilhada com um máximo de 50 volumes utilizáveis.

```
define stgpool backtape tape
 description='storage pool for shared sangroup' maxscratch=50
```

Informações relacionadas

CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)
DEFINE DEVCLASS (Definir uma Classe de Dispositivo)
DEFINE DRIVE (Definir uma Unidade para uma Biblioteca)
DEFINE LIBRARY (Definir uma biblioteca)
DEFINE PATH (Definir um caminho)
DEFINE STGPOOL (definir um volume em um conjunto de armazenamentos)

Windows Configurando os servidores clientes de biblioteca

Deve-se configurar um ou mais servidores clientes de biblioteca para configurar os servidores do IBM Spectrum Protect para compartilhar dispositivos conectados ao SAN.

Antes de Iniciar

Assegure-se de que um servidor do gerenciador de bibliotecas esteja definido.

Sobre Esta Tarefa

Deve-se definir o servidor do gerenciador de bibliotecas. Utilize o procedimento a seguir como um exemplo de como configurar um servidor do IBM Spectrum Protect que é denominado JUDY como um cliente de biblioteca.

Procedimento

1. Assegure-se de que o servidor do gerenciador de bibliotecas esteja em execução:
   a) Inicie o Console de Gerenciamento de Serviços do Windows (services.msc).
   b) Selecione o serviço. Por exemplo, TSM Server1.
   c) Se o serviço não estiver em execução, clique com o botão direito e selecione **Iniciar**.
2. Obtenha as informações da biblioteca e da unidade para o dispositivo de biblioteca compartilhada:

a) Execute o utilitário `tsmdlst.exe`. O utilitário está no diretório `\Program Files\Tivoli\TSM \server`.

3. Defina a biblioteca compartilhada, SANGROUP e identifique o gerenciador de biblioteca. Assegure-se de que o nome da biblioteca seja igual ao nome da biblioteca no gerenciador de biblioteca.

```
define library sangroup libtype=shared primarylibmanager=astro
```

4. Defina os caminhos do servidor cliente de biblioteca para cada uma das unidades emitindo comandos no cliente administrativo:

```
define path judy drivea srctype=server desttype=drive library=sangroup
 device=mt0.1.0.3
 define path judy driveb srctype=server desttype=drive library=sangroup
 device=mt0.2.0.3
```

5. Defina pelo menos uma classe de dispositivo emitindo comandos a partir do cliente de biblioteca:

```
define devclass tape devtype=dlt mountretention=1 mountwait=10
library=sangroup
```

   Configure os parâmetros para a classe de dispositivo o mesmo no cliente de biblioteca como no gerenciador de biblioteca. Tornar os nomes de classe de dispositivo iguais em ambos os servidores também é uma boa prática, mas não é necessário.

   Os parâmetros de classe de dispositivo que são especificados no servidor do gerenciador de bibliotecas substituem aqueles especificados para o cliente de biblioteca. Isso se aplicará, independentemente se os nomes de classe de dispositivo forem os mesmos em ambos os servidores ou não. Se os nomes de classe de dispositivo forem diferentes, o gerenciador de biblioteca utilizará os parâmetros especificados em uma classe de dispositivo que corresponder ao tipo de dispositivo especificado para o cliente de biblioteca.

   Se um cliente de biblioteca requerer uma configuração que é diferente da que estiver especificada na classe de dispositivo do gerenciador de biblioteca (por exemplo, um limite de montagem diferente), conclua as etapas a seguir:

   a. Crie uma classe de dispositivo adicional no servidor do gerenciador de bibliotecas. Especifique as configurações de parâmetro que você deseja que o cliente de biblioteca utilize.

   b. Crie uma classe de dispositivo no cliente da biblioteca com o mesmo nome e tipo de dispositivo que a nova classe de dispositivo que foi criada no servidor de bibliotecas.

6. Defina o conjunto de armazenamentos, BACKTAPE, que usará a biblioteca compartilhada:

```
define stgpool backtape tape
description='storage pool for shared sangroup' maxscratch=50
```

7. Repita este procedimento para definir servidores adicionais como clientes de biblioteca.

Informações relacionadas

DEFINE DEVCLASS (Definir uma Classe de Dispositivo)
DEFINE LIBRARY (Definir uma biblioteca)
DEFINE PATH (Definir um caminho)
DEFINE STGPOOL (definir um volume em um conjunto de armazenamentos)

Configurando uma hierarquia do conjunto de armazenamentos

Como parte do processo de implementação, você deve configurar uma hierarquia do conjunto de armazenamentos. Configure pelo menos um conjunto de armazenamentos primários no disco e um conjunto de armazenamentos primários na fita. Certifique-se de que os dados sejam migrados do disco para a fita diariamente.

Antes de Iniciar

1. Certifique-se de ter revisado as informações em "Planejando a hierarquia do conjunto de armazenamentos" na página 21.
2. Certifique-se de que as regras apropriadas, também conhecidas como *políticas*, sejam especificadas para fazer backup de dados do cliente. Siga as instruções em "Especificando regras para backup e arquivamento de dados de cliente" na página 107.
3. Certifique-se de que uma política esteja designada a cada nó. Para obter instruções sobre como designar uma política ao registrar um nó, consulte "Registrando clientes" na página 112.

Procedimento

Para configurar uma hierarquia do conjunto de armazenamentos, conclua as seguintes etapas:

1. Defina um conjunto de armazenamentos primários para o dispositivo de fita emitindo o comando **DEFINE STGPOOL**.

   Por exemplo, defina um conjunto de armazenamentos primários, TAPE1, com uma classe de dispositivo de LTO, e ative a disposição de grupo. Configure o número máximo de volumes utilizáveis que o servidor pode solicitar para esse conjunto de armazenamentos como 999. Emita o seguinte comando:

   ```
   define stgpool tape1 lto pooltype=primary collocate=group
   maxscratch=999
   ```

2. Defina as unidades, caminhos e bibliotecas para o conjunto de armazenamentos primários em fita. Siga as instruções em "Definindo dispositivos de fita" na página 88.
3. Defina um conjunto de armazenamentos primários para o dispositivo de disco emitindo o comando **DEFINE STGPOOL**.

   Por exemplo, defina um conjunto de armazenamentos, DISK1, com uma classe de dispositivo de FILE. Certifique-se de que os dados possam ser migrados para o conjunto de armazenamento em fita, TAPE1, mas evite a migração automática especificando 100 para o parâmetro **HIGHMIG** e 0 para o parâmetro **LOWMIG**. Evite a recuperação especificando 100 para o parâmetro **RECLAIM**. Ative a disposição de nó. Configure o número máximo de volumes utilizáveis que o servidor pode solicitar para esse conjunto de armazenamentos como 9999. Use o parâmetro **MIGPROCESS** para especificar o número de processos de migração. O valor do parâmetro **MIGPROCESS** deve ser igual ao número de unidades na biblioteca menos o número de unidades que são reservadas para operações de restauração. Emita o seguinte comando:

   ```
   define stgpool disk1 file pooltype=primary nextstgpool=tape1
   highmig=100 lowmig=0 reclaim=100 collocate=node maxscratch=9999 migprocess=5
   ```

   Para obter informações adicionais sobre como configurar a migração de disco para fita, consulte Migrar conjuntos de armazenamentos em disco.

O que Fazer Depois

Uma hierarquia do conjunto de armazenamentos inclui apenas conjuntos de armazenamentos primários. Depois de configurar a hierarquia do conjunto de armazenamentos, conclua as seguintes etapas:

1. Crie um conjunto de armazenamento de cópia em um dispositivo de fita. Para obter instruções, consulte DEFINE STGPOOL (Definir um conjunto de armazenamento de cópia designado a dispositivos de acesso sequencial).
2. Faça backup do conjunto de armazenamentos primários baseado em fita para o conjunto de armazenamento de cópia usando o comando **BACKUP STGPOOL**. Para obter instruções, consulte BACKUP STGPOOL (fazer backup dos dados do conjunto de armazenamentos primários para o conjunto de armazenamentos de cópia).
3. Para assegurar que os dados possam ser recuperados em um desastre, configure um procedimento para mover volumes de fita do conjunto de armazenamento de cópia para um local externo. Para obter

instruções, consulte “Preparando para um desastre e recuperando-se de um desastre usando o DRM” na página 212.

Informações relacionadas

CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)

DEFINE STGPOOL (definir um volume em um conjunto de armazenamentos)

Protegendo aplicativos e sistemas

O servidor protege dados para clientes, que podem incluir aplicativos, máquinas virtuais e sistemas.

Incluindo clientes

Após a configuração bem-sucedida do servidor IBM Spectrum Protect, instale e configure o software cliente para iniciar o backup de dados.

Sobre Esta Tarefa

O procedimento descreve as etapas básicas para a inclusão de um cliente. Para obter instruções mais específicas sobre como configurar clientes, consulte a documentação para o produto instalado no nó cliente. É possível ter os seguintes tipos de nós clientes:

Nós clientes do aplicativo

Os nós clientes do aplicativo incluem servidores de email, bancos de dados e outros aplicativos. Por exemplo, qualquer um dos seguintes aplicativos pode ser um nó cliente do aplicativo:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- Ambientes IBM Spectrum Protect for Virtual

Nós clientes do sistema

Os nós clientes do sistema incluem estações de trabalho, servidores de arquivos de armazenamento conectado à rede (NAS) e clientes da API.

Nós clientes de máquina virtual

Os nós clientes de máquina virtual consistem em um host convidado individual em um hypervisor. Cada máquina virtual é representada como um espaço no arquivo.

Procedimento

Para incluir um cliente, conclua as etapas a seguir:

1. Selecione o software a ser instalado no nó cliente e planeje a instalação. Siga as instruções em “Selecionando o software cliente e planejando a instalação” na página 106.
2. Especifique como fazer backup e arquivar dados de cliente. Siga as instruções em “Especificando regras para backup e arquivamento de dados de cliente” na página 107.
3. Especifique quando fazer backup e arquivar dados de cliente. Siga as instruções em “Planejando operações de backup e archive” na página 111.
4. Para permitir que o cliente se conecte ao servidor, registre o cliente. Siga as instruções em “Registrando clientes” na página 112.
5. Para começar a proteger um nó cliente, instale e configure o software selecionado no nó cliente. Siga as instruções em “Instalando e configurando clientes” na página 112.

Selecionando o software cliente e planejando a instalação

Diferentes tipos de dados requerem diferentes tipos de proteção. Identifique o tipo de dados que devem ser protegidos e selecione o software apropriado.

Sobre Esta Tarefa

A prática preferencial é instalar o cliente de backup-archive em todos os nós clientes para que seja possível configurar e iniciar o client acceptor no nó cliente. O client acceptor é projetado para executar operações planejadas de forma eficiente.

O client acceptor executa planejamentos para os produtos a seguir: o cliente de backup-archive, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail e Ambientes IBM Spectrum Protect for Virtual. Se você instalar um produto para o qual o client acceptor não executa planejamentos, deverá seguir as instruções de configuração na documentação do produto para assegurar que as operações planejadas possam ocorrer.

Procedimento

Com base em seu objetivo, selecione o produto a ser instalado e revise as instruções de instalação.

Dica: Se você instalar o software cliente agora, também deverá concluir as tarefas de configuração do cliente que estão descritas em "Instalando e configurando clientes" na página 112 antes de poder usar o cliente.

Objetivo	Produto e descrição	Instruções de instalação
Proteger um servidor de arquivos ou estação de trabalho	O cliente de backup-archive faz backup e arquiva os arquivos e diretórios de servidores de arquivos e estações de trabalho para armazenamento. Também é possível restaurar e recuperar versões de backup e cópias de arquivos arquivadas.	• Requisitos do Ambiente do Cliente • Instale deus clientes de archive de backup do UNIX e do Linux • Instalando o cliente Windows pela primeira vez
Proteger aplicativos com recursos de backup e restauração de captura instantânea	O IBM Spectrum Protect Snapshot protege dados com recursos integrados de backup e restauração de captura instantânea direcionados ao aplicativo. É possível proteger dados que são armazenados pelo IBM Db2 software de banco de dados e aplicativos SAP, Oracle, Microsoft Exchange e Microsoft SQL Server.	• Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot para UNIX e Linux • Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot for VMware • Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot for Windows
Proteja um aplicativo de e-mail em um servidor IBM Domino	O IBM Spectrum Protect for Mail: Data Protection for IBM Domino automatiza a proteção de dados para que os backups sejam concluídos sem encerrar servidores IBM Domino.	• Instalação do Data Protection for IBM Domino em um sistema UNIX, AIX ou Linux (V7.1.0) • Instalação do Data Protection for IBM Domino em um sistema Windows (V7.1.0)
Proteja um aplicativo de e-mail em um servidor Microsoft Exchange	O IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server automatiza a proteção de dados para que os backups sejam concluídos sem encerrar servidores Microsoft Exchange.	Instalando, fazendo upgrade e migrando o IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
Proteja um banco de dados do Db2	A interface de programação de aplicativos (API) do cliente de backup e archive pode ser usada para fazer backup de dados do Db2 para o servidor IBM Spectrum Protect.	Instalando os clientes de backup e archive do IBM Spectrum Protect (UNIX, Linux e Windows)

Objetivo	Produto e descrição	Instruções de instalação
Proteja um banco de dados IBM Informix	A API do cliente de backup-archive pode ser usada para fazer backup de dados do Informix no servidor IBM Spectrum Protect.	Instalando os clientes de backup e archive do IBM Spectrum Protect (UNIX, Linux e Windows)
Proteja um banco de dados Microsoft SQL	O IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server protege dados do Microsoft SQL.	Instalando o Data Protection for SQL Server no Núcleo do Sistema Windows
Proteger um banco de dados Oracle	O IBM Spectrum Protect for Databases: Data Protection for Oracle protege dados do Oracle.	Instalação do Data Protection for Oracle
Proteger um ambiente SAP	O IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP fornece proteção customizada para ambientes SAP. O produto foi projetado para melhorar a disponibilidade de servidores de banco de dados SAP e reduzir a carga de trabalho de administração.	• Instalando a proteção de dados para o SAP para Db2 • Instalando o Data Protection for SAP for Oracle
Proteger uma máquina virtual	O Ambientes IBM Spectrum Protect for Virtual fornece proteção que é customizada para ambientes virtuais Microsoft Hyper-V e VMware. É possível usar o Ambientes IBM Spectrum Protect for Virtual para criar backups incrementais contínuos que estão armazenados e um servidor centralizado, criar políticas de backup e restaurar máquinas virtuais ou arquivos individuais. Como alternativa, use o cliente de backup-archive para fazer backup e restaurar uma máquina virtual integral do VMware ou Microsoft Hyper-V. Também é possível fazer backup e restaurar arquivos ou diretórios a partir de uma máquina virtual VMware.	• Instalando e fazendo upgrade do Data Protection for Microsoft Hyper-V • Instalando e fazendo upgrade do Data Protection for VMware • Instalando os clientes de backup e archive do IBM Spectrum Protect (UNIX, Linux e Windows)

Dica: Para usar o cliente para gerenciamento de espaço, é possível instalar o IBM Spectrum Protect for Space Management ou o IBM Spectrum Protect HSM for Windows.

Especificando regras para backup e arquivamento de dados de cliente

Antes de incluir um cliente, assegure-se de que as regras sejam especificadas para operações de backup e archive para os dados de cliente. Durante o processo de registro do cliente, você atribua o nó cliente a um domínio de política, que tem as regras que controlam como e quando os dados de cliente são armazenados.

Antes de Iniciar

Determine como continuar:

- Se estiver familiarizado com as políticas que estão configuradas para sua solução e souber que elas não requerem mudanças, continue com “Planejando operações de backup e archive” na página 111.
- Se não estiver familiarizado com as políticas, siga as etapas nesse procedimento.

Sobre Esta Tarefa

As políticas afetam a quantidade de dados que são armazenados ao longo do tempo e por quanto tempo os dados ficam retidos e disponíveis para restauração. Para atender aos objetivos de proteção de dados, é possível atualizar a política padrão e criar suas próprias políticas. Uma política inclui as seguintes regras:

- Como e quando os arquivos são submetidos a backup e arquivados no armazenamento do servidor.
- O número de cópias de um arquivo e o período pelo qual as cópias são mantidas no armazenamento do servidor.

Durante o processo de registro do cliente, você designa um cliente a um *domínio de política*. A política para um cliente específico é determinada pelas regras no domínio de política ao qual o cliente está designado. No domínio de política, as regras que estão em vigor estão no *conjunto de políticas* ativas.

Quando um cliente faz backup ou arquiva um arquivo, o arquivo é ligado a uma classe de gerenciamento no conjunto de políticas ativas do domínio de política. Uma *classe de gerenciamento* é o conjunto de chaves de regras para gerenciar dados de cliente. As operações de backup e archive no cliente usam as configurações na classe de gerenciamento padrão do domínio de política, a menos que você customize ainda mais a política. Uma política pode ser customizada definindo mais classes de gerenciamento e designando seu uso por meio de opções do cliente.

As opções do cliente podem ser especificadas em um arquivo local, editável no sistema do cliente e em um conjunto de opções do cliente no servidor. As opções no conjunto de opções do cliente no servidor podem substituir ou incluir nas opções no arquivo de opções do cliente local.

Procedimento

1. Revise as políticas que estão configuradas para sua solução seguindo as instruções em "Visualizando políticas" na página 108.
2. Se precisar fazer pequenas mudanças para atender aos requisitos de retenção de dados, siga as instruções em "Editando políticas" na página 109.
3. Opcional: Se precisar criar domínios de política ou fazer mudanças extensivas nas políticas para atender aos requisitos de retenção de dados, consulte Customizando políticas.

Visualizando políticas

Visualize políticas para determinar se elas devem ser editadas para atender às suas necessidades.

Procedimento

1. Para visualizar o conjunto de políticas ativas para um domínio de política, conclua as etapas a seguir:
   a) Na página **Serviços** do Operations Center, selecione um domínio de política e clique em **Detalhes**.
   b) Na página **Resumo** do domínio de política, clique na guia **Conjuntos de políticas**.

      Dica: Para ajudar a assegurar que seja possível recuperar dados após um ataque de ransomware, aplique as seguintes diretrizes:

      - Assegure-se de que o valor na coluna Backups seja no mínimo de 2. O valor preferencial é 3, 4 ou mais.
      - Assegure-se de que o valor na coluna Manter backups extras seja no mínimo de 14 dias. O valor preferencial é 30 ou mais dias.
      - Assegure-se de que o valor na coluna Manter archives seja no mínimo de 30 dias.

      Se o software IBM Spectrum Protect for Space Management está instalado no cliente, assegure-se de que os dados sejam submetidos a backup antes de migrá-lo. No comando **DEFINE MGMTCLASS** ou **UPDATE MGMTCLASS**, especifique **MIGREQUIRESBKUP=YES**. Em seguida, siga as diretrizes na dica.
2. Para visualizar conjuntos de políticas inativas para um domínio de política, conclua as seguintes etapas:

a) Na página **Conjuntos de políticas**, clique na alternância **Configurar**. Agora é possível visualizar e editar os conjuntos de políticas que estão inativas.

b) Role pelos conjuntos de políticas inativas usando as setas para avançar e voltar. Ao visualizar um conjunto de políticas inativas, as configurações que diferenciam o conjunto de políticas inativas do conjunto de políticas ativas são destacadas.

c) Clique na alternância **Configurar**. Os conjuntos de políticas não são mais editáveis.

Editando políticas

Para alterar as regras que se aplicam a um domínio de política, edite o conjunto de políticas ativas para o domínio de política. Também é possível ativar um conjunto de políticas diferente para um domínio.

Antes de Iniciar

As mudanças na política podem afetar a retenção de dados. Certifique-se de continuar fazendo backup de dados que são essenciais para sua organização para que seja possível restaurar esses dados se ocorrer um desastre. Além disso, certifique-se de que seu sistema tenha espaço de armazenamento suficiente para operações de backup planejadas.

Sobre Esta Tarefa

Edite um conjunto de políticas alterando uma ou mais classes de gerenciamento no conjunto de políticas. Se editar o conjunto de políticas ativas, as mudanças não estarão disponíveis para os clientes, a menos que você reative o conjunto de políticas. Para disponibilizar o conjunto de políticas editadas para os clientes, ative o conjunto de políticas.

Embora seja possível definir vários conjuntos de políticas para um domínio de política, apenas um conjunto de políticas pode estar ativo. Ao ativar um conjunto de políticas diferente, ele substitui o conjunto de políticas ativas atualmente.

Para saber sobre práticas preferenciais para definir políticas, consulte Customizando políticas.

Procedimento

1. Na página **Serviços** do Operations Center, selecione um domínio de política e clique em **Detalhes**.
2. Na página **Resumo** do domínio de política, clique na guia **Conjuntos de políticas**.

   A página **Conjuntos de políticas** indica o nome do conjunto de políticas ativas e lista todas as classes de gerenciamento para esse conjunto de políticas.
3. Clique na alternância **Configurar**. O conjunto de políticas é editável.
4. Para editar um conjunto de políticas que não está ativo, clique nas setas avançar e voltar para localizar o conjunto de políticas.
5. Edite o conjunto de políticas concluindo qualquer uma das seguintes ações:

Opção	Descrição
Incluir uma classe de gerenciamento	a. Na tabela Conjuntos de políticas, clique em **+Classe de gerenciamento**. b. Para especificar as regras para fazer backup e arquivar dados, preencha os campos na janela **Incluir classe de gerenciamento**. c. Para tornar a classe de gerenciamento a classe de gerenciamento padrão, selecione a caixa de seleção **Tornar padrão**. d. Clique em **Incluir**.
Excluir uma classe de gerenciamento	Na coluna Classe de gerenciamento, clique em **-**. **Dica:** Para excluir a classe de gerenciamento padrão, primeiro você deve designar uma classe de gerenciamento diferente como o padrão.

Opção	Descrição
Tornar uma classe de gerenciamento a classe de gerenciamento padrão	Na coluna Padrão para a classe de gerenciamento, clique no botão de opções. **Dica:** A classe de gerenciamento padrão gerencia arquivos do cliente quando outra classe de gerenciamento não está designada ou não é apropriada para gerenciar um arquivo. Para assegurar que os clientes sempre possam fazer backup e arquivar arquivos, escolha uma classe de gerenciamento padrão que contenha regras para fazer backup e arquivar arquivos.
Modificar uma classe de gerenciamento	Para alterar as propriedades de uma classe de gerenciamento, atualize os campos na tabela.

6. Clique em **Salvar**.

   Atenção: Ao ativar um novo conjunto de políticas, os dados podem ser perdidos. Os dados que estão protegidos em um conjunto de políticas podem não ser protegidos em outro conjunto de políticas. Portanto, antes de ativar um conjunto de políticas, certifique-se de que as diferenças entre o conjunto de políticas anterior e o novo conjunto de políticas não causem perda de dados.
7. Clique em **Ativar**. É exibido um resumo das diferenças entre o conjunto de políticas ativas e o novo conjunto de políticas. Certifique-se de que as mudanças no novo conjunto de políticas sejam consistentes com seus requisitos de retenção de dados, concluindo as etapas a seguir:
   a) Revise as diferenças entre as classes de gerenciamento correspondentes nos dois conjuntos de políticas e considere as consequências para arquivos do cliente. Os arquivos do cliente que estão ligados às classes de gerenciamento no conjunto de políticas ativas serão ligados às classes de gerenciamento com os mesmos nomes no novo conjunto de políticas.
   b) Identifique classes de gerenciamento no conjunto de políticas ativas que não possuem contrapartes no novo conjunto de políticas e considere as consequências para arquivos do cliente. Os arquivos do cliente que estão ligados a essas classes de gerenciamento serão gerenciados pela classe de gerenciamento padrão no novo conjunto de políticas.
   c) Se as mudanças a serem implementadas pelo conjunto de políticas forem aceitáveis, selecione a caixa de seleção **Entendo que essas atualizações podem causar perda de dados** e clique em **Ativar**.

Modificando o escopo de um backup de cliente

Ao configurar operações de backup do cliente, a prática preferencial é excluir objetos desnecessários. Por exemplo, geralmente você deseja excluir arquivos temporários de uma operação de backup.

Sobre Esta Tarefa

Ao excluir objetos desnecessários de operações de backup, você obtém melhor controle da quantidade de espaço de armazenamento necessário para operações de backup e do custo de armazenamento. Dependendo de seu pacote de licenciamento, também é possível limitar custos de licenciamento.

Procedimento

Como você modifica o escopo de operações de backup depende do produto que está instalado no nó cliente:

- Para um cliente de backup-archive, é possível criar uma lista de inclusão/exclusão para incluir ou excluir um arquivo, grupos de arquivos ou diretórios de operações de backup. Para criar uma lista de inclusão/exclusão, siga as instruções em Criando uma Lista de Inclusão-Exclusão.

  Para assegurar o uso consistente de uma lista de inclusão/exclusão para todos os clientes de um tipo, é possível criar um conjunto de opções do cliente no servidor que contenha as opções necessárias. Em seguida, designe o conjunto de opções do cliente a cada um dos clientes do mesmo tipo. Para obter

detalhes, consulte a seção Controlando operações do cliente através dos conjuntos de opções do cliente.

- Para um cliente de backup-archive, é possível especificar os objetos a serem incluídos em uma operação de backup incremental usando a opção **domain**. Siga as instruções em Opção de domínio.
- Para outros produtos, para definir quais objetos são incluídos em e excluídos das operações de backup, siga as instruções na documentação do produto.

Planejando operações de backup e archive

Antes de registrar um novo cliente no servidor, certifique-se de que um planejamento esteja disponível para especificar quando ocorrerão as operações de backup e archive. Durante o processo de registro, você designa um planejamento ao cliente.

Antes de Iniciar

Determine como continuar:

- Se estiver familiarizado com os planejamentos que estão configurados para a solução e souber que eles não requerem modificação, continue com "Registrando clientes" na página 112.
- Se não estiver familiarizado com os planejamentos ou os planejamentos precisarem de modificação, siga as etapas nesse procedimento.

Sobre Esta Tarefa

Geralmente as operações de backup para todos os clientes devem ser concluídas diariamente. Planeje as cargas de trabalho do cliente e do servidor para atingir o melhor desempenho para o seu ambiente de armazenamento. Para evitar a sobreposição de operações do cliente e do servidor, considere planejar operações de backup e archive do cliente para execução durante a noite. Se as operações do cliente e do servidor se sobrepuserem ou não tiverem tempo e recursos suficientes para serem processadas, pode ocorrer diminuição do desempenho do sistema, operações com falha e outros problemas.

Procedimento

1. Revise os planejamentos disponíveis passando o mouse sobre **Clientes** na barra de menus do Operations Center. Clique em **Planejamentos**.
2. Opcional: Modifique ou crie um planejamento concluindo as etapas a seguir:

Opção	Descrição
Modificar um planejamento	a. Na visualização **Planejamentos**, selecione o planejamento e clique em **Detalhes**. b. Na página **Detalhes do planejamento**, visualize detalhes clicando nas setas azuis no início das linhas. c. Modifique as configurações no planejamento e clique em **Salvar**.
Criar um planejamento	Na visualização **Planejamentos**, clique em **+Planejamento** e conclua as etapas para criar um planejamento.

3. Opcional: Para definir as configurações de planejamento que não estão visíveis no Operations Center, use um comando do servidor. Por exemplo, talvez você queira planejar uma operação do cliente que faça backup de um diretório específico e designe-o a uma classe de gerenciamento diferente do padrão.
   a) Na página **Visão geral** do Operations Center, passe o mouse sobre o ícone de configurações e clique em **Construtor de comando**.
   b) Emita o comando **DEFINE SCHEDULE** para criar um planejamento ou o comando **UPDATE SCHEDULE** para modificar um planejamento. Para obter mais informações sobre os comandos, veja DEFINE SCHEDULE (Definir um Planejamento de Cliente) ou UPDATE SCHEDULE (Atualizar um planejamento do cliente).

Informações relacionadas

Ajustando o Planejamento para Operações Diárias

Registrando clientes

Registre um cliente para assegurar que ele possa se conectar ao servidor e o servidor possa proteger os dados de cliente.

Antes de Iniciar

Determine se o cliente requer um ID do usuário administrativo com autoridade do proprietário cliente no nó cliente. Para determinar quais clientes requerem um ID do usuário administrativo, consulte a nota técnica 7048963.

Restrição: Para alguns tipos de clientes, o nome do nó cliente e o ID do usuário administrativo devem corresponder. Não é possível autenticar esses clientes usando o método de autenticação Lightweight Directory Access Protocol que foi introduzido na V7.1.7. Para obter detalhes sobre esse método de autenticação, às vezes referido como modo integrado, consulte Autenticando usuários usando um banco de dados do Active Directory.

Procedimento

Para registrar um cliente, conclua uma das seguintes ações.

- Se o cliente requerer um ID do usuário administrativo, registre o cliente usando o comando **REGISTER NODE** e especifique o parâmetro **USERID**:

  ```
  register node node_name password userid=node_name
  ```

  em que *node_name* especifica o nome do nó e *password* especifica a senha do nó. Para obter detalhes, consulte a seção Registrar um Nó.
- Se o cliente não requerer um ID de usuário administrativo, registre o cliente usando o assistente Incluir Cliente do Operations Center. Execute as etapas a seguir:
  a. Na barra de menus do Operations Center, clique em **Clientes**.
  b. Na tabela Clientes, clique em **+ Cliente**.
  c. Conclua as etapas no assistente **Incluir cliente**:
     1) Especifique se os dados redundantes podem ser eliminados no cliente e no servidor. Na área de deduplicação de dados do lado do cliente, selecione a caixa de seleção **Ativar**.
     2) Na janela **Configuração**, copie os valores das opções **TCPSERVERADDRESS**, **TCPPORT**, **NODENAME** e **DEDUPLICATION**.

        Dica: Registre os valores da opção e mantenha-os em um local seguro. Após concluir o registro do cliente e instalar o software no nó cliente, use os valores para configurar o cliente.
     3) Siga as instruções no assistente para especificar o domínio de política, planejamento e conjunto de opções.
     4) Configure como os riscos são exibidos para o cliente, especificando a configuração em risco.
     5) Clique em **Incluir cliente**.

Informações relacionadas

Opção Tcpserveraddress
Opção de tcpport
Opção de nome do nó
Opção deduplication

Instalando e configurando clientes

Para começar a proteger um nó cliente, deve-se instalar e configurar o software selecionado.

Procedimento

Se você já tiver instalado o software, inicie na etapa “2” na página 114.

1. Execute uma das seguintes ações:

   - Para instalar o software em um aplicativo ou nó cliente, siga as instruções.

Software	Link para instruções
Cliente de backup-archive do IBM Spectrum Protect	– Instale deus clientes de archive de backup do UNIX e do Linux – Instalando o cliente Windows pela primeira vez **Dica:** Também é possível atualizar clientes existentes usando o Operations Center. Para obter instruções, consulte Planejando atualizações do cliente.
IBM Spectrum Protect for Databases	– Instalação do Data Protection for Oracle – Instalando o Data Protection for SQL Server no Núcleo do Sistema Windows
IBM Spectrum Protect for Mail	– Instalação do Data Protection for IBM Domino em um sistema UNIX, AIX ou Linux (V7.1.0) – Instalação do Data Protection for IBM Domino em um sistema Windows (V7.1.0) – Instalando, fazendo upgrade e migrando o IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect Snapshot	– Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot para UNIX e Linux – Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot for VMware – Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot for Windows
IBM Spectrum Protect for Enterprise Resource Planning	– Instalando a proteção de dados para o SAP para Db2 – Instalando o Data Protection for SAP for Oracle

   - Para instalar o software em um nó cliente de máquina virtual, siga as instruções para o tipo de backup selecionado.

Tipo de backup	Link para instruções
Se você planeja criar backups completos do VMware de máquinas virtuais, instale e configure o cliente de backup-archive do IBM Spectrum Protect.	– Instale deus clientes de archive de backup do UNIX e do Linux – Instalando o cliente Windows pela primeira vez
Se você planeja criar backups completos incrementais contínuos de máquinas virtuais, instale e configure o Ambientes IBM Spectrum Protect for Virtual e o cliente de backup-archive no mesmo nó cliente ou em nós clientes diferentes.	– Proteção de Dados para VMware **Dica:** É possível obter o software para o Ambientes IBM Spectrum Protect for Virtual e o cliente de backup-archive no pacote de instalação do Ambientes IBM Spectrum Protect for Virtual.

2. Para permitir que o cliente se conecte ao servidor, inclua ou atualize os valores para as opções **TCPSERVERADDRESS**, **TCPPORT** e **NODENAME** no arquivo de opções do cliente. Use os valores registrados durante o registro do cliente ("Registrando clientes" na página 112).
   - Para clientes instalados em um sistema operacional AIX, Linux ou Mac OS X, inclua os valores no arquivo de opções do sistema do cliente, `dsm.sys`.
   - Para clientes que estão instalados em um sistema operacional Windows, inclua os valores no arquivo `dsm.opt`.

   Por padrão, os arquivos de opções estão no diretório de instalação.
3. Opcional: Se você instalou um cliente de backup-archive em um sistema operacional Linux ou Windows, instale o client management service no cliente. Siga as instruções em Instalando o serviço de gerenciamento de clientes.
4. Configure o cliente para executar operações planejadas. Siga as instruções em "Configurando o cliente para executar operações planejadas" na página 114.
5. Opcional: Configure comunicações através de um firewall. Siga as instruções em "Configurando as comunicações entre o servidor e o cliente por meio de um firewall" na página 116.
6. Execute um backup de teste para verificar se os dados estão protegidos conforme planejado.

   Por exemplo, para um cliente de backup-archive, conclua as etapas a seguir:

   a) Na página **Clientes** do Operations Center, selecione o cliente do qual você deseja fazer backup e clique em **Fazer backup**.

   b) Verifique se o backup foi concluído com sucesso e se não há mensagens de aviso ou de erro.
7. Monitore os resultados das operações planejadas para o cliente no Operations Center.

O que Fazer Depois

Se precisar mudar o que está sendo submetido a backup no cliente, siga as instruções em "Modificando o escopo de um backup de cliente" na página 110.

Configurando o cliente para executar operações planejadas

Deve-se configurar e iniciar um planejador de cliente no nó cliente. O planejador de cliente permite a comunicação entre o cliente e servidor para que operações planejadas possam ocorrer. Por exemplo, as operações planejadas geralmente incluem fazer backup de arquivos a partir de um cliente.

Sobre Esta Tarefa

O método preferencial é instalar o cliente de backup-archive em todos os nós clientes para que seja possível configurar e iniciar o client acceptor no nó cliente. O client acceptor é projetado para executar operações planejadas de forma eficiente. O client acceptor gerencia o planejador de cliente para que o planejador seja executado apenas quando necessário:

- Quando for tempo de consultar o servidor sobre a próxima operação planejada
- Quando for tempo de iniciar a próxima operação planejada

Ao usar o client acceptor, é possível reduzir o número de processos de segundo plano no cliente e ajudar a evitar problemas de retenção de memória.

O client acceptor executa planejamentos para os produtos a seguir: o cliente de backup-archive, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail e Ambientes IBM Spectrum Protect for Virtual. Se você instalou um produto para o qual o client acceptor não executa planejamentos, siga as instruções de configuração na documentação do produto para assegurar que as operações planejadas possam ocorrer.

Se seu negócio usar uma ferramenta de planejamento de terceiros como prática padrão, será possível usar essa ferramenta de planejamento como uma alternativa para o client acceptor. Geralmente, as ferramentas de planejamento de terceiros iniciam programas clientes diretamente usando comandos do sistema operacional. Para configurar uma ferramenta de planejamento de terceiros, consulte a documentação do produto.

Procedimento

Para configurar e iniciar o planejador de cliente usando o client acceptor, siga as instruções para o sistema operacional instalado no nó cliente:

AIX e Oracle Solaris

a. Na GUI do cliente de backup-archive, clique em **Editar** > **Preferências do cliente**.
b. Clique na guia **Web client**.
c. No campo **Opções de serviços gerenciados**, clique em **Planejar**. Se você também quiser que o client acceptor gerencie o Web client, clique na opção **Ambos**.
d. Para assegurar que o planejador possa iniciar de forma não assistida, no arquivo `dsm.sys`, configure a opção **passwordaccess** como `generate`.
e. Para armazenar a senha de nó do cliente, emita o seguinte comando e insira a senha de nó do cliente quando solicitada:

```
dsmc query sess
```

f. Inicie o client acceptor emitindo o comando a seguir na linha de comandos:

```
/usr/bin/dsmcad
```

g. Para permitir que o client acceptor seja iniciado automaticamente após uma reinicialização do sistema, inclua a entrada a seguir no arquivo de inicialização do sistema (geralmente, `/etc/inittab`):

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Client Acceptor Daemon
```

Linux

a. Na GUI do cliente de backup-archive, clique em **Editar** > **Preferências do cliente**.
b. Clique na guia **Web client**.
c. No campo **Opções de serviços gerenciados**, clique em **Planejar**. Se você também quiser que o client acceptor gerencie o Web client, clique na opção **Ambos**.
d. Para assegurar que o planejador possa iniciar de forma não assistida, no arquivo `dsm.sys`, configure a opção **passwordaccess** como `generate`.
e. Para armazenar a senha de nó do cliente, emita o seguinte comando e insira a senha de nó do cliente quando solicitada:

```
dsmc query sess
```

f. Inicie o client acceptor efetuando login com o ID do usuário raiz e emitindo o comando a seguir:

```
service dsmcad start
```

g. Para permitir que o client acceptor seja iniciado automaticamente após uma reinicialização do sistema, inclua o serviço emitindo o comando a seguir em um prompt de shell:

```
# chkconfig --add dsmcad
```

MAC OS X

a. Na GUI do cliente de backup-archive, clique em **Editar** > **Preferências do cliente**.
b. Para assegurar que o planejador possa iniciar de forma não assistida, clique em **Autorização**, selecione **Geração de Senha** e clique em **Aplicar**.
c. Para especificar como os serviços são gerenciados, clique em **Web Client**, selecione **Planejar**, clique em **Aplicar** e clique em **OK**.
d. Para assegurar que a senha gerada seja salva, reinicie o cliente de backup-archive.
e. Use o aplicativo IBM Spectrum Protect Tools for Administrators para iniciar o client acceptor.

Windows

a. Na GUI do cliente de backup-archive, clique em **Utilitários** > **Assistente de Configuração** > **Ajude-me a configurar o Client Scheduler**. Clique em **Avançar**.
b. Leia as informações na página **Assistente do planejador** e clique em **Avançar**.
c. Na página **Tarefa do planejador**, selecione **Instalar um planejador novo ou adicional** e clique em **Avançar**.
d. No **Nome e localização do planejador**, especifique um nome para o planejador de cliente que você está incluindo. Em seguida, selecione **Usar o Client Acceptor daemon (CAD)** para gerenciar o planejador e clique em **Avançar**.
e. Insira o nome que deseja designar a esse client acceptor. O nome padrão é Client Acceptor. Clique em **Avançar**.
f. Conclua a configuração percorrendo o assistente.
g. Atualize o arquivo de opções do cliente, `dsm.opt`, e configure a opção **`passwordaccess`** como `generate`.
h. Para armazenar a senha de nó do cliente, emita o seguinte comando no prompt de comandos:

```
dsmc query sess
```

Insira a senha de nó do cliente quando solicitado.
i. Inicie o serviço do client acceptor a partir da página **Controle de serviços**. Por exemplo, se você usou o nome padrão, inicie o serviço do Client Acceptor. Não inicie o serviço do planejador que você especificou na página **Nome e Local do Planejador**. O serviço do planejador é iniciado e interrompido automaticamente pelo serviço de client acceptor conforme necessário.

Configurando as comunicações entre o servidor e o cliente por meio de um firewall

Se um cliente precisar se comunicar com um servidor por meio de um firewall, deve-se ativar as comunicações entre o servidor e o cliente por meio do firewall.

Antes de Iniciar

Se você usou o assistente Incluir Cliente para registrar um cliente, localize os valores de opção no arquivo de opções do cliente que você obteve durante esse processo. É possível usar valores para especificar portas.

Sobre Esta Tarefa

Atenção: Não configure um firewall de uma maneira que possa causar o término de sessões que estão em uso por um servidor ou agente de armazenamento. O término de uma sessão válida pode causar resultados imprevisíveis. Os processos e sessões podem parecer parar devido a erros de entrada/saída. Para ajudar a excluir sessões de restrições de tempo limite, configure as portas conhecidas para componentes do IBM Spectrum Protect. Certifique-se de que a opção do servidor **KEEPALIVE** permaneça configurada como o valor padrão de YES. Dessa forma, é possível ajudar a assegurar que a comunicação entre o servidor e o cliente seja ininterrupta. Para obter instruções sobre como configurar a opção do servidor **KEEPALIVE**, consulte KEEPALIVE.

Procedimento

Abra as seguintes portas para permitir acesso pelo firewall:

Porta TCP/IP para o cliente de backup-archive, o cliente administrador da linha de comandos e o planejador de cliente

Especifique a porta usando a opção **`tcpport`** no arquivo de opções do cliente. A opção **`tcpport`** no arquivo de opções do cliente deve corresponder à opção **TCPPORT** no arquivo de opções do servidor. O valor padrão é 1500. Se você decidir usar um valor diferente do padrão, especifique um número no intervalo de 1024 a 32767.

Porta HTTP para ativar a comunicação entre o Web client e estações de trabalho remotas
Especifique a porta para a estação de trabalho remota configurando a opção **httpport** no arquivo de opções do cliente da estação de trabalho remota. O valor padrão é 1581.

Portas TCP/IP para a estação de trabalho remota
O valor padrão de 0 (zero) faz com que dois números de portas livres sejam designados aleatoriamente à estação de trabalho remota. Se não desejar que os números de portas sejam designados aleatoriamente, especifique valores configurando a opção **webports** no arquivo de opções do cliente da estação de trabalho remota.

Porta TCP/IP para sessões administrativas
Especifique a porta na qual o servidor espera solicitações para sessões administrativas do cliente. O valor da opção **tcpadminport** do cliente deve corresponder ao valor da opção do servidor **TCPADMINPORT**. Dessa forma, é possível proteger sessões administrativas em uma rede privada.

Configurando a Movimentação de Dados sem LAN

É possível configurar o cliente e o servidor para que o cliente, por meio de um agente de armazenamento, possa mover dados diretamente para o armazenamento em uma SAN.

Sobre Esta Tarefa

A movimentação de dados sem LAN é fornecida pelo produto IBM Spectrum Protect for SAN. Para obter detalhes, consulte a documentação para o IBM Spectrum Protect for SAN.

Procedimento

Para configurar a movimentação de dados sem LAN, conclua as etapas a seguir.

1. Verifique a conexão de rede.
2. Estabeleça comunicação entre o cliente, o agente de armazenamento e o servidor.
3. Instale e configure o software em sistemas do cliente.
4. Configure os dispositivos no servidor para acesso do agente de armazenamento.
5. Configure políticas do IBM Spectrum Protect para movimentação de dados sem a LAN para o cliente.
6. Se estiver utilizando armazenamento FILE compartilhado, instale e configure o IBM TotalStorage SAN File System ou o IBM Spectrum Scale.

   Restrição: Windows Se um volume IBM Spectrum Scale for formatado por um servidor AIX, o sistema Windows usará TCP/IP para transferir dados e não a rede de área de armazenamento.
7. Defina caminhos do agente de armazenamento para unidades.
8. Inicie o agente de armazenamento e verifique a configuração sem a LAN.

O que Fazer Depois

Para ajudar a ajustar o uso de seus recursos LAN e SAN, será possível controlar o caminho que as transferências de dados usam para os clientes com o recurso de movimentação de dados sem a LAN. Controle o caminho usando o comando **UPDATE NODE**. Para cada cliente, é possível selecionar uma das seguintes configurações para operações de leitura e gravação de dados. Especifique as operações de leitura de dados usando o parâmetro **DATAREADPATH** e operações de gravação de dados usando o parâmetro **DATAWRITEPATH**. O parâmetro é opcional. O valor padrão é ANY.

LAN (Somente caminho da LAN)
Especifique o valor da LAN se alguma das seguintes condições for verdadeira:

- Você deseja fazer backup ou restaurar uma pequena quantidade de dados.
- O cliente não tem conectividade de SAN.

LANFREE (Somente caminho sem LAN)
Especifique o valor LANFREE se o cliente e o servidor estiverem na mesma SAN e se qualquer das condições a seguir for verdadeira:

- Você deseja fazer backup ou restaurar uma grande quantidade de dados.
- Você deseja transferir a carga de processamento do servidor para o cliente.
- Você quer aliviar o congestionamento de LAN.

ANY (Qualquer caminho disponível)
Um caminho sem LAN será usado se estiver disponível. Se um caminho sem LAN estiver indisponível, os dados serão movidos usando a LAN.

Validando sua configuração sem a LAN

Depois de configurar um cliente do IBM Spectrum Protect para movimentação de dados sem a LAN, é possível verificar as definições de configuração e do servidor usando o comando **VALIDATE LANFREE**.

Sobre Esta Tarefa

O comando **VALIDATE LANFREE** permite determinar quais destinos para um nó que estiver usando um agente de armazenamento específico são aptos para movimentação de dados sem a LAN. A saída de comando também pode ajudar a identificar se há um problema com uma configuração sem a LAN existente. É possível avaliar a política, o conjunto de armazenamentos e as definições de caminho para um nó e um agente de armazenamento que o nó estiver usando para assegurar que a operação funcione corretamente.

Procedimento

- Determine se um nó cliente tem um problema com sua configuração sem a LAN emitindo o comando **VALIDATE LANFREE**. Por exemplo, se o nó cliente FRED estiver usando o agente de armazenamento FRED_STA, emita o comando a seguir:

  ```
  validate lanfree fred fred_sta
  ```

  Os resultados ajudam a identificar ajustes que podem ser necessários na configuração ou nas políticas de armazenamento. A saída exibe quais destinos de classe de gerenciamento para um tipo de operação específico não são aptos para transferências de dados sem a LAN. Ela também relata o número total de destinos sem a LAN.

Informações relacionadas
VALIDATE LANFREE (Validar caminhos sem a LAN)

Métodos de criptografia de fita

A decisão sobre o método de criptografia a ser usado depende de como você deseja gerenciar seus dados.

É essencial para proteger dados do cliente, especialmente quando esses dados são sensíveis. Para assegurar que os dados em volumes no local e externo estejam protegidos, a tecnologia de criptografia de fita IBM está disponível.

Essa tecnologia usa um nível mais forte de criptografia, exigindo chaves de criptografia de Padrão de Criptografia Avançado (AES) de 256 bits. As chaves são passadas para a unidade por um gerenciador de chaves para criptografar e descriptografar dados.

A tecnologia de fita IBM suporta diferentes métodos de criptografia de unidade para os dispositivos a seguir:

- IBM 3592 Geração 2 e Geração 3

- IBM Linear Tape Open Geração 4 e Geração 5

Os método de criptografia de unidade que podem ser usados com o IBM Spectrum Protect são configurados no nível de hardware. O IBM Spectrum Protect não pode controlar ou mudar qual método de criptografia é usado na configuração de hardware. Se o hardware estiver configurado para o método de Aplicativo, o IBM Spectrum Protect poderá ativar ou desativar a criptografia, dependendo do valor **DRIVEENCRYPTION** na classe de dispositivo.

Para criptografar todos os dados em uma biblioteca lógica específica ou criptografar dados em mais do que apenas volumes do conjunto de armazenamentos, use o método de Biblioteca ou de Sistema. Se o gerenciador de chave de criptografia estiver configurado para compartilhar chaves, os métodos de Biblioteca e de Sistema poderão compartilhar a chave de criptografia, o que permite que os dois métodos sejam trocados. O IBM Spectrum Protect não pode compartilhar ou usar chaves de criptografia entre o método de Aplicativo e os métodos de Biblioteca ou de Sistema de criptografia.

Tabela 24. Métodos de Criptografia

Método de Criptografia	**descrição**
Criptografia de aplicativo	Com a criptografia gerenciada por aplicativo, é possível criar conjuntos de armazenamentos dedicados que contêm somente volumes criptografados. Dessa forma, é possível usar hierarquias e políticas do conjunto de armazenamentos para gerenciar a maneira com que os dados são criptografados. As chaves de criptografia são gerenciadas pelo aplicativo, nesse caso, o IBM Spectrum Protect. O IBM Spectrum Protect gera e armazena as chaves no banco de dados do servidor. Os dados são criptografados durante operações de gravação, quando a chave de criptografia é transmitida do servidor para a unidade. Os dados são decriptografados para operações de leitura. Para criptografar volumes do conjunto de armazenamentos e eliminar algum processo de criptografia em seu sistema, ative o método de Aplicativo. Use a criptografia gerenciada por aplicativo somente para volumes do conjunto de armazenamentos. Outros volumes, como fitas do conjunto de backup, volumes de exportação e backups de banco de dados, não são criptografados usando o método de Aplicativo. **Exigência:** Quando a criptografia de aplicativo estiver ativada, você deve ter cuidado extra para proteger backups de banco de dados, porque as chaves de criptografia que são usadas para criptografar e decriptografar dados são armazenadas no banco de dados do servidor. Para restaurar seus dados, você deve ter o backup de banco de dados correto e chaves de criptografia correspondentes para acessar suas informações. Certifique-se de fazer backup do banco de dados frequentemente e de proteger os backups para evitar perda ou roubo de dados. Quem tem acesso ao backup de banco de dados e às chaves de criptografia tem acesso a seus dados.

Tabela 24. Métodos de Criptografia (continuação)	
Método de Criptografia	**descrição**
Criptografia de biblioteca	Com a criptografia gerenciada por biblioteca, é possível controlar quais volumes são criptografados usando seus números de série. É possível especificar um intervalo ou conjunto de volumes para criptografar. As chaves de criptografia são gerenciadas pela biblioteca. As chaves são armazenadas em um gerenciador de chaves de criptografia e fornecidas para a unidade. Se você configurar o hardware para usar a criptografia gerenciada por biblioteca, será possível usar este método executando o comando **DEFINE DEVCLASS** e especificando o parâmetro **DRIVEENCRYPTION=ALLOW**. **Restrição:** Apenas certas bibliotecas IBM suportam criptografia IBM LTO-4 e mais recente. Para obter informações adicionais, consulte "Configurando criptografia de unidade de fita" na página 120.
Criptografia do sistema	A criptografia gerenciada pelo sistema está disponível apenas no sistema operacional AIX®. As chaves de criptografia que são fornecidas para a unidade são gerenciadas pelo driver de dispositivo ou sistema operacional e armazenadas em um gerenciador de chave de criptografia. Se o hardware for configurado para usar a criptografia do sistema, será possível usar esse método executando o comando **DEFINE DEVCLASS** e especificando o parâmetro **DRIVEENCRYPTION=ALLOW**.

Para determinar se um volume é criptografado e qual método foi usado, execute o comando **QUERY VOLUME** e especifique o parâmetro **FORMAT=DETAILED**.

Configurando criptografia de unidade de fita

É possível usar criptografia de unidade para proteger fitas que contenham dados críticos ou sensíveis, por exemplo, e fitas que contenham informações financeiras confidenciais. A criptografia de unidade pode ser útil ao mover fitas do ambiente do servidor do IBM Spectrum Protect para uma localização interna ou externa.

Sobre Esta Tarefa

Para determinar quais métodos de criptografia podem ser usados com vários tipos de unidade, consulte a tabela a seguir.

Tabela 25. Métodos de criptografia disponíveis			
	Método da aplicação	**Método da biblioteca**	**Método do sistema**
3592 Geração 2 e posterior	SIM	Sim.	SIM
HP LTO-4 e mais recente	SIM	Nº.	Sim

Tabela 25. Métodos de criptografia disponíveis (continuação)			
	Método da aplicação	**Método da biblioteca**	**Método do sistema**
IBM LTO-4 e mais recente	SIM	Sim, mas somente se seu hardware do sistema (por exemplo, uma biblioteca de fitas TS3500) suportá-lo.	SIM
Oracle StorageTek T10000B	SIM	Nº.	Sim
Oracle StorageTek T10000C	SIM	Nº.	Sim
Oracle StorageTek T10000D	SIM	Nº.	Sim

Uma biblioteca pode conter uma combinação de unidades, algumas das quais suportam criptografia e outras não. Por exemplo, uma biblioteca pode conter duas unidades LTO-2, duas unidades LTO-3 e duas unidades LTO-4. Também é possível combinar mídia em uma biblioteca usando, por exemplo, classes de dispositivos criptografadas e não criptografadas que possuam diferentes tecnologias de fita e de unidade.

Restrições:

- Para aplicar a criptografia a unidades LTO-4 ou mais recente, todas as unidades devem suportar criptografia.
- Para aplicar a criptografia a uma biblioteca lógica, deve-se usar o mesmo método de criptografia para todas as unidades dentro da biblioteca. Não crie um ambiente no qual algumas unidades usam o método do aplicativo e algumas unidades usam os métodos de criptografia da biblioteca ou do sistema.

Para obter mais informações sobre como configurar seu ambiente de hardware para usar a criptografia de unidade, consulte a documentação do hardware.

Procedimento

1. Instale um driver de dispositivo que suporte a criptografia da unidade:
   - Para ativar a criptografia para uma unidade IBM LTO-4 ou mais recente, você deve instalar o driver de dispositivo IBM RMSS Ultrium. As unidades SCSI não suportam a criptografia IBM LTO-4 ou mais recente.
   - Para ativar a criptografia para uma unidade HP LTO-4 ou mais recente, você deve instalar o driver de dispositivo IBM Spectrum Protect.
2. Ative a criptografia de unidade especificando o parâmetro **DRIVEENCRYPTION** no comando **DEFINE DEVCLASS** ou **UPDATE DEVCLASS** para os tipos de dispositivo 3592, LTO ou ECARTRIDGE.

O que Fazer Depois

Ao usar unidades com capacidade de criptografia com um método de criptografia suportado, um formato diferente é usado para gravar dados criptografados nas fitas. Quando os dados são gravados em volumes que usam o formato diferente e se os volumes forem, então, retornados para o estado inicial, eles conterão rótulos que podem ser lidos apenas por unidades ativadas para criptografia. Para usar esses volumes utilizáveis em uma unidade que não esteja ativada para criptografia, porque o hardware não tem capacidade de criptografia ou porque o método de criptografia está configurado como NONE, deve-se etiquetar os volumes novamente.

Tarefas relacionadas

Ativando e desativando a criptografia de unidade 3592 Geração 2 e mais recente

Com o IBM Spectrum Protect, é possível usar os seguintes tipos de criptografia de unidade com unidades que são 3592 Geração 2 e mais recente: Aplicativo, Sistema e Biblioteca. Esses métodos são definidos por meio do hardware.

Ativando e desativando a criptografia de unidade para unidades de fita LTO Geração 4 ou mais recente
O IBM Spectrum Protect suporta os três tipos de criptografia de unidade que estão disponíveis com unidades LTO Geração 4 ou mais recente: Aplicativo, Sistema e Biblioteca. Esses métodos são definidos por meio do hardware.

Informações relacionadas
DEFINE DEVCLASS (Definir uma Classe de Dispositivo)
UPDATE DEVCLASS (atualizar uma classe de dispositivo)

Controlando operações de armazenamento em fita

As definições de classe de dispositivo para fitas incluem parâmetros que permitem controlar operações de armazenamento.

Como o IBM Spectrum Protect preenche os volumes

O comando **DEFINE DEVCLASS** tem um parâmetro **ESTCAPACITY** opcional que indica a capacidade estimada para os volumes sequenciais que estiverem associados à classe de dispositivo. O IBM Spectrum Protect usa a capacidade estimada de volumes para determinar a capacidade estimada de um conjunto de armazenamentos e a porcentagem estimada utilizada.

Se o parâmetro **ESTCAPACITY** não for especificado, o IBM Spectrum Protect usará um valor padrão que é baseado no formato de gravação que é especificado para a classe de dispositivo usando o parâmetro **FORMAT**.

Se você especificar uma capacidade estimada que excede a capacidade real do volume na classe de dispositivo, o IBM Spectrum Protect atualizará a capacidade estimada do volume quando o volume se tornar cheio. Quando o IBM Spectrum Protect atinge o término do volume, ele atualiza a capacidade para corresponder à quantia que é gravada no volume.

É possível aceitar a capacidade estimada padrão para a classe de dispositivo ou especificar explicitamente uma capacidade estimada. Um valor exato de capacidade estimada não é necessário, mas é útil. O IBM Spectrum Protect usa a capacidade estimada de volumes para determinar a capacidade estimada de um conjunto de armazenamentos e a porcentagem estimada que é usada. Talvez você queira mudar a capacidade estimada se uma ou ambas as condições a seguir forem verdadeiras:

- A capacidade estimada padrão é imprecisa devido à compactação de dados.
- Você tem volumes de tamanho não padrão.

Informações relacionadas
DEFINE DEVCLASS (Definir uma Classe de Dispositivo)
UPDATE DEVCLASS (atualizar uma classe de dispositivo)

Especificando a capacidade estimada de volumes de fita

O IBM Spectrum Protect também usa capacidade estimada para determinar quando iniciar a recuperação de volumes do conjunto de armazenamentos.

Sobre Esta Tarefa

Para classes de dispositivo de fita, os valores padrão selecionados pelo servidor dependem do formato de gravação que é utilizado para gravar dados no volume. É possível aceitar o padrão para um tipo de dispositivo ou especificar um valor.

Para especificar a capacidade estimada para volumes de fita, use o parâmetro **ESTCAPACITY** ao definir a classe de dispositivo ou atualize a sua definição.

Informações relacionadas
DEFINE DEVCLASS (Definir uma Classe de Dispositivo)

UPDATE DEVCLASS (atualizar uma classe de dispositivo)

Especificando formatos de gravação para mídia de fita

É possível especificar o formato de gravação que é usado pelo IBM Spectrum Protect para gravar dados na mídia de fita. Se você planeja combinar gerações de unidades, ou diferentes tipos de unidade, em uma biblioteca, você deve especificar um formato de gravação para cada geração de unidade e cada tipo de unidade. Dessa forma, o servidor pode diferenciar entre as gerações de unidade e os tipos de unidades.

Sobre Esta Tarefa

Para especificar um formato de gravação, use o parâmetro **FORMAT** ao definir a classe de dispositivo ou atualizar sua definição.

Se todas as unidades associadas a essa classe de dispositivo forem idênticas, especifique **FORMAT=DRIVE**. O servidor seleciona o formato mais alto suportado pela unidade na qual um volume é montado.

Se algumas unidades associadas à classe de dispositivo suportarem um formato de densidade mais alta que outras unidades, especifique um formato que seja compatível com todas as unidades.

Se as unidades em uma única biblioteca SCSI usarem diferentes tecnologias de fita (por exemplo, DLT e LTO Ultrium), especifique um valor exclusivo para o parâmetro **FORMAT** em cada definição de classe de dispositivo.

Para obter um exemplo de configuração, consulte Exemplo: configure uma biblioteca SCSI ou Virtual Tape Library com múltiplos tipos de dispositivo da unidade.

O formato de gravação que o servidor utiliza para um volume é selecionado quando os dados são gravados pela primeira vez no volume. A atualização do parâmetro **FORMAT** não afeta a mídia que já contiver dados até que ela seja regravada desde o início. Este processo pode ocorrer depois que um volume é recuperado ou excluído ou depois que todos os dados no volume expiram.

Informações relacionadas

DEFINE DEVCLASS (Definir uma Classe de Dispositivo)

UPDATE DEVCLASS (atualizar uma classe de dispositivo)

Associando objetos de biblioteca às classes de dispositivo

Uma biblioteca contém as unidades que podem ser usadas para montar o volume. Apenas uma biblioteca pode ser associada a uma classe de dispositivo. No entanto, múltiplas classes de dispositivos podem fazer referência à mesma biblioteca.

Sobre Esta Tarefa

Para associar uma classe de dispositivo a uma biblioteca, use o parâmetro **LIBRARY** ao definir uma classe de dispositivo ou atualizar sua definição.

Informações relacionadas

DEFINE DEVCLASS (Definir uma Classe de Dispositivo)

UPDATE DEVCLASS (atualizar uma classe de dispositivo)

Controlando operações de montagem de mídia para dispositivos de fita

Usando definições de classe de dispositivo, é possível controlar o número de volumes montados, a quantia de tempo que um volume permanece montado e a quantia de tempo que o servidor do IBM Spectrum Protect aguarda por uma unidade ficar disponível.

Controlando o número de volumes montados simultaneamente

Ao configurar um limite de montagem para uma classe de dispositivo, você deve considerar o número de dispositivos de armazenamento que estão conectados a seu sistema. Você também deve considerar se

usar a função de gravação simultânea, se associar várias classes de dispositivo a uma única biblioteca e o número de processos que são executados ao mesmo tempo.

Sobre Esta Tarefa

Ao selecionar um limite de montagem para uma classe de dispositivo, considere os seguintes problemas:

- Quantos dispositivos de armazenamento estão conectados ao seu sistema?

  Não especifique um valor limite de montagem maior que o número de unidades disponíveis associadas em sua instalação. Se o servidor tentar montar quantos volumes forem especificados pelo limite de montagem e nenhuma unidade estiver disponível para o volume necessário, ocorrerá um erro e as sessões do cliente podem ser encerradas. (Esta restrição não se aplica quando o parâmetro **DRIVES** é especificado.)

  Se estiver compartilhando recursos da biblioteca em uma SAN entre servidores IBM Spectrum Protect, você deverá limitar o número de unidades de fita que um cliente de biblioteca pode usar de cada vez. Para permitir que vários servidores clientes de biblioteca usem uma biblioteca simultaneamente, especifique o parâmetro **MOUNTLIMIT** ao definir ou atualizar a classe de dispositivo no cliente de biblioteca. Para obter informações adicionais sobre como configurar o compartilhamento de biblioteca, consulte "Configurando o compartilhamento de biblioteca" na página 98.

- Você está usando a função de gravação simultânea para conjuntos de armazenamentos primários, conjuntos de armazenamentos de cópia e conjuntos de dados ativos.

  Especifique um valor limite de montagem que fornece pontos de montagem suficientes para suportar a gravação de dados simultaneamente para o conjunto de armazenamentos primários e todos os conjuntos de armazenamentos de cópia associados e conjuntos de dados ativos.

- Você está associando múltiplas classes de dispositivo a uma única biblioteca?

  Uma classe de dispositivo que está associada a uma biblioteca pode usar qualquer unidade na biblioteca que seja compatível com o tipo de dispositivo da classe de dispositivo. Como é possível associar mais de uma classe de dispositivo a uma biblioteca, uma única unidade na biblioteca pode ser usada por mais de uma classe de dispositivo. O IBM Spectrum Protect assegura que duas operações não podem usar a mesma unidade simultaneamente usando duas classes de dispositivo diferentes.

- Quantos processos do IBM Spectrum Protect você deseja executar ao mesmo tempo usando dispositivos nessa classe de dispositivo?

  O IBM Spectrum Protect cancela automaticamente alguns processos para executar outros processos de prioridade mais alta. Se o servidor estiver usando todas as unidades disponíveis em uma classe de dispositivo para concluir processos de prioridade mais alta, os processos de prioridade mais baixa deverão esperar até que uma unidade se torne disponível. Por exemplo, o IBM Spectrum Protect cancela o processo para um cliente que faz backup diretamente na fita, se a unidade for necessária para um processo de migração de servidor ou de recuperação de fita. O IBM Spectrum Protect cancela um processo de recuperação de fita se a unidade for necessária para uma operação de restauração do cliente. Para obter informações adicionais, consulte "Priorizando operações" na página 125.

  Se os processos forem geralmente cancelados por outros processos, considere se será possível tornar mais unidades disponíveis para uso do IBM Spectrum Protect. Caso contrário, revise o planejamento de operações para reduzir a contenção para unidades.

  Essa consideração também se aplica à função de gravação simultânea. Deve-se ter unidades suficientes disponíveis para permitir uma operação de gravação simultânea bem-sucedida.

  Para especificar o número máximo de volumes que podem ser montados simultaneamente, use o parâmetro **MOUNTLIMIT** quando definir a classe de dispositivo ou atualizar sua definição.

Informações relacionadas

DEFINE DEVCLASS (Definir uma Classe de Dispositivo)
UPDATE DEVCLASS (atualizar uma classe de dispositivo)

Controlando a quantia de tempo que um volume permanece montado

É possível controlar a quantia de tempo que um volume montado permanece montado após sua última atividade de E/S. Se um volume for usado com frequência, será possível melhorar o desempenho configurando um período de retenção de montagem maior para evitar operações de montagem e desmontagem desnecessárias.

Sobre Esta Tarefa

Se as operações de montagem estiverem sendo manipuladas por atividades manuais assistidas pelo operador, você poderá querer especificar um período de retenção de montagem longo. Por exemplo, se apenas um operador fornecer suporte a toda a sua operação no fim de semana, então, defina um período de retenção de montagem longo para que não seja solicitado ao operador que monte volumes a cada poucos minutos.

Para controlar a quantia de tempo que um volume montado permanece montado, use o parâmetro **MOUNTRETENTION** ao definir a classe de dispositivo ou atualizar sua definição. Por exemplo, se o valor de retenção de montagem for 60 e um volume montado permanecer inativo por 60 minutos, o servidor desmontará o volume.

Enquanto o IBM Spectrum Protect tiver um volume montado, a unidade estará alocada para o IBM Spectrum Protect e não poderá ser usada para mais nada. Se você precisar liberar a unidade para outros usos, será possível cancelar as operações do IBM Spectrum Protect que estão usando a unidade e, em seguida, desmontar o volume. Por exemplo, é possível cancelar as operações de migração ou backup do servidor. Para obter informações sobre como cancelar processos e desmontar volumes, consulte “Gerenciando solicitações do servidor para volumes” na página 193

Informações relacionadas

DEFINE DEVCLASS (Definir uma Classe de Dispositivo)
UPDATE DEVCLASS (atualizar uma classe de dispositivo)

Controlando a quantia de tempo que o servidor aguarda por uma unidade

É possível especificar a quantia máxima de tempo, em minutos, que o servidor do IBM Spectrum Protect aguarda uma unidade tornar-se disponível para a solicitação de montagem atual.

Sobre Esta Tarefa

Para controlar o tempo de espera para uma unidade tornar-se disponível para uma solicitação de montagem, use o parâmetro **MOUNTWAIT** ao definir ou atualizar uma classe de dispositivo.

Informações relacionadas

DEFINE DEVCLASS (Definir uma Classe de Dispositivo)
UPDATE DEVCLASS (atualizar uma classe de dispositivo)

Priorizando operações

O servidor pode priorizar operações do servidor ou do cliente para uma operação de prioridade mais alta quando um ponto de montagem estiver em uso e nenhum outro estiver disponível ou quando o acesso a um volume específico é necessário. Quando uma operação é priorizada, ela é cancelada.

É possível usar o comando **QUERY MOUNT** para ver o status do volume para o ponto de montagem.

Por padrão, a preempção é ativada no servidor. Para desativar a priorização, especifique a opção **NOPREEMPT** no arquivo de opções do servidor. Se especificar esta opção, o comando **BACKUP DB** e os comandos de exportação e importação serão as únicas operações que poderão priorizar outras operações.

Informações relacionadas

BACKUP DB (Fazer Backup do Banco de Dados)
QUERY MOUNT (Exibir informações sobre volumes de acesso sequencial montados)

Preempção de ponto de montagem

Se uma operação de alta prioridade requerer um ponto de montagem que esteja em uma classe de dispositivo específica e todos os pontos de montagem na classe de dispositivo estiverem em uso, a operação de alta prioridade poderá priorizar um ponto de montagem de uma operação de prioridade mais baixa.

Os pontos de montagem podem ser priorizados apenas quando a classe de dispositivo da operação priorizada e a operação que está sendo priorizada for a mesma.

As seguintes operações de alta prioridade podem priorizar outras operações para um ponto de montagem.

- Operações de backup de banco de dados
- Operações de recuperação, restauração ou rechamada do HSM que são iniciadas por clientes
- Operações de restauração usando um movedor de dados remoto
- Exportar as operações
- Importar operações
- Operações para gerar conjuntos de backup

As seguintes operações do servidor não podem priorizar outras operações ou serem priorizadas:

- Auditar um volume
- Restaurar dados de uma cópia ou de um datapool ativo
- Preparar um arquivo de plano de recuperação
- Armazenar dados usando um movedor de dados remoto

As seguintes operações podem ser priorizadas e são listadas em ordem de prioridade, da mais alta para a mais baixa. O servidor seleciona a operação de prioridade mais baixa para priorizar, por exemplo, identificar duplicatas.

- Replicar nós
- Fazer backup de dados para um conjunto de armazenamentos de cópia
- Copiar dados ativos para um datapool ativo
- Mover dados em um volume do conjunto de armazenamentos
- Migrar dados do disco para a mídia sequencial
- Migrar dados de uma mídia sequencial para outra mídia sequencial
- Operações de backup, archive ou migração de HSM que são iniciadas por clientes
- Recuperar volumes em um conjunto de armazenamentos de acesso sequencial
- Identificar duplicatas

Preempção de acesso do volume

Se uma operação de alta prioridade requerer acesso a um volume específico e esse volume estiver em uso, a operação de alta prioridade poderá priorizar a operação de prioridade mais baixa para esse volume.

Por exemplo, se uma solicitação de restauração requerer acesso a um volume em uso por uma operação de recuperação e uma unidade estiver disponível, a operação de recuperação será cancelada.

As seguintes operações de alta prioridade podem priorizar operações para acesso a um volume específico:

- Operações de backup de banco de dados
- Operações de recuperação, restauração ou rechamada do HSM que são iniciadas por clientes
- Operações de restauração usando um movedor de dados remoto
- Exportar as operações

- Importar operações
- Operações para gerar conjuntos de backup

As seguintes operações não podem priorizar outras operações ou serem priorizadas:

- Volume de auditoria
- Restaurar dados de uma cópia ou de um datapool ativo
- Preparar um plano de recuperação
- Armazenar dados usando um movedor de dados remoto

As seguintes operações podem ser priorizadas e são listadas em ordem de prioridade, da mais alta para a mais baixa. O servidor seleciona a operação de prioridade mais baixa para priorizar, por exemplo, identificar duplicatas.

- Replicar nós
- Fazer backup de dados para um conjunto de armazenamentos de cópia
- Copiar dados ativos para um datapool ativo
- Mover dados em um volume do conjunto de armazenamentos
- Migrar dados do disco para a mídia sequencial
- Migrar dados de uma mídia sequencial para outra mídia sequencial
- Operações de backup, archive ou migração de dados do HSM que são iniciadas pelo cliente
- Recuperar volumes em um conjunto de armazenamentos de acesso sequencial
- Identificar duplicatas

Impactos de mudanças de dispositivo na SAN

O ambiente SAN pode mudar drasticamente devido a mudanças de dispositivo ou de cabeamento. A natureza dinâmica da SAN pode causar falha nas definições estáticas ou podem se tornar imprevisíveis.

Os IDs de dispositivo que são designados pela SAN e conhecidos pelo servidor ou agente de armazenamento podem ser mudados devido a reconfigurações de barramento ou outras mudanças ambientais. Por exemplo, o servidor pode conhecer um dispositivo X como *rmt0* (no AIX), com base na especificação de caminho original para o servidor e configuração original da LAN. No entanto, algum evento na SAN, por exemplo, a inclusão do novo dispositivo Y, faz o dispositivo X ser designado a *rmt1*. Quando o servidor tenta acessar o dispositivo X usando *rmt0*, o acesso falha ou o dispositivo de destino errado é acessado. O servidor tenta recuperar-se de mudanças nos dispositivos na SAN usando os números de série do dispositivo para confirmar a identidade de dispositivos que ele contata.

Ao definir uma unidade ou biblioteca, há a opção de especificar o número de série para esse dispositivo. Se você não especificar o número de série ao definir o dispositivo, o servidor obterá o número de série quando definir o caminho para o dispositivo. Em qualquer caso, o servidor tem então o número de série do dispositivo em seu banco de dados e pode usá-lo para confirmar a identidade de um dispositivo para operações.

Quando o servidor usa unidades e bibliotecas em uma SAN, ele tenta verificar se o dispositivo correto será usado. O servidor entra em contato com o dispositivo usando o nome do dispositivo no caminho que você definiu para ele. O servidor então solicita o número de série do dispositivo e compara esse número de série com o que está armazenado no banco de dados do servidor para esse dispositivo.

Se o número de série não corresponder, o servidor iniciará o processo de descoberta da SAN, tentando encontrar o dispositivo com o número de série correspondente. Se o servidor localizar o dispositivo com o número de série correspondente, ele corrigirá a definição do caminho no banco de dados do servidor atualizando o nome do dispositivo nesse caminho. O servidor emite uma mensagem com informações sobre a mudança que é feita no dispositivo. Em seguida, o servidor continuará a usar o dispositivo.

Para determinar quando as mudanças de dispositivo na SAN afetam o servidor IBM Spectrum Protect, é possível monitorar o log de atividades para mensagens. As seguintes mensagens são relacionadas a números de série:

- ANR8952 a ANR8958
- ANR8961 a ANR8968
- ANR8974 a ANR8975

Restrição: Alguns dispositivos não podem relatar seus números de série para aplicativos como o servidor do IBM Spectrum Protect. Se o servidor não puder obter o número de série de um dispositivo, ele não poderá ajudar o sistema a se recuperar de uma mudança de localização de dispositivo na SAN.

Windows Exibindo Informações sobre o Dispositivo

É possível exibir informações sobre dispositivos que estão conectados ao servidor usando o utilitário de informações sobre o dispositivo (tsmdlst).

Antes de Iniciar

- Certifique-se de que a API HBA esteja instalada. A API HBA é necessária para executar o utilitário de informações sobre o dispositivo.
- Certifique-se de que o driver de dispositivo de fita esteja instalado e configurado.

Procedimento

1. Em um prompt de comandos, mude para o subdiretório `server` do diretório de instalação do servidor, por exemplo, `C:\Program Files\Tivoli\TSM\server`.
2. Execute o arquivo executável `tsmdlst.exe`.

Informações relacionadas

QUERY SAN (Consultar os dispositivos na SAN)
tsmdlst (Exibir informações sobre os dispositivos)

Tipo de mídia write-once, read-many

Ajuda da mídia Write-once, read-many (WORM) para evitar exclusão acidental ou deliberada de dados críticos. No entanto, o IBM Spectrum Protect impõe determinadas restrições e diretrizes a serem seguidas ao usar a mídia WORM.

É possível utilizar os seguintes tipos de mídia WORM com o IBM Spectrum Protect:

- IBM 3592, todas as gerações suportadas
- IBM LTO-3 e todas as gerações suportadas
- HP LTO-3 e todas as gerações suportadas
- Quantum LTO-3 e todas as gerações suportadas
- Quantum SDLT 600, Quantum DLT V4 e Quantum DLT S4
- StorageTek VolSafe
- Sony AIT50 e AIT100

Dicas:

- Um conjunto de armazenamentos pode consistir em mídia WORM ou RW, mas não em ambas.
- Para evitar o desperdício de uma fita após uma operação de restauração ou importação, não use fitas WORM para operações de backup ou exportação de banco de dados.

Unidades com capacidade para WORM

Para utilizar a mídia WORM em uma biblioteca, todas as unidades na biblioteca devem ter capacidade para WORM. Uma montagem falhará se um cartucho WORM for montado em uma unidade de leitura/gravação (RW).

No entanto, uma unidade com capacidade para WORM poderá ser usada como uma unidade RW se o parâmetro WORM na classe de dispositivo for configurado como NO. Qualquer tipo de biblioteca poderá

ter mídia WORM e RW se *todas* as unidades estiverem ativadas para WORM. A única exceção a essa regra é bibliotecas anexadas ao NAS em que a mídia de fita WORM não pode ser usada.

Informações relacionadas

DEFINE DEVCLASS (Definir uma Classe de Dispositivo)

UPDATE DEVCLASS (atualizar uma classe de dispositivo)

Check-in de mídia WORM

O tipo de mídia WORM determina se o rótulo da mídia precisa ser lido durante o check-in.

Alteradores de mídia de biblioteca não podem identificar a diferença entre a mídia de fita de leitura/gravação (RW) padrão e os seguintes tipos de mídia de fita WORM:

- VolSafe
- Sony AIT
- LTO
- SDLT
- DLT

Para determinar o tipo de mídia WORM que está sendo usado, um volume deverá ser carregado em uma unidade. Portanto, ao efetuar check-in de um desses tipos de volumes WORM, deve-se usar a opção CHECKLABEL=YES no comando **CHECKIN LIBVOLUME**.

Se eles fornecerem suporte para mídia WORM, os alteradores de mídia da biblioteca IBM 3592 poderão detectar se um volume é uma mídia WORM sem carregar o volume em uma unidade. Não é necessário especificar CHECKLABEL=YES. Verifique com os fornecedores do hardware se as unidades e bibliotecas 3592 fornecem o suporte necessário.

Informações relacionadas

CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)

Restrições na mídia WORM

Não é possível usar a mídia WORM rotulada previamente com a classe de dispositivo LTO ou ECARTRIDGE.

Não é possível usar a mídia WORM com o IBM Spectrum Protect especificado como o gerenciador de chave de criptografia de unidade para as seguintes unidades:

- IBM LTO-5, LTO-6 e mais recente
- HP LTO-5, LTO-6 e mais recente
- Oracle StorageTek T10000B
- Oracle StorageTek T10000C
- Oracle StorageTek T10000D

Falhas de montagem com mídia WORM

Se a mídia de fita WORM for carregada em uma unidade para uma montagem de classe de dispositivo de leitura/gravação (RW), isso causará uma falha de montagem. Da mesma forma, se a mídia de fita RW for carregada em uma unidade para uma montagem de classe de dispositivo WORM, a montagem falhará.

Rotulando mídia WORM

Não será possível rotular um cartucho WORM se ele contiver dados. Isso se aplica a cartuchos Sony AIT WORM, LTO WORM, SDLT WORM, DLT WORM e IBM 3592. O rótulo em um volume VolSafe deverá ser sobrescrito apenas uma vez e somente se o volume não contiver dados utilizáveis, excluídos ou expirados.

Emita o comando **LABEL LIBVOLUME** apenas uma vez para volumes VolSafe. É possível proteger-se contra a sobrescrição de rótulo utilizando a opção OVERWRITE=NO no comando **LABEL LIBVOLUME**.

Informações relacionadas

LABEL LIBVOLUME (Rotular um volume de biblioteca)

Removendo volumes WORM privados de uma biblioteca

Se você executar uma ação em um volume WORM (por exemplo, se excluir espaços de arquivo) e o servidor não marcar o volume como cheio, o volume será retornado para o status inicial. Se um volume WORM não for marcado como cheio e você excluí-lo de um conjunto de armazenamentos, o volume permanecerá privado. Para remover um volume WORM privado de uma biblioteca, deve-se emitir o comando **CHECKOUT LIBVOLUME**.

Informações relacionadas

CHECKOUT LIBVOLUME (Verificar um Volume de Armazenamento Fora de uma Biblioteca)

Criação de volumes WORM DLT

Os volumes WORM DLT podem ser convertidos de volumes de leitura/gravação (RW).

Se você tiver unidades SDLT-600, DLT-V4 ou DLT-S4 e desejar permiti-las para mídia WORM, faça upgrade das unidades usando um firmware V30 ou mais recente disponível no Quantum. Também é possível usar o software DLTIce para converter volumes RW não formatados ou volumes em branco em volumes WORM.

Em bibliotecas SCSI, o servidor IBM Spectrum Protect cria volumes DLT WORM utilizáveis automaticamente quando o servidor não pode localizar nenhum volume WORM utilizável em um inventário da biblioteca. O servidor converte volumes utilizáveis RW não formatados ou em branco ou volumes privados RW vazios em volumes WORM utilizáveis. O servidor também regrava rótulos em volumes WORM recém-criados usando as informações de rótulo em volumes RW existentes.

Suporte para fitas WORM 3592 curtas e normais

O IBM Spectrum Protect suporta fitas WORM 3592 curtas e normais. Para obter melhores resultados, defina-as em conjuntos de armazenamentos separados

Consultando uma classe de dispositivo para a configuração do parâmetro WORM

É possível determinar a configuração do parâmetro WORM para uma classe de dispositivo usando o comando **QUERY DEVCLASS**. A saída contém um campo, rotulado WORM e um valor (YES ou NO).

Informações relacionadas

QUERY DEVCLASS (Exibir Informações Sobre Uma ou Mais Classes de Dispositivo)

Resolução de problemas com dispositivos

É possível resolver problemas de erros que ocorrem ao configurar ou usar dispositivos com o IBM Spectrum Protect.

Sobre Esta Tarefa

Use o Tabela 26 na página 130 para localizar uma solução para o problema relacionado ao dispositivo.

Tabela 26. Resolvendo problemas de dispositivo

Sintoma	Problema	Solução
Conflitos com outros aplicativos.	O IBM Spectrum Protect requer uma rede de área de armazenamento para compartilhar dispositivos.	Configure uma rede de área de armazenamento. **Atenção:** Poderá ocorrer perda de dados se múltiplos servidores IBM Spectrum Protect usarem o mesmo dispositivo. Defina ou use um dispositivo com apenas um servidor IBM Spectrum Protect. Linux AIX Outros aplicativos podem acessar dispositivos IBM Spectrum Protect usando um driver de fita SCSI.

Tabela 26. Resolvendo problemas de dispositivo (continuação)

Sintoma	Problema	Solução
A rotulagem falha.	Um dispositivo para rotulagem de volumes não pode ser usado no mesmo tempo em que o servidor usa o dispositivo para outros processos.	Não é possível sobrescrever volumes existentes em um conjunto de armazenamentos. Você deve resolver quaisquer problemas de hardware antes de rotular um volume.
	Registro de licença incorreto ou incompleto.	Registre a licença para o suporte de dispositivo que foi comprado.
Conflitos entre drivers de dispositivos	O IBM Spectrum Protect emite mensagens sobre erros de E/S ao definir ou usar um dispositivo de acesso sequencial.	Windows Os drivers de dispositivo do Windows e drivers que são fornecidos por outros aplicativos poderão interferir com o driver de dispositivo do IBM Spectrum Protect se o driver do IBM Spectrum Protect não for iniciado primeiro. Para verificar a ordem em que os drivers de dispositivo são iniciados pelo sistema, conclua as etapas a seguir: 1. Clique em **Painel de Controle**. 2. Clique em **Dispositivos**. Os drivers de dispositivo e seus tipos de inicialização são listados.
erros de E/S	Ao tentar definir ou usar um dispositivo de fita, pode haver conflitos de drivers de dispositivo. Os drivers de dispositivo do Windows e os drivers que forem fornecidos por outros aplicativos poderão interferir com o driver de dispositivo do IBM Spectrum Protect se ele não for iniciado primeiro.	

Linux Não é possível priorizar o conflito de reserva de unidade de fita com a Reserva Persistente na plataforma Linux.	Linux Em uma plataforma Linux, o agente de armazenamento ou o servidor do IBM Spectrum Protect requer que o driver de dispositivo lin_tape da IBM esteja configurado para Reserva Persistente e que um pseudoarquivo de dispositivo IBM `/dev/TSMtape` seja criado.	Linux Se o failover do caminho de dados estiver ativado no driver lin_tape da IBM, o arquivo `/dev/TSMtape` será criado automaticamente e a Reserva Persistente poderá ser usada. Como alternativa, configure a Reserva Persistente para a reserva de unidade de fita em uma plataforma Linux de acordo com o procedimento a seguir:
		Dica: Por padrão, o driver de dispositivo lin_tape da IBM usa a reserva SCSI-2 para reservar unidades de fita.
		Linux
		1. Descarregue o driver de dispositivo lin_tape da IBM.
		2. No arquivo de configuração lin_tape `/etc/modprobe.conf` ou `/etc/modprobe.conf.local` (ou, se você estiver executando o RHEL 6 ou mais recente, o `/etc/modprobe.d/lin_tape.conf`), inclua a linha a seguir:
		`options lin_tape tape_reserve_type=persistent`
		3. No arquivo de regras `/etc/udev/rules.d/98-lin_tape.rules`, inclua a linha a seguir:
		`KERNEL=="TSMtape", MODE="0666"`
		4. Recarregue o driver de dispositivo lin_tape da IBM.
		Linux O pseudoarquivo `/dev/TSMtape` da IBM é criado e o servidor IBM Spectrum Protect pode usar a Reserva Persistente para priorizar a reserva de unidade de fita nas plataformas Linux.

Concluindo a implementação

Após a solução IBM Spectrum Protect estar configurada e em execução, teste as operações de backup e configure o monitoramento para assegurar que tudo seja executado corretamente.

Procedimento

1. Teste as operações de backup para verificar se seus dados estão protegidos como você espera.
   a) Na página **Clientes** do Operations Center, selecione os clientes do qual deseja fazer backup e clique em **Fazer backup**.
   b) Na página **Servidores** do Operations Center, selecione o servidor para o qual deseja fazer backup do banco de dados. Clique em **Fazer backup** e siga as instruções na janela **Fazer backup do banco de dados**.
   c) Verifique se as operações de backup foram concluídas com sucesso sem nenhum aviso ou mensagens de erro.

      Dica: Como alternativa, é possível usar a GUI do cliente de backup-archive para fazer backup de dados do cliente e é possível fazer backup do banco de dados do servidor emitindo o comando **BACKUP DB** de uma linha de comandos administrativa.
2. Configure o monitoramento para sua solução seguindo as instruções em Parte 3, “Monitorando uma solução de fita”, na página 133.

Parte 3. Monitorando uma solução de fita

Monitore sua solução baseada em fita para assegurar a operação correta.

Sobre Esta Tarefa

Depois de implementar sua solução de fita com o IBM Spectrum Protect, monitore a solução diariamente e periodicamente para identificar problemas existentes e potenciais. As informações reunidas podem ser usadas para resolver problemas e otimizar o desempenho do sistema. A maneira preferencial de monitorar uma solução é usar o Operations Center, que fornece um status do sistema geral e detalhado em uma interface gráfica com o usuário. Além disso, é possível configurar o Operations Center para gerar relatórios de e-mail que resumem o status do sistema.

Procedimento

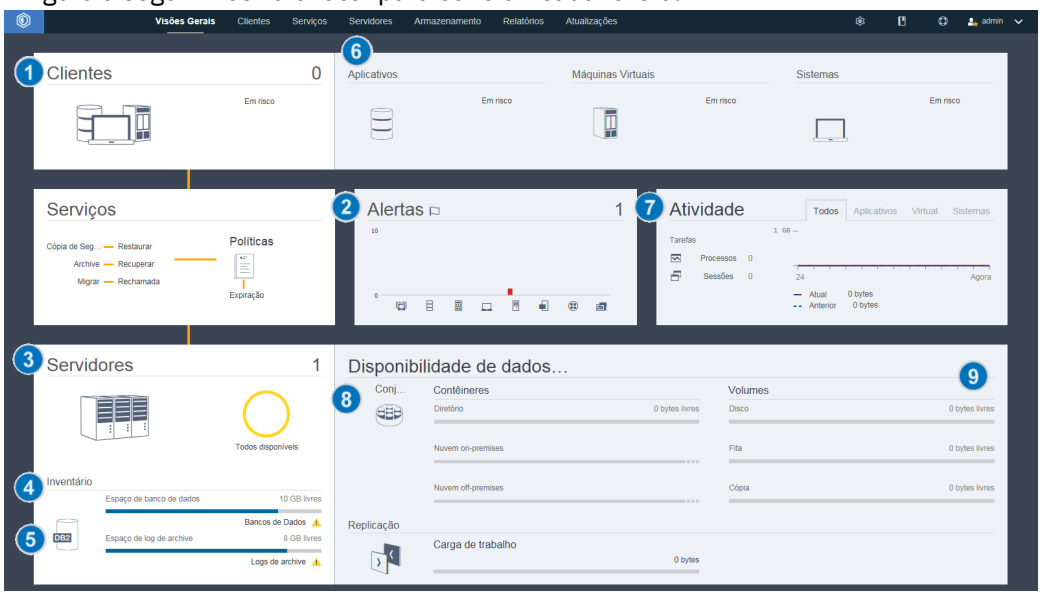
1. Concluir tarefas de monitoramento diárias. Para obter instruções, consulte Lista de verificação de monitoramento diário.
2. Concluir tarefas de monitoramento periódicas. Para obter instruções, consulte Lista de verificação de monitoramento periódico.
3. Verifique se seu sistema está em conformidade com os requisitos de licenciamento. Para obter instruções, consulte Verificando a conformidade da licença.
4. Opcional: Configure relatórios de e-mail de status do sistema. Para obter instruções, consulte “Rastreando o status do sistema usando relatórios de e-mail” na página 154

Lista de verificação de monitoramento diária

Para assegurar que você esteja concluindo as tarefas diárias de monitoramento para sua solução IBM Spectrum Protect, revise a lista de verificação diária de monitoramento.

Conclua as tarefas de monitoramento diário por meio da página de **Visão geral** do Operations Center. É possível acessar a página **Visão geral** abrindo o Operations Center e clicando em **Visões gerais**.

A figura a seguir mostra o local para concluir cada tarefa.



Dica: Para executar comandos administrativos para tarefas de monitoramento avançado, use o construtor de comando do Operations Center. O construtor de comando fornece uma função de digitação

antecipada para orientá-lo conforme você insere comandos. Para abrir o construtor de comando, acesse a página de Operations Center **Visão geral**. Na barra de menus, passe o mouse sobre o ícone de configurações  e clique em **Construtor de Comando**.

A tabela a seguir lista as tarefas de monitoramento de diárias e fornece instruções para concluir cada tarefa.

Tabela 27. Tarefas de monitoramento diárias

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
Observe as notificações de segurança, que podem indicar um ataque de ransomware.	Se um ataque de ransomware em potencial for detectado no ambiente do IBM Spectrum Protect, uma mensagem de notificação de segurança será exibida no primeiro plano do Operations Center. Para obter mais informações, clique na mensagem para abrir a página **Notificações de segurança**.	Na página **Notificações de segurança**, é possível tomar as ações a seguir: • Visualizar detalhes de notificação por cliente. **Restrição:** As notificações estão disponíveis apenas para os clientes de backup e archive e os clientes do Ambientes IBM Spectrum Protect for Virtual. • Reconhecer uma notificação de segurança selecionando-a e clicando em **Reconhecer**. Quando você reconhece uma notificação de segurança, um visto é incluído na coluna Reconhecido da página **Notificações de segurança** para o cliente selecionado. O padrão pelo qual uma notificação é reconhecida é determinado por sua organização. Um visto pode significar que você investigou o problema e determinou que ele é um falso positivo. Ou pode significar que um problema existe e está sendo resolvido. • Designar uma notificação de segurança para um administrador selecionando a notificação de segurança e clicando em **Designar**. Para visualizar a designação, o administrador deve conectar-se ao Operations Center e clicar em **Visões gerais** > **Segurança**. Se você não tiver certeza de que o administrador monitora regularmente a página **Notificações de segurança**, notifique o administrador sobre a designação. • Se a notificação for um falso positivo, será possível selecionar a notificação de segurança e clicar em **Reconfigurar**. A notificação de segurança é excluída. Os dados históricos que são usados para comparações de linha de base com a operação de backup mais recente são excluídos. Uma nova linha de base é calculada daí em diante. • Opcionalmente, é possível desativar as notificações de segurança usando o comando **SET SECURITYNOTIF**.

Tabela 27. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
1 Determine se os clientes correm risco de ficarem desprotegidos devido a operações de backup com falha ou ausentes.	Para verificar se os clientes estão em risco, na área de Clientes, procure uma notificação **Em risco**. Para visualizar detalhes, clique na área Clientes.  **Atenção:** Se a porcentagem **Em risco** for muito maior do que o normal, isso poderá indicar um ataque de ransomware. Um ataque de ransomware pode fazer com que as operações de backup falhem, colocando os clientes em risco. Por exemplo, se a porcentagem de clientes em risco normalmente estiver entre 5% e 10%, mas aumentar para 40% ou 50%, investigue a causa. Se você instalou o serviço de gerenciamento de clientes em um cliente de backup-archive, será possível visualizar e analisar os logs de erro e de planejamento, concluindo as etapas a seguir: 1. Na tabela Clientes, selecione o cliente e clique em **Detalhes**. 2. Para diagnosticar um problema, clique em **Diagnóstico**.	Para clientes que não têm o serviço de gerenciamento de clientes instalado, acesse o sistema do cliente para revisar os logs de erro do cliente.
2 Determine se os erros relacionados ao cliente ou ao servidor requerem atenção.	Para determinar a gravidade de qualquer um dos alertas relatados, na área Alertas, passe o mouse sobre as colunas.	Para visualizar informações adicionais sobre alertas, conclua as etapas a seguir: 1. Clique na área Alertas. 2. Na tabela Alertas, selecione um alerta. 3. Na área de janela Log de atividades, revise as mensagens. A área de janela exibe mensagens relacionadas que foram emitidas antes e após o alerta selecionado ter ocorrido.
3 Determine se os servidores que são gerenciados pelo Operations Center estão disponíveis para fornecer serviços de proteção de dados para clientes.	1. Para verificar se os servidores estão em risco, na área Servidores, procure uma notificação **Indisponível**. 2. Para visualizar informações adicionais, clique na área Servidores. 3. Selecione um servidor na tabela Servidores e clique em **Detalhes**.	**Dica:** Se você detectar um problema que está relacionado às propriedades do servidor, atualize as propriedades do servidor: 1. Na tabela Servidores, selecione um servidor e clique em **Detalhes**. 2. Para atualizar propriedades do servidor, clique em **Propriedades**.

Tabela 27. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
4 Determine se há espaço suficiente disponível para o inventário do servidor, que consiste no banco de dados do servidor, no log ativo e no log de archive.	1. Clique na área Servidores. 2. Na coluna Status da tabela, visualize o status do servidor e resolva os problemas: • **Normal** Há espaço suficiente disponível para o banco de dados do servidor, o log ativo e o log de archive. • **Crítico** Não há espaço suficiente disponível para o banco de dados do servidor, o log ativo ou o log de archive. Deve-se incluir espaço imediatamente ou os serviços de proteção de dados que são fornecidos pelo servidor serão interrompidos. • **Aviso** O banco de dados do servidor, o log ativo ou o log de archive estão sem espaço. Se essa condição persistir, deve-se incluir espaço. • **Indisponível** O status não pode ser obtido. Certifique-se de que o servidor esteja em execução e que não haja problemas de rede. Este status também será mostrado se o ID de administrador de monitoramento estiver bloqueado ou, de outra forma, indisponível no servidor. Este ID é denominado IBM-OC-hub_server_name. • **Não monitorado** Os servidores não monitorados estão definidos para o servidor do hub, mas não estão configurados para gerenciamento pelo Operations Center. Para configurar um servidor não monitorado, selecione o servidor e clique em **Monitorar spoke**.	Também é possível procurar alertas relacionados na página **Alertas**. Para obter instruções adicionais sobre resolução de problemas, consulte Resolvendo Problemas do Servidor.

Tabela 27. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
5 Verifique as operações de backup de banco de dados do servidor.	Para determinar quando um servidor foi submetido a backup mais recentemente, conclua as etapas a seguir: 1. Clique na área Servidores. 2. Na tabela Servidores, revise a coluna Último backup de banco de dados.	Para obter informações mais detalhadas sobre as operações de backup, conclua as etapas a seguir: 1. Na tabela Servidores, selecione uma linha e clique em **Detalhes**. 2. Na área Backup do BD, passe o mouse sobre as marcas de seleção para revisar informações sobre operações de backup. Se um banco de dados não foi submetido a backup recentemente (por exemplo, nas últimas 24 horas), é possível iniciar uma operação de backup: 1. Na página de Operations Center **Visão geral**, clique na área Servidores. 2. Na tabela, selecione um servidor e clique em **Fazer backup**. Para determinar se o banco de dados do servidor está configurado para operações de backup automático, conclua as etapas a seguir: 1. Na barra de menus, passe o mouse sobre o ícone de configurações e clique em **Construtor de Comando**. 2. Emita o comando **QUERY DB**: `query db f=d` 3. Na saída, revise o campo `Nome completo da classe de dispositivo`. Se uma classe de dispositivo for especificada, o servidor será configurado para backups de banco de dados automáticos.
6 Monitore outras tarefas de manutenção de servidor. As tarefas de manutenção de servidor podem incluir a execução de planejamentos de comandos administrativos, de scripts de manutenção e de comandos relacionados.	Para procurar informações sobre processos que falharam devido a problemas do servidor, conclua as etapas a seguir: 1. Clique em **Servidores** > **Manutenção**. 2. Para obter o histórico de duas semanas de um processo, visualize a coluna Histórico. 3. Para obter mais informações sobre um processo planejado, passe o mouse sobre a caixa de seleção que está associada ao processo.	Para obter informações adicionais sobre como monitorar processos e resolver problemas, consulte a ajuda online do Operations Center.

Tabela 27. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
7 Verifique se a quantidade de dados que foram enviados recentemente para e de servidores está dentro do intervalo esperado.	• Para obter uma visão geral de atividade nas últimas 24 horas, visualize a área Atividade. • Para comparar a atividade nas últimas 24 horas com a atividade nas 24 horas anteriores, revise as figuras nas áreas Atual e Anterior.	• Se foram enviados ao servidor mais dados do que o esperado, determine quais clientes estão fazendo backup de mais dados e investigue a causa. É possível que a deduplicação de dados do lado do cliente não esteja funcionando corretamente.  **Atenção:** Se a quantidade de dados de backup é significativamente maior que o normal, isso pode indicar um ataque de ransomware. Quando o ransomware criptografa dados, o sistema detecta os dados como sendo mudados e tais dados mudados são submetidos a backup. Assim, volumes de backup se tornam maiores. Para determinar quais clientes são afetados, clique na guia **Aplicativos**, **Máquinas virtuais** ou **Sistemas**. • Se foram enviados ao servidor menos dados do que o esperado, investigue se as operações de backup do cliente continuam dentro do planejamento.

Tabela 27. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
8 Verifique se os conjuntos de armazenamentos estão disponíveis para fazer backup de dados de cliente.	1. Se os problemas forem indicados na área Armazenamento e Disponibilidade de dados, clique em **Conjuntos** para visualizar os detalhes: • Se o status **Crítico** for exibido, não há espaço suficiente disponível no conjunto de armazenamentos ou seu status de acesso está indisponível. **Atenção:** Se o status for crítico, investigue a causa: – Se a taxa de deduplicação de dados para um conjunto de armazenamentos cair significativamente, isso poderá indicar um ataque de ransomware. Durante um ataque de ransomware, os dados são criptografados e não podem ser deduplicados. Para verificar a taxa de deduplicação de dados, na tabela Conjuntos de Armazenamento, revise o valor na coluna % de Economia. – Se um conjunto de armazenamento inesperadamente torna-se 100% utilizado, isso pode indicar um ataque de ransomware. Para verificar a utilização, revise o valor na coluna Capacidade Utilizada. Passe o mouse sobre os valores para ver as porcentagens de espaço usado e livre. • Se o status **Aviso** for exibido, o conjunto de armazenamentos está sem espaço ou seu status de acesso é somente leitura. 2. Para visualizar o espaço usado, livre e total para seu conjunto de armazenamentos selecionado, passe o mouse sobre as entradas na coluna Capacidade utilizada.	Para visualizar a capacidade do conjunto de armazenamentos que foi usada nas últimas duas semanas, selecione uma linha na tabela Conjuntos de armazenamentos e clique em **Detalhes**.

Tabela 27. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
9 Verifique se os dispositivos de armazenamento estão disponíveis para operações de backup.	Na área Armazenamento e disponibilidade de dados, na seção Volumes, sob as barras de capacidade, revise o status que é suportado, ao lado de **Dispositivos**. Se um status **Crítico** ou **Aviso** for exibido para qualquer dispositivo, investigue o problema. Para visualizar detalhes, clique em **Dispositivos**.	Os dispositivos de fita podem apresentar o status de aviso ou crítico quando as unidades estão indisponíveis. Uma unidade estará indisponível se estiver off-line, tiver parado de responder ao servidor ou se seu caminho estiver off-line. Um dispositivo de fita também pode apresentar o status crítico quando a biblioteca está off-line. Outras colunas da tabela Dispositivos de fita mostram o estado das robóticas, das unidades e dos caminhos da biblioteca. Para resolver problemas com unidades de fita que têm um estado crítico, é possível tornar a unidade off-line se for preciso usá-la para outra atividade, como manutenção. Para tornar uma unidade off-line, conclua as seguintes etapas: 1. Na página Operations Center**Armazenamento**, selecione Dispositivos de fita. 2. Para visualizar informações adicionais sobre uma biblioteca de fitas, selecione uma linha e clique em **Detalhes**. 3. Para tornar uma unidade off-line, selecione a unidade de fita e clique em **Off-line**. Para operações de fita de backup, verifique se há fitas utilizáveis suficientes disponíveis. Se você não tiver certeza que o número de fitas utilizáveis disponíveis é suficiente, abra as anotações de detalhes para visualizar o uso de fita e uma estimativa da disponibilidade de fita utilizável. Para abrir as anotações, selecione uma biblioteca na tabela e clique em Detalhes.

Tabela 27. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
10 Monitorar conjuntos de retenção.	Para obter o status geral dos conjuntos de retenção, visualize a área de **Conjuntos de retenção** na página de Operations Center **Visão geral**: • O campo **Concluído** especifica o número de conjuntos de retenção que foram criados no banco de dados do servidor e que são rastreados no inventário do servidor. • O campo **Concluído** especifica o número de conjuntos de retenção que possuem dados expirados. • O campo **Excluído** especifica o número de conjuntos de retenção que foram excluídos. Para visualizar ou modificar as regras de retenção, clique em **Serviços** > **Regras de retenção**.	Para obter mais informações sobre os conjuntos de retenção, clique na área **Conjuntos de retenção** para abrir a página **Conjuntos de retenção**. Para visualizar ou modificar as propriedades de conjuntos de retenção, dê um clique duplo em um conjunto de retenção. Para obter informações mais detalhadas, é possível executar comandos relacionados: 1. Na página de Operations Center **Visão geral**, passe o mouse sobre o ícone de configurações e clique em **Construtor de Comando**. 2. Para determinar quais tarefas de criação de conjunto de retenção estão em execução, interrompidas ou concluídas, execute o comando **QUERY JOB**. Para obter instruções, consulte QUERY JOB (Consultar uma tarefa de criação do conjunto de retenção). 3. Para consultar regras de retenção, execute o comando **QUERY RETRULE**. Para obter instruções, consulte QUERY RETRULE (Consultar uma regra de retenção). 4. Para consultar conjuntos de retenção, execute o comando **QUERY RETSET**. Para obter instruções, consulte QUERY RETSET (Consultar um conjunto de retenção). 5. Para consultar o conteúdo de conjuntos de retenção, execute o comando **QUERY RETSETCONTENTS**. Para obter instruções, consulte QUERY RETSETCONTENTS (Consultar os conteúdos de um conjunto de retenção).

Tabela 27. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
11 Monitorar regras de armazenamento.	Para obter o status geral das operações de regra de armazenamento, visualize a área de **Regras de armazenamento** na página de Operations Center **Visão geral**.	O resumo de status mostra os resultados de processamento mais recentes para as regras de armazenamento. O número de regras de armazenamento em cada um dos estados a seguir é mostrado: **Normal** O número de regras de armazenamento que foram executadas sem erros. **Aviso** O número de regras de armazenamento que concluíram o processamento, mas não moveram ou copiaram todos os dados elegíveis. Alguns arquivos foram ignorados, o limite de tempo da regra foi atingido ou o processo foi cancelado. **Com Falha** O número de regras de armazenamento que não concluíram o processamento. Por exemplo, o servidor pode falhar ao processar dados porque o conjunto de armazenamentos de destino tem espaço insuficiente ou porque o servidor não pode acessar o conjunto de armazenamentos. **Outros estados** O número de regras de armazenamento em outros estados. O servidor no qual a regra de armazenamento é definida pode estar indisponível para fornecer os dados ou pode estar executando uma versão anterior de IBM Spectrum Protect que não suporta o status. O status pode não ser aplicável porque a regra de armazenamento não foi ativada ou não foi executada. **Dica:** Um ícone será exibido apenas se uma ou mais regras de armazenamento estiverem no estado correspondente. Para visualizar informações mais detalhadas sobre cada regra de armazenamento, clique em **Regras de armazenamento** para abrir a página **Regras de armazenamento**.

Lista de verificação de monitoramento periódica

Para ajudar a assegurar que as operações sejam executadas corretamente, conclua as tarefas na lista de verificação de monitoramento periódico. Planeje tarefas periódicas com frequência suficiente para que seja possível detectar possíveis problemas antes que eles se tornem problemáticos.

Dica: Para executar comandos administrativos para tarefas de monitoramento avançado, use o construtor de comando do Operations Center. O construtor de comando fornece uma função de digitação antecipada para orientá-lo conforme você insere comandos. Para abrir o construtor de comando, acesse a página de Operations Center **Visão geral**. Na barra de menus, passe ou mouse sobre o ícone de configurações  e clique em **Construtor de comando**.

Tabela 28. Tarefas de monitoramento periódicas

Tarefa	Procedimentos básicos	Procedimentos avançados e resolução de problemas
Monitore o desempenho do sistema.	Determine o período de tempo necessário para operações de backup do cliente: 1. Na página Operations Center **Visão geral**, clique em **Clientes**. Localize o servidor que está associado ao cliente. 2. Clique em **Servidores**. Selecione o servidor e clique em **Detalhes**. 3. Para visualizar a duração de tarefas concluídas nas últimas 24 horas, clique em **Tarefas concluídas**. 4. Para visualizar a duração de tarefas que foram concluídas mais de 24 horas atrás, use o comando **ACTLOG QUERY**. Para obter informações sobre esse comando, consulte QUERY ACTLOG (Consultar o log de atividades). 5. Se a duração de operações de backup do cliente estiver aumentando e as razões não forem claras, investigue a causa. Se você instalou o serviço de gerenciamento de clientes em um cliente de backup-archive, será possível diagnosticar problemas de desempenho para o cliente de backup-archive concluindo as etapas a seguir: 1. Na página Operations Center **Visão geral**, clique em **Clientes**. 2. Selecione um cliente de backup-archive e clique em **Detalhes**. 3. Para recuperar logs do cliente, clique em **Diagnóstico**.	Limitar o tempo para operações de backup de cliente para 8 a 12 horas. Certifique-se de que os planejamentos de cliente não se sobreponham com tarefas de manutenção de servidor. Para obter instruções sobre como reduzir o tempo que leva para o cliente fazer backup de dados para o servidor, consulte Resolvendo problemas de desempenho comuns do cliente. Procure gargalos de desempenho. Para obter instruções, consulte Identificando gargalos de desempenho. Para obter informações sobre como identificar e resolver outros problemas de desempenho, consulte Desempenho.

Tabela 28. Tarefas de monitoramento periódicas (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e resolução de problemas

Verifique se os arquivos de backup atuais para configuração do dispositivo e informações do histórico do volume foram salvos.	Acesse os locais de armazenamento para assegurar que os arquivos estejam disponíveis. O método preferencial é salvar os arquivos de backup em dois locais.
	
	Para localizar o histórico do volume e arquivos de configuração de dispositivo, conclua as etapas a seguir:
	
	1. Na página Operations Center **Visão geral**, passe o mouse sobre o ícone de configurações e clique em **Construtor de comando**.
	2. Para localizar o histórico do volume e arquivos de configuração de dispositivo, emita os seguintes comandos:
	
	`query option volhistory`
	
	`query option devconfig`
	
	3. Na saída, revise a coluna Configuração de opção para localizar os locais do arquivo.
	
	Se ocorrer um desastre, o arquivo do histórico de volume e o arquivo de configuração de dispositivo serão necessários para restaurar o banco de dados do servidor.	

Tabela 28. Tarefas de monitoramento periódicas (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e resolução de problemas

Determine se há espaço suficiente disponível no diretório para a instância do servidor.	Verifique se há pelo menos 50 GB de espaço livre disponível no diretório para a instância do servidor. Execute a ação apropriada para seu sistema operacional:
	• AIX Para visualizar o espaço disponível no sistema de arquivos, na linha de comandos do sistema operacional, emita o seguinte comando:
	`df -g instance_directory`
	em que *instance_directory* especifica o diretório de instâncias.
	• Linux Para visualizar o espaço disponível no sistema de arquivos, na linha de comandos do sistema operacional, emita o seguinte comando:
	`df -h instance_directory`
	em que *instance_directory* especifica o diretório de instâncias.
	• Windows No programa Windows Explorer, clique com o botão direito no sistema e clique em **Propriedades**. Visualize as informações de capacidade.
	O local preferido do diretório de instâncias depende do sistema operacional em que o servidor está instalado:
	• Linux AIX `/home/tsminst1/tsminst1`
	• Windows `C:\tsminst1`
	Dica: Se você concluiu uma planilha de planejamento, o local do diretório de instâncias será registrado na planilha.	

Tabela 28. Tarefas de monitoramento periódicas (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e resolução de problemas
Identifique a atividade do cliente inesperada.	Para monitorar a atividade de cliente para determinar se os volumes de dados excederam as quantidades esperadas, conclua as etapas a seguir: 1. Na página Operations Center **Visão geral** , clique na área Clientes. 2. Para visualizar a atividade durante as duas últimas semanas, dê um clique duplo em qualquer cliente. 3. Para visualizar o número de bytes enviados ao cliente, clique na guia **Propriedades**. 4. Na área Última sessão, visualize a linha Enviados ao cliente.	Ao dar um clique duplo em um cliente na tabela Clientes, a área **Atividade durante 2 semanas** exibe a quantidade de dados que o cliente enviou ao servidor a cada dia. Revise periodicamente a tabela de resumo de atividade SQL que contém estatísticas sobre sessões do cliente. Para comparar a atividade atual com a atividade anterior, use uma instrução SQL SELECT. Se o nível de atividade for significativamente diferente da atividade anterior, isso poderá indicar um ataque de ransomware. Periodicamente, revise o log de atividades. Procure mensagens ANE que indiquem quantos arquivos foram submetidos a backup e inspecionados. Compare as taxas atuais de deduplicação de dados com as taxas anteriores. Se um número extraordinariamente alto de arquivos foi submetido a backup ou a taxa de deduplicação de dados cai inesperadamente para 0, isso pode indicar um ataque de ransomware.

Tabela 28. Tarefas de monitoramento periódicas (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e resolução de problemas
Monitore o crescimento do conjunto de armazenamentos ao longo do tempo.	1. Na página Operations Center **Visão geral**, clique na área Conjuntos. 2. Para visualizar a capacidade que foi usada durante as duas últimas semanas, selecione um conjunto e clique em **Detalhes**.	**Dicas:** • Para especificar o período que deve decorrer até que todas as extensões deduplicadas sejam removidas de um conjunto de armazenamentos de contêiner de diretório ou de um conjunto de armazenamentos de contêiner em nuvem após não serem mais referenciadas pelo inventário, conclua as seguintes etapas: 1. Na página **Conjuntos de armazenamentos** do Operations Center, selecione o conjunto de armazenamentos. 2. Clique em **Detalhes** > **Propriedades**. 3. Especifique a duração no campo `Período de atraso para reutilização do contêiner`. • Para determinar o desempenho da deduplicação de dados para conjuntos de armazenamentos de contêiner em diretório e de contêiner em nuvem, use o comando **`GENERATE DEDUPSTATS`**. • Para visualizar estatísticas de deduplicação de dados para um conjunto de armazenamentos, conclua as seguintes etapas: 1. Na página **Conjuntos de armazenamentos** do Operations Center, selecione o conjunto de armazenamentos. 2. Clique em **Detalhes** > **Propriedades**. Como alternativa, use o comando **QUERY EXTENTUPDATES** para exibir informações sobre atualizações em extensões de dados em conjuntos de armazenamentos de contêiner em diretório e de contêiner em nuvem. A saída de comando pode ajudá-lo a determinar quais extensões de dados não são mais referenciadas e quais são elegíveis para serem excluídas do sistema. Na saída, monitore o número de extensões de dados que podem ser excluídas do sistema. Essa métrica tem uma correlação direta com a quantia de espaço livre que está disponível no conjunto de armazenamentos de contêiner. • Para exibir a quantidade de espaço físico que é ocupada por um espaço de arquivo após a remoção da economia da deduplicação de dados, use o comando **`select * from occupancy`**. A saída de comando inclui o valor LOGICAL_MB. LOGICAL_MB é a quantidade de espaço

Tabela 28. Tarefas de monitoramento periódicas (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e resolução de problemas
Monitore e mantenha dispositivos de fita.	Monitore seu ambiente para erros de hardware em unidades e bibliotecas de fitas. Para obter instruções, consulte “Monitorando mensagens de alerta de fita para erros de hardware” na página 151. Monitore a compatibilidade de mídia para evitar erros nas unidades de fita. Para obter instruções, consulte “Evitando erros causados por incompatibilidade de mídia” na página 152. Monitore as mensagens de limpeza para unidades de fita. Para obter instruções, consulte “Operações com cartuchos de limpeza” na página 152.	
Avalie a sincronização dos planejamentos de cliente. Certifique-se de que os horários de início e de encerramento de planejamentos de cliente não se sobreponham com tarefas de manutenção do servidor. Limite o tempo para operações de backup do cliente para 8 a 12 horas.	Na página Operations Center **Visão geral**, clique em **Clientes** > **Planejamentos**. Na tabela Planejamentos, a coluna Início exibe o horário de início configurado para a operação planejada. Para ver quando a operação mais recente foi iniciada, passe o mouse sobre o ícone de relógio.	**Dica:** É possível receber uma mensagem de aviso se uma operação do cliente for executada por mais tempo que o esperado. Execute as etapas a seguir: 1. Na página Visão geral do Operations Center, passe o mouse sobre **Clientes** e clique em **Planejamentos**. 2. Selecione um planejamento e clique em **Detalhes**. 3. Visualize os detalhes de um planejamento clicando na seta azul próxima à linha. 4. No campo **Alerta de tempo de execução**, especifique o horário em que uma mensagem de aviso será emitida se a operação planejada não for concluída. 5. Clique em **Salvar**.

Tabela 28. Tarefas de monitoramento periódicas (continuação)		
Tarefa	**Procedimentos básicos**	**Procedimentos avançados e resolução de problemas**
Avalie a sincronização das tarefas de manutenção. Certifique-se de que os horários de início e de encerramento de tarefas de manutenção não se sobreponham com planejamentos de cliente.	Na página Operations Center **Visão geral**, clique em **Servidores** > **Manutenção**. Na tabela Manutenção, revise as informações na coluna Último tempo de execução. Para ver quando a última tarefa de manutenção foi iniciada, passe o mouse sobre o ícone de relógio.	O método preferencial é assegurar que cada tarefa de manutenção seja executada até a conclusão antes do início da próxima tarefa de manutenção. Exemplos de tarefas de manutenção incluem expiração de inventário, cópia de conjuntos de armazenamentos, recuperação de espaço e backup de banco de dados. **Dica:** Se uma tarefa de manutenção demorar muito tempo para executar, mude o horário de início e o tempo de execução máximo. Execute as etapas a seguir: 1. Na página Operations Center **Visão geral**, passe o mouse sobre o ícone de configurações e clique em **Construtor de comando**. 2. Para mudar o horário de início ou o tempo de execução máximo para uma tarefa, emita o comando **UPDATE SCHEDULE**. Para obter informações sobre esse comando, consulte UPDATE SCHEDULE (Atualizar um planejamento do cliente).

Informações relacionadas

QUERY ACTLOG (Consultar o log de atividades)

Monitorando mensagens de alerta de fita para erros de hardware

Mensagens de alerta de fita são geradas por dispositivos de fita e de biblioteca para relatar erros de hardware. Essas mensagens ajudam a determinar problemas que não estão relacionados ao servidor.

Sobre Esta Tarefa

Uma página de log é criada e pode ser recuperada a qualquer momento ou em um momento específico, como quando uma unidade é desmontada.

Uma mensagem de alerta de fita pode ter um dos seguintes níveis de severidade:

- Informativo (por exemplo, tentando carregar um tipo de cartucho que não é suportado)
- Aviso (por exemplo, uma falha no hardware é predita)
- Crítico (por exemplo, há um problema com a fita e os dados estão em risco)

Mensagens de alerta de fita são desativadas por padrão.

Procedimento

- Para ativar as mensagens de alerta de fita, emita o comando **SET TAPEALERTMSG** e especifique o valor **ON**: `set tapealertmsg on`
- Para verificar se as mensagens de alerta de fita estão ativadas, emita o comando **QUERY TAPEALERTMSG**: `query tapealertmsg`

Evitando erros causados por incompatibilidade de mídia

Ao monitorar e resolver problemas de compatibilidade de mídia, será possível evitar erros em uma solução baseada em fita. Uma nova unidade pode ter uma capacidade limitada para usar formatos de mídia que sejam suportados por uma versão anterior da unidade. Geralmente, uma nova unidade pode ler, mas não gravar no formato de mídia anterior.

Sobre Esta Tarefa

Por padrão, os volumes existentes com um status de FILLING permanecem nesse estado após um upgrade da unidade. Em alguns casos, talvez você queira continuar a usar uma unidade anterior para preencher esses volumes. Isso preserva a capacidade de leitura/gravação para os volumes existentes até que eles sejam recuperados. Se optar por fazer upgrade de todas as unidades em uma biblioteca, verifique se os formatos de mídia são suportados pelo novo hardware. A menos que você planeja usar somente a mídia mais atual com a sua nova unidade, é necessário estar atento à qualquer problema de compatibilidade. Para obter instruções sobre migração, consulte "Migrando dados para unidades com upgrade" na página 205.

Para usar uma nova unidade com uma mídia que possa ser lida, mas não gravada, emita o comando **UPDATE VOLUME** para configurar o acesso a esses volumes para somente leitura. Isso evita erros que são causados por incompatibilidade de leitura/gravação. Por exemplo, uma nova unidade poderá ejetar mídia que é gravada em um formato que a unidade não suporta assim que a mídia estiver carregada na unidade. Ou uma nova unidade poderá falhar no primeiro comando de gravação para a mídia parcialmente gravada em um formato que a unidade não suporta.

Quando os dados na mídia somente leitura expiram e o volume é recuperado, substitua-o pela mídia que seja totalmente compatível com a nova unidade. Erros poderão ser gerados se uma nova unidade for incapaz de calibrar corretamente um volume que é gravado ao usar um formato anterior. Para evitar esse problema, certifique-se de que a unidade original esteja em boas condições de funcionamento e nos níveis de microcódigo atuais.

Operações com cartuchos de limpeza

Para assegurar que as unidades de fita sejam limpas quando necessário e para evitar problemas com armazenamento em fita, siga estas diretrizes.

Monitorando o processo de limpeza

Se um cartucho de limpeza estiver registrado em uma biblioteca e uma unidade tiver que ser limpa, o servidor desmontará o volume de dados e executará a operação de limpeza. Se a operação de limpeza falhar ou for cancelada ou se nenhum cartucho de limpeza estiver disponível, talvez você não saiba que a unidade precisa de limpeza. Monitore as mensagens de limpeza para esses problemas para assegurar que as unidades sejam limpas, conforme necessário. Se necessário, emita o comando **CLEAN DRIVE** para que o servidor tente a limpeza novamente ou carregue manualmente um cartucho de limpeza na unidade.

Usando múltiplos cartuchos de limpeza

O servidor usa um cartucho de limpeza para o número de limpezas que você especifica ao efetuar check-in do cartucho de limpeza. Se efetuar check-in de dois ou mais cartuchos de limpeza, o servidor usará apenas um dos cartuchos até que o número designado de limpeza para esse cartucho seja atingido. Em seguida, o servidor usa o próximo cartucho de limpeza. Se você efetuar check-in de dois ou mais cartuchos de limpeza e emitir dois ou mais comando **CLEAN DRIVE** simultaneamente, o servidor usará múltiplos cartuchos ao mesmo tempo e diminuirá as limpezas restantes em cada cartucho.

Informações relacionadas

AUDIT LIBRARY (Auditar inventários de volume em uma biblioteca automatizada)
CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)
CLEAN DRIVE (Limpar uma Unidade)
LABEL LIBVOLUME (Rotular um volume de biblioteca)
QUERY LIBVOLUME (Consultar um volume de biblioteca)

Verificando a conformidade da licença

Verifique se a solução do IBM Spectrum Protect está em conformidade com as disposições de seu contrato de licença. Ao verificar a conformidade regularmente, é possível controlar as tendências em crescimento de dados ou no uso da unidade de valor do processador (PVU). Use essas informações para planejar uma futura compra de licença.

Sobre Esta Tarefa

O método a ser usado para verificar se sua solução está em conformidade com os termos da licença varia de acordo com as disposições de seu contrato de licença do IBM Spectrum Protect.

Licenciamento de capacidade front-end

O modelo front-end determina os requisitos de licença com base na quantidade de dados primários que são relatados como sendo submetidos a backup por clientes. Os clientes incluem aplicativos, máquinas virtuais e sistemas.

Licenciamento de capacidade back-end

O modelo de backend determina os requisitos de licença com base nos terabytes de dados que são armazenados em conjuntos de armazenamentos primários e repositórios.

Dicas:

- Para assegurar a exatidão das estimativas de capacidade de front-end e backend, instale a versão mais recente do software cliente em cada nó cliente.
- As informações de capacidade de front-end e backend no Operations Center são para propósitos de planejamento e estimação.

Licenciamento de PVU

O modelo PVU é baseado no uso de PVUs por dispositivos do servidor.

Importante: Os cálculos de PVU que são fornecidos pelo IBM Spectrum Protect são considerados estimativas e não são ligados legalmente. As informações sobre licença de PVU que são relatadas pelo IBM Spectrum Protect não são consideradas um substituto aceitável para o IBM License Metric Tool. O IBM License Metric Tool foi desenvolvido para refletir o uso real. Por exemplo, após instalar o Cliente de backup e archive do IBM Spectrum Protect, a ferramenta conta o cliente somente após o primeiro uso. Para obter mais informações sobre a IBM License Metric Tool, consulte IBM License Metric Tool.

Se você tiver perguntas ou dúvidas sobre requisitos de licenciamento, entre em contato com o provedor de software do IBM Spectrum Protect.

Procedimento

Para monitorar a conformidade da licença, conclua as etapas que correspondem aos as disposições de seu contrato de licença.

Dica: O Operations Center fornece um relatório de e-mail que resume o uso de capacidade de front-end e backend. Os relatórios podem ser enviados automaticamente para um ou mais destinatários regularmente. Para configurar e gerenciar relatórios de e-mail, clique em **Relatórios** na barra de menus do Operations Center.

Opção	Descrição
Modelo front-end	a. Na barra de menus do Operations Center, passe o mouse sobre o ícone de configurações  e clique em **Licenciamento**. A estimativa de capacidade front-end é exibida na página Uso de front-end.

Opção	Descrição
	b. Se for exibido um valor na coluna Sem relatório, clique no número para identificar clientes que não relataram o uso de capacidade. c. Para estimar a capacidade para os clientes que não relataram o uso de capacidade, acesse o site de download a seguir, que fornece ferramentas de medição e instruções: https://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools Para medir a capacidade de front-end por script, conclua as instruções no guia de licenciamento mais recente disponível. d. Inclua a estimativa do Operations Center e todas as estimativas obtidas usando um script. e. Verifique se a capacidade estimada está em conformidade com seu contrato de licença.
Modelo backend	**Restrição:** Se os servidores de replicação de origem e de destino não usarem as mesmas configurações de política, não será possível usar o Operations Center para monitorar o uso de capacidade de backend para clientes replicados. Para obter informações sobre como estimar o uso de capacidade para esses clientes, consulte a nota técnica 1656476. a. Na barra de menus do Operations Center, passe o mouse sobre o ícone de configurações e clique em **Licenciamento**. b. Clique na guia **Back-end**. c. Verifique se a quantidade estimada de dados está em conformidade com seu contrato de licença.
Modelo de PVU	Para obter informações sobre como avaliar a conformidade com os termos de licenciamento PVU, consulte Avaliando a conformidade com o modelo de licenciamento PVU.

Rastreando o status do sistema usando relatórios de e-mail

Configure o Operations Center para gerar relatórios de e-mail que resumem o status do sistema. É possível configurar uma conexão do servidor de e-mail, alterar configurações de relatório e, de modo opcional, criar relatórios customizados.

Antes de Iniciar

Antes de configurar relatórios de e-mail, certifique-se de que os requisitos a seguir sejam atendidos:

- Um servidor host do Protocolo Simples de Transporte de Correio (SMTP) está disponível para enviar e receber relatórios por email. O servidor SMTP deve ser configurado como uma retransmissão de e-mail aberta. Também é necessário assegurar que o servidor do IBM Spectrum Protect que envia emails tenha acesso ao servidor SMTP. Se o Operations Center for instalado em um computador separado, esse computador não precisará de acesso ao servidor SMTP.
- Para configurar relatórios de e-mail, deve-se ter privilégio no sistema para o servidor.
- Para especificar os destinatários, é possível inserir um ou mais endereços de email ou IDs de administrador. Se você deseja inserir um ID de administrador, o ID deve estar registrados no servidor

do hub e deve ter um endereço de e-mail associado a ele. Para especificar um endereço de email para um administrador, use o parâmetro **EMAILADDRESS** do comando **UPDATE ADMIN**.

Sobre Esta Tarefa

É possível configurar o Operations Center para enviar um relatório de operações gerais, um relatório de conformidade da licença e um ou mais relatórios customizados. É possível criar relatórios customizados selecionando um modelo a partir de um conjunto de modelos de relatórios comumente usados ou inserindo instruções SQL SELECT para consultar servidores gerenciados.

Procedimento

Para configurar e gerenciar relatórios de e-mail, conclua as etapas a seguir:

1. Na barra de menus do Operations Center, clique em **Relatórios**.
2. Se uma conexão do servidor de e-mail ainda não estiver configurada, clique em**Configurar servidor de Correio** e complete os campos.

   Após você configurar o servidor de correio, o relatório de operações gerais e o relatório de conformidade da licença são ativados.
3. Para alterar configurações de relatório, selecione um relatório, clique em **Detalhes** e atualize o formulário.
4. Opcional: Para incluir um relatório customizado, clique em **+ Relatório**, e preencha os campos.

   Dica: Para executar e enviar um relatório imediatamente, selecione o relatório e clique em **Enviar**.

Resultados

Relatórios ativados são enviados de acordo com as configurações especificadas.

O que Fazer Depois

O relatório de operações gerais inclui um anexo. Para localizar informações mais detalhadas, expanda as seções no anexo.

Se não for possível visualizar a imagem em um relatório, você pode estar usando um cliente de e-mail que converte HTML em um outro formato. Para obter informações sobre restrições, consulte a ajuda online do Operations Center.

Parte 4. Gerenciando operações para uma solução de fita

Use estas informações para gerenciar operações para uma implementação de fita para um servidor do IBM Spectrum Protect.

Gerenciando o Operations Center

O Operations Center fornece acesso à web e por dispositivo móvel a informações de status sobre o ambiente do IBM Spectrum Protect.

Sobre Esta Tarefa
É possível usar o Operations Center para monitorar vários servidores e concluir algumas tarefas administrativas. O Operations Center também fornece acesso à web para a linha de comandos do IBM Spectrum Protect. Para obter informações adicionais sobre como gerenciar o Operations Center, consulte Gerenciando o Operations Center.

Gerenciando operações do cliente

É possível resolver erros do cliente, gerenciar upgrades do cliente e desatribuir nós clientes que não são mais necessários. Para liberar espaço de armazenamento no servidor, é possível desativar dados obsoletos que são armazenados por aplicativos clientes.

Sobre Esta Tarefa
Em alguns casos, é possível resolver erros do cliente parando e iniciando o client acceptor. Se os nós clientes ou IDs de administrador estiverem bloqueados, será possível resolver o problema desbloqueando o nó cliente ou o ID de administrador e, em seguida, reconfigurando a senha.

Para obter instruções detalhadas sobre como identificar e resolver erros de clientes, consulte Resolvendo problemas do cliente.

Para obter instruções sobre como incluir clientes, consulte “Protegendo aplicativos e sistemas” na página 105.

Avaliando erros nos logs de erros do cliente

É possível resolver erros do cliente obtendo sugestões do Operations Center ou revisando os logs de erro no cliente.

Antes de Iniciar

Opcionalmente, para resolver erros em um cliente de backup-archive em um sistema operacional Linux ou Windows, certifique-se de que o client management service esteja instalado e iniciado. Para obter instruções de instalação, consulte Instalando o serviço de gerenciamento de clientes.

Procedimento

Para diagnosticar e resolver erros do cliente, execute uma das seguintes ações:

- Se o client management service estiver instalado no nó cliente, conclua as etapas a seguir:
  a) Na página Visão geral do Operations Center, clique em **Clientes** e selecione o cliente.
  b) Clique em **Detalhes**.

c) Na página Resumo do cliente, clique na guia **Diagnóstico**.

d) Revise as mensagens de log recuperadas.

Dicas:

– Para mostrar ou ocultar a área de janela Logs do cliente, dê clique duplo na barra Logs do cliente.

– Para redimensionar a área de janela Logs do cliente, clique e arraste a barra Logs do cliente.

Se forem exibidas sugestões na página Diagnóstico, selecione uma sugestão. Na área de janela Logs do cliente, as mensagens de log do cliente às quais a sugestão está relacionada são destacadas.

e) Use as sugestões para resolver os problemas indicados pelas mensagens de erro.

Dica: Sugestões são fornecidas apenas para um subconjunto de mensagens do cliente.

- Se o client management service não estiver instalado no nó cliente, revise os logs de erro para o cliente instalado.

Parando e reiniciando o client acceptor

Se você mudar a configuração de sua solução, deverá reiniciar o client acceptor em todos os nós clientes em que um cliente de backup-archive está instalado.

Sobre Esta Tarefa

Em alguns casos, é possível resolver problemas de planejamento de cliente parando e reiniciando o client acceptor. O client acceptor deve estar em execução para assegurar que as operações planejadas possam ocorrer no cliente. Por exemplo, se você mudar o endereço IP ou nome de domínio do servidor, deverá reiniciar o client acceptor.

Procedimento

Siga as instruções para o sistema operacional que está instalado no nó cliente:

AIX e Oracle Solaris

- Para parar o client acceptor, conclua as etapas a seguir:
  a. Determine o ID do processo para o client acceptor, emitindo o comando a seguir na linha de comandos:

     ```
     ps -ef | grep dsmcad
     ```

     Revise a saída. Na saída de amostra a seguir, 6764 é o ID do processo para o client acceptor:

     ```
     root  6764     1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
     ```

  b. Emita o seguinte comando na linha de comandos:

     ```
     kill -9 PID
     ```

     em que *PID* especifica o ID do processo para o client acceptor.
- Para iniciar o client acceptor, emita o comando a seguir na linha de comandos:

  ```
  /usr/bin/dsmcad
  ```

Linux

- Para parar o client acceptor (e não reiniciá-lo), emita o comando a seguir:

  ```
  # service dsmcad stop
  ```

- Para parar e reiniciar o client acceptor, emita o comando a seguir:

```
# service dsmcad restart
```

MAC OS X

Clique em **Aplicativos** > **Utilitários** > **Terminal**.

- Para parar o client acceptor, emita o comando a seguir:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Para iniciar o client acceptor, emita o comando a seguir:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

Janelas

- Para parar o serviço de client acceptor, conclua as etapas a seguir:
  a. Clique em **Iniciar** > **Ferramentas administrativas** > **Serviços**.
  b. Clique duas vezes no serviço de client acceptor.
  c. Clique em **Parar** e em **OK**.
- Para reiniciar o serviço de client acceptor, conclua as etapas a seguir:
  a. Clique em **Iniciar** > **Ferramentas administrativas** > **Serviços**.
  b. Clique duas vezes no serviço de client acceptor.
  c. Clique em **Iniciar** e em **OK**.

Informações relacionadas

Resolvendo Problemas de Planejamento de Cliente

Reconfigurando senhas

Se uma senha para um nó cliente ou um ID de administrador for perdida ou esquecida, será possível reconfigurar a senha. Várias tentativas de acessar o sistema com uma senha incorreta podem causar bloqueio de um nó cliente ou de um ID de administrador. É possível executar etapas para resolver o problema.

Procedimento

Para resolver problemas de senha, execute uma das seguintes ações:

- Se um cliente de backup-archive estiver instalado em um nó cliente, e a senha for perdida ou esquecida, conclua as etapas a seguir:
  1. Gere uma nova senha emitindo o comando **UPDATE NODE**:

     ```
     update node node_name new_password forcepwreset=yes
     ```

     em que *node_name* especifica o nó cliente e *new_password* especifica a senha designada.
  2. Informe o proprietário do nó cliente sobre a senha alterada. Quando o proprietário do nó cliente efetuar login com a senha especificada, uma nova senha será gerada automaticamente. Essa senha é desconhecida para os usuários para aprimorar a segurança.

     Dica: A senha será gerada automaticamente se você configurou anteriormente a opção **passwordaccess** como `generate` no arquivo de opções do cliente.
- Se um administrador estiver bloqueado devido a problemas de senha, conclua as etapas a seguir:
  1. Para fornecer ao administrador acesso ao servidor, emita o comando **UNLOCK ADMIN**. Para obter instruções, consulte UNLOCK ADMIN (Desbloquear um Administrador).

2. Configure uma nova senha usando o comando **UPDATE ADMIN**:

   ```
   update admin admin_name new_password forcepwreset=yes
   ```

   em que *admin_name* especifica o nome do administrador e *new_password* especifica a senha designada.

- Se um nó cliente estiver bloqueado, conclua as etapas a seguir:

  1. Determine por que o nó cliente está bloqueado e se ele deve ser desbloqueado. Por exemplo, se o nó cliente for desatribuído, ele está sendo removido do ambiente de produção. Não é possível reverter a operação de desatribuição, e o nó cliente permanece bloqueado. Um nó cliente também pode ser bloqueado se os dados de cliente forem o assunto de uma investigação judicial.
  2. Se precisar desbloquear um nó cliente, use o comando **UNLOCK NODE**. Para obter instruções, consulte UNLOCK NODE (Desbloquear um nó de cliente).
  3. Gere uma nova senha emitindo o comando **UPDATE NODE**:

     ```
     update node node_name new_password forcepwreset=yes
     ```

     em que *node_name* especifica o nome do nó e *new_password* especifica a senha designada.
  4. Informe o proprietário do nó cliente sobre a senha alterada. Quando o proprietário do nó cliente efetuar login com a senha especificada, uma nova senha será gerada automaticamente. Essa senha é desconhecida para os usuários para aprimorar a segurança.

     Dica: A senha será gerada automaticamente se você configurou anteriormente a opção **passwordaccess** como `generate` no arquivo de opções do cliente.

Gerenciando upgrades do cliente

Quando um fix pack ou correção temporária se torna disponível para um cliente, é possível fazer upgrade do cliente para tirar vantagem das melhorias do produto. Os servidores e clientes podem ser atualizados em diferentes horários e podem estar em diferentes níveis com algumas restrições.

Antes de Iniciar

1. Revise os requisitos de compatibilidade do cliente/servidor em Considerações sobre compatibilidade e upgrade do servidor/cliente IBM Spectrum Protect . Se sua solução incluir servidores ou clientes em um nível anterior à V7.1, revise as diretrizes para assegurar que as operações de backup e archive do cliente não sejam interrompidas.
2. Verifique os requisitos do sistema para o cliente em Sistemas operacionais suportados do IBM Spectrum Protect.
3. Se a solução incluir agentes de armazenamento ou clientes de biblioteca, revise as informações sobre compatibilidade de agente de armazenamento e cliente de biblioteca com servidores que estão configurados como gerenciadores de biblioteca. Consulte Compatibilidade do agente de armazenamento e do cliente de biblioteca com um servidor IBM Spectrum Protect .

   Se você planeja fazer upgrade de um gerenciador de biblioteca e de um cliente de biblioteca, deve-se fazer upgrade do gerenciador de biblioteca primeiro.

Procedimento

Para fazer upgrade do software, conclua as instruções que estão listadas na tabela a seguir.

Software	Link para instruções
Cliente de backup-archive do IBM Spectrum Protect	• Planejando atualizações do cliente

Software	Link para instruções
IBM Spectrum Protect Snapshot	• Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot para UNIX e Linux • Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot for VMware • Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot for Windows
IBM Spectrum Protect for Databases	• Atualizando o Data Protection for SQL Server • Instalação do Data Protection for Oracle • Instalando, fazendo upgrade e migrando o IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	• Fazendo upgrade do IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Db2 • Fazendo upgrade do IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle
IBM Spectrum Protect for Mail	• Instalação do Data Protection for IBM Domino em um sistema UNIX, AIX ou Linux (V7.1.0) • Instalação do Data Protection for IBM Domino em um sistema Windows (V7.1.0) • Instalando, fazendo upgrade e migrando o IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
Ambientes IBM Spectrum Protect for Virtual	• Instalando e fazendo upgrade do Data Protection for VMware • Instalando e fazendo upgrade do Data Protection for Microsoft Hyper-V

Desatribuindo um nó cliente

Se um nó cliente não for mais necessário, será possível iniciar um processo para removê-lo do ambiente de produção. Por exemplo, se uma estação de trabalho estava fazendo backup dos dados para o servidor IBM Spectrum Protect, mas ela não for mais usada, será possível desatribuir a estação de trabalho.

Sobre Esta Tarefa

Ao iniciar o processo de desatribuição, o servidor bloqueia o nó cliente para evitar que ele acesse o servidor. Os arquivos que pertencem ao nó cliente são excluídos gradualmente e, em seguida, o nó cliente é excluído. É possível desatribuir os seguintes tipos de nós clientes:

Nós clientes do aplicativo

Os nós clientes do aplicativo incluem servidores de e-mail, bancos de dados e outros aplicativos. Por exemplo, qualquer um dos seguintes aplicativos pode ser um nó cliente do aplicativo:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- Ambientes IBM Spectrum Protect for Virtual

Nós clientes do sistema

Os nós clientes do sistema incluem estações de trabalho, servidores de arquivos de armazenamento conectado à rede (NAS) e clientes da API.

Nós clientes de máquina virtual

Os nós clientes de máquina virtual consistem em um host convidado individual em um hypervisor. Cada máquina virtual é representada como um espaço no arquivo.

Restrição: Não é possível desatribuir um nó cliente de objeto.

O método mais simples para desatribuir um nó cliente é usar o Operations Center. O processo de desatribuição é executado no segundo plano. Se o cliente estiver configurado para replicar dados de cliente, o Operations Center removerá automaticamente o cliente da replicação nos servidores de replicação de origem e de destino antes de desatribuir o cliente.

Dica: Como alternativa, é possível desatribuir um nó cliente emitindo o comando **DECOMMISSION NODE** ou **DECOMMISSION VM**. Talvez você queira usar esse método nos seguintes casos:

- Para planejar o processo de desatribuição para o futuro ou para executar uma série de comandos usando um script, especifique o processo de desatribuição para execução no segundo plano.
- Para monitorar o processo de desatribuição para propósitos de depuração, especifique o processo de desatribuição para execução no primeiro plano. Se você executar o processo no primeiro plano, deverá aguardar a conclusão do processo antes de continuar com outras tarefas.

Procedimento

Execute uma das seguintes ações:

- Para desatribuir um cliente no segundo plano usando o Operations Center, conclua as etapas a seguir:
  a) Na página Operations Center **Visão geral**, clique em **Clientes** e selecione o cliente.
  b) Clique em **Mais** > **Desatribuir**.
- Para desatribuir um nó cliente usando um comando administrativo, execute uma das seguintes ações:
  - Para desatribuir um nó cliente do aplicativo ou do sistema no segundo plano, emita o comando **DECOMMISSION NODE**. Por exemplo, se o nó cliente chamar-se AUSTIN, emita o seguinte comando:

    ```
    decommission node austin
    ```

  - Para desatribuir um nó cliente do aplicativo ou do sistema no primeiro plano, emita o comando **DECOMMISSION NODE** e especifique o parâmetro `wait=yes`. Por exemplo, se o nó cliente chamar-se AUSTIN, emita o seguinte comando:

    ```
    decommission node austin wait=yes
    ```

  - Para desatribuir uma máquina virtual no segundo plano, emita o comando **DECOMMISSION VM**. Por exemplo, se a máquina virtual chamar-se AUSTIN, o espaço no arquivo for 7 e o nome do espaço no arquivo for especificado pelo ID do espaço no arquivo, emita o seguinte comando:

    ```
    decommission vm austin 7 nametype=fsid
    ```

    Se o nome da máquina virtual incluir um ou mais espaços, coloque-o entre aspas duplas. Por exemplo:

    ```
    decommission vm "austin 2" 7 nametype=fsid
    ```

  - Para desatribuir uma máquina virtual no primeiro plano, emita o comando **DECOMMISSION VM** e especifique o parâmetro `wait=yes`. Por exemplo, emita o seguinte comando:

    ```
    decommission vm austin 7 nametype=fsid wait=yes
    ```

    Se o nome da máquina virtual incluir um ou mais espaços, coloque-o entre aspas duplas. Por exemplo:

    ```
    decommission vm "austin 2" 7 nametype=fsid wait=yes
    ```

O que Fazer Depois

Fique atento às mensagens de erro, que podem ser exibidas na interface com o usuário ou na saída de comando, imediatamente após a execução do processo.

É possível verificar se o nó cliente está desatribuído:

1. Na página Operations Center **Visão geral**, clique em **Clientes**.
2. Na tabela Clientes, na coluna Em risco, revise o estado:
   - Um estado DECOMMISSIONED especifica que o nó está desatribuído.
   - Um valor nulo especifica que o nó não está desatribuído.
   - Um estado PENDING especifica que o nó está sendo desatribuído ou que o processo de desatribuição falhou.

   Dica: Se quiser determinar o status de um processo de desatribuição pendente, emita o seguinte comando:

   ```
   query process
   ```
3. Revise a saída de comando:
   - Caso um status seja fornecido para o processo de desatribuição, o processo está em andamento. Por exemplo:

   ```
   query process

    Process     Process Description           Process Status
     Number
   --------     --------------------     -------------------------------------------
          3          DECOMMISSION NODE        Number of backup objects deactivated
                                              for node NODE1: 8 objects deactivated.
   ```
   - Caso nenhum status seja fornecido para o processo de desatribuição e você não receber uma mensagem de erro, o processo está incompleto. Um processo pode estar incompleto caso os arquivos que estão associados ao nó ainda não tenham sido desativados. Após a desativação dos arquivos, execute o processo de desatribuição novamente.
   - Caso nenhum status seja fornecido para o processo de desatribuição e você receber uma mensagem de erro, o processo falhou. Execute o processo de desatribuição novamente.

Dica: Para reconfigurar o status de um nó ou de uma máquina virtual que foi desatribuída anteriormente, use os comandos administrativos a seguir:

- Para reconfigurar o status de um nó que foi desatribuído anteriormente do ambiente de produção usando o comando **DECOMMISSION NODE**, use o comando **RECOMMISSION NODE**.
- Para reconfigurar o status de um espaço de arquivo de máquina virtual que foi desatribuído anteriormente do ambiente de produção usando o comando **DECOMMISSION VM**, use o comando **RECOMMISSION VM**.

Informações relacionadas

DECOMMISSION NODE (Desatribuir um nó cliente)
DECOMMISSION VM (Desatribuir uma máquina virtual)

Desativando dados para liberar espaço de armazenamento

Em alguns casos, é possível desativar os dados que são armazenados no servidor IBM Spectrum Protect. Ao executar o processo de desativação, os dados de backup que foram armazenados antes da data e hora especificadas serão desativados e excluídos conforme expiram. Dessa forma, é possível liberar espaço no servidor.

Sobre Esta Tarefa

Alguns aplicativos clientes sempre salvam dados no servidor como dados de backup ativo. Como os dados de backup ativo não são gerenciados por políticas de expiração de inventário, os dados não são excluídos automaticamente e usam o espaço de armazenamento do servidor indefinidamente. Para liberar o espaço de armazenamento que é usado por dados obsoletos, é possível desativar os dados.

Ao executar o processo de desativação, todos os dados de backup ativo que foram armazenados antes da data especificada se tornam inativos. Os dados são excluídos conforme expiram e não podem ser restaurados. O recurso de desativação aplica-se apenas aos aplicativos clientes que protegem bancos de dados Oracle.

Procedimento

1. Na página Visão geral do Operations Center, clique em **Clientes**.
2. Na tabela Clientes, selecione um ou mais clientes e clique em **Mais** > **Limpar**.

   Método de linha de comandos: Desative os dados usando o comando **DEACTIVATE DATA**.

Informações relacionadas

DEACTIVATE DATA (Desativar dados para um nó cliente)

Gerenciando armazenamento de dados

Gerencie seus dados para eficiência e inclua dispositivos suportados e mídia no servidor para armazenar os dados do cliente.

Informações relacionadas

Tipos de conjuntos de armazenamentos

Gerenciando a capacidade do inventário

Gerencie a capacidade do banco de dados, do log ativo e dos logs de archive para assegurar que o inventário seja dimensionado para as tarefas, com base no status dos logs.

Antes de Iniciar

Os logs ativos e de archive possuem as seguintes características:

- O log ativo pode ter um tamanho máximo de 512 GB. Para obter mais informações sobre o dimensionamento do log ativo para o seu sistema, consulte “Planejando as matrizes de armazenamento” na página 13.
- O tamanho do log de archive é limitado ao tamanho do sistema de arquivos no qual está instalado. O tamanho do log de archive não é mantido em um tamanho predefinido, como o log ativo. Os arquivos de log de archive são excluídos automaticamente quando não são mais necessários.

Como uma melhor prática, opcionalmente, é possível criar um log de failover de archive para armazenar arquivos de log de archive quando o diretório de log de archive estiver cheio.

Verifique o Operations Center para determinar o componente do inventário que está cheio. Certifique-se de parar o servidor antes de aumentar o tamanho de um dos componentes do inventário.

Procedimento

- Para aumentar o espaço em disco para o banco de dados, conclua as seguintes etapas:
  - Crie um ou mais diretórios para o banco de dados em unidades ou sistemas de arquivos separados.
  - Emita o comando **EXTEND DBSPACE** para incluir o diretório ou diretórios no banco de dados. Os diretórios devem estar acessíveis ao ID do usuário da instância do gerenciador do banco de dados.

Por padrão, os dados são redistribuídos entre todos os diretórios do banco de dados e o espaço é recuperado.

Dicas:

- O tempo necessário para concluir a redistribuição de dados e a recuperação de espaço é variável, dependendo do tamanho de seu banco de dados. Certifique-se de planejar de forma apropriada.
- Assegure-se de que os diretórios especificados sejam do mesmo tamanho que os diretórios existentes, para assegurar um grau de paralelismo consistente para operações de 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.

- Pare e reinicie o servidor para usar totalmente os novos diretórios.
- Reorganize o banco de dados, se necessário. A reorganização de índice e de tabela para o banco de dados do servidor pode ajudar a evitar o crescimento inesperado do banco de dados e problemas de desempenho. Para obter informações adicionais sobre a reorganização do banco de dados, consulte Resolvendo e evitando problemas relacionados ao crescimento do banco de dados e desempenho comprometido no Tivoli Storage Manager V7.1.1.200 e servidores mais recentes.

- Para diminuir o tamanho do banco de dados para servidores V7.1 e mais recente, consulte as informações em Resolvendo e evitando problemas relacionados ao crescimento do banco de dados e desempenho comprometido no Tivoli Storage Manager V7.1.1.200 e servidores mais recentes.

  Restrição: Os comandos podem aumentar a atividade de E/S e podem afetar o desempenho do servidor. Para minimizar problemas de desempenho, aguarde até que um comando seja concluído antes de emitir o próximo comando. Os comandos do Db2 podem ser emitidos durante a execução do servidor.
- Para aumentar ou diminuir o tamanho do log ativo, conclua as etapas a seguir:
  a) Certifique-se de que o local do log ativo tenha espaço suficiente para o tamanho de log aumentado.
  b) Pare o servidor.
  c) No arquivo `dsmserv.opt`, atualize a opção **ACTIVELOGSIZE** para o novo tamanho do log ativo, em megabytes.

  O tamanho de um arquivo de log ativo é baseado no valor da opção `ACTIVELOGSIZE`. As diretrizes para requisitos de espaço estão na seguinte tabela:

  Tabela 29. Como estimar requisitos de volume e de espaço no arquivo

Valor da opção ACTIVELOGSize	**Reserve essa quantidade de espaço livre no diretório de log ativo, além do espaço ACTIVELOGSize**
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

  Para alterar o log ativo para seu tamanho máximo de 512 GB, insira a seguinte opção do servidor:

  ```
  activelogsize 524288
  ```

  d) Se você planeja usar um novo diretório de log ativo, atualize o nome do diretório especificado na opção do servidor **ACTIVELOGDIRECTORY**. O novo diretório deve estar vazio e deve estar acessível para o ID do usuário do gerenciador do banco de dados.
  e) Reinicie o servidor.
- Compacte os logs de archive para reduzir a quantidade de espaço necessário para armazenamento. Ative a compactação dinâmica do log de archive emitindo o seguinte comando:

  ```
  setopt archlogcompress yes
  ```

Restrição: Tenha cuidado ao ativar a opção do servidor **ARCHLOGCOMPRESS** em sistemas com alto uso de volumes sustentados e cargas de trabalho pesadas. A ativação dessa opção neste ambiente do sistema pode causar atrasos no arquivamento de arquivos de log do sistema de arquivos de log ativo para o sistema de arquivos de log de archive. Este atraso pode fazer com que o sistema de arquivos de log ativo fique sem espaço. Certifique-se de monitorar o espaço disponível no sistema de arquivos de log ativo após a compactação do log de archive ser ativada. Se o uso do sistema de arquivos do diretório de log ativo se aproximar de condições de falta de espaço, a opção do servidor **ARCHLOGCOMPRESS** deve ser desativada. É possível usar o comando **SETOPT** para desativar a compactação de log de archive imediatamente sem parar o servidor.

Informações relacionadas

Opção do servidor ACTIVELOGSIZE

EXTEND DBSPACE (Aumentar o Espaço do Banco de Dados)

SETOPT (Definir uma opção do servidor para atualização dinâmica)

Ajustando atividades planejadas

Planeje tarefas de manutenção diariamente para assegurar que sua solução funcione corretamente. Ao ajustar sua solução, você maximiza os recursos do servidor e usa efetivamente diferentes funções disponíveis em sua solução.

Procedimento

1. Monitore o desempenho do sistema regularmente para assegurar que as tarefas de backup e manutenção sejam concluídas com sucesso. Para obter informações adicionais sobre monitoramento, consulte Parte 3, “Monitorando uma solução de fita”, na página 133.
2. Se as informações de monitoramento mostrarem que houve aumento da carga de trabalho do servidor, pode ser necessário que você revise as informações de planejamento. Revise se a capacidade do sistema é adequada nos seguintes casos:
   - O número de clientes aumentou
   - A quantidade de dados que está sendo feito backup aumentou
   - A quantidade de tempo que está disponível para backups foi alterada
3. Determine se sua solução tem problemas de desempenho.
   Revise os planejamentos de cliente para verificar se as tarefas estão sendo concluídas dentro do prazo planejado:
   a. Na página **Clientes** do Operations Center, selecione o cliente.
   b. Clique em **Detalhes**.
   c. Na página **Resumo** do cliente, revise as atividades **Backup Realizado** e **Replicados** para identificar quaisquer riscos.

   Ajuste o tempo e a frequência de operações de backup de cliente, se necessário.
4. Planeje tempo suficiente para que as seguintes tarefas de manutenção sejam concluídas com sucesso dentro de um período de 24 horas:
   a. Fazer backup do banco de dados
   b. Execute a expiração para remover backups de cliente e cópias de archive do armazenamento do servidor.

Informações relacionadas

Deduplicando dados (V7.1.1)

Desempenho

Otimizando operações ativando a disposição de arquivos do cliente

A disposição de arquivos do cliente reduz o número de montagens de volume que são necessárias quando os usuários restauram, recuperam ou rechamam muitos arquivos a partir de um conjunto de armazenamentos. Portanto, a disposição reduz a quantidade de tempo necessário para essas operações.

Sobre Esta Tarefa

Com a disposição ativada, o servidor tenta manter arquivos em um número mínimo de volumes de armazenamento de acesso sequencial. Os arquivos podem pertencer a um único nó cliente, a um grupo de nós clientes, a um espaço no arquivo do cliente ou a um grupo de espaços no arquivo. É possível configurar a disposição para cada conjunto de armazenamentos de acesso sequencial ao definir ou atualizar o conjunto.

Figura 7 na página 167 mostra um exemplo de disposição por nó cliente com três clientes, cada um com um volume separado que contém os dados do cliente.

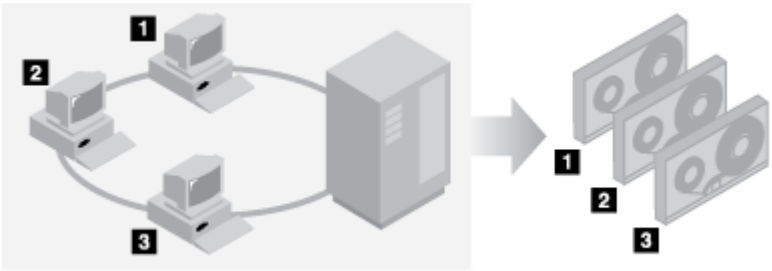


Figura 7. Exemplo de disposição ativada por nó

A Figura 8 na página 167 mostra um exemplo de disposição por grupo de nós clientes. Três grupos são definidos, e os dados para cada grupo são armazenados em volumes separados.

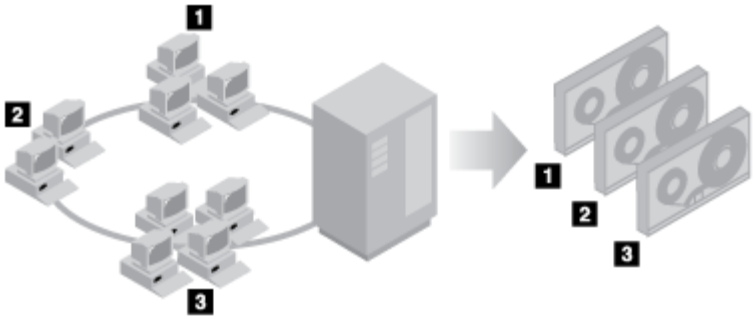


Figura 8. Exemplo de disposição ativada por grupo de disposição de nó

A Figura 9 na página 168 mostra um exemplo de disposição por grupo de espaço no arquivo. Seis grupos são definidos. Cada grupo contém dados de espaços no arquivo que pertencem a um único nó. Os dados para cada grupo são armazenados em um volume separado.

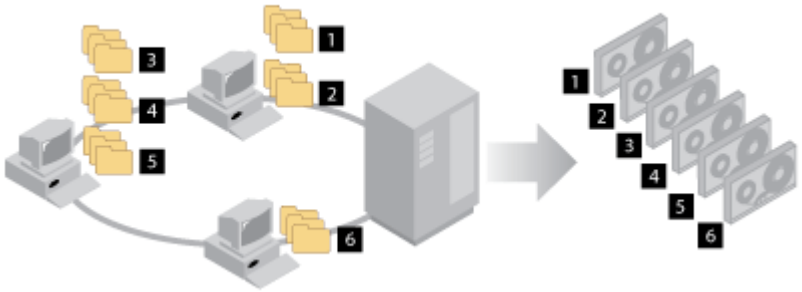


Figura 9. Exemplo de disposição ativada por grupo de disposição de espaço no arquivo

Quando a disposição está desativada, o servidor tenta usar todo o espaço disponível em cada volume antes de selecionar um novo volume. Embora esse processo forneça melhor uso de volumes individuais, os arquivos do usuário podem ser tornar dispersos em muitos volumes. A Figura 10 na página 168 mostra um exemplo de disposição que está desativada, com três clientes que compartilham espaço no único volume.

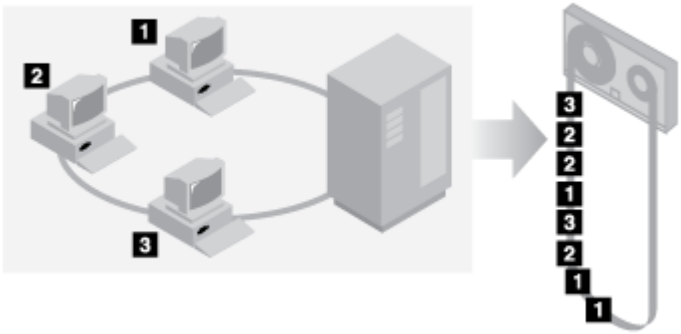


Figura 10. Exemplo de disposição desativada

Com a disposição desativada, mais operações de montagem de mídia podem ser necessárias para montar volumes quando usuários restauram, recuperam ou rechamam muitos arquivos.

A disposição por grupo é o padrão do sistema IBM Spectrum Protect para conjuntos de armazenamentos de acesso sequencial primários. O padrão para conjuntos de armazenamentos de cópia e conjuntos de armazenamentos de retenção é sem disposição.

Efeitos de disposição em operações

O efeito da disposição em recursos e no desempenho do sistema depende do tipo de operação que está sendo executado.

A Tabela 30 na página 168 resume os efeitos da disposição em operações.

Tabela 30. Efeito de disposição em operações

Operação	Disposição ativada	Disposição desativada
Fazer backup, arquivar ou migrar arquivos do cliente	Mais montagens de mídia para dispor arquivos.	São necessárias menos montagens de mídia.

Tabela 30. Efeito de disposição em operações (continuação)

Operação	Disposição ativada	Disposição desativada
Restaurar, recuperar ou rechamar arquivos do cliente	Grandes números de arquivos podem ser restaurados, recuperados ou rechamados mais rapidamente porque os arquivos estão em menos volumes.	Várias montagens de mídia podem ser necessárias para um único usuário, porque os arquivos podem ser difundidos entre vários volumes. Arquivos de mais de um usuário podem ser armazenados no mesmo volume de armazenamento de acesso sequencial. Por exemplo, se dois usuários tentarem recuperar um arquivo que está no mesmo volume, o segundo usuário será forçado a esperar até que os arquivos do primeiro usuário sejam recuperados.
Armazenar dados em fita	O servidor tenta usar todos os volumes de fita disponíveis para separar arquivos do usuário antes dele usar todo o espaço disponível em cada volume de fita.	O servidor tenta usar todo o espaço disponível em cada volume da fita antes de o servidor usar outro volume da fita.
Operações de montagem de mídia	São necessárias mais operações de montagem quando os arquivos do usuário são submetidos a backup, arquivados ou migrados de nós clientes diretamente para volumes de acesso sequencial. São necessárias mais operações de montagem durante a recuperação e migração do conjunto de armazenamentos. Mais volumes são gerenciados porque os volumes não são totalmente usados.	Mais operações de montagem são necessárias durante a restauração, recuperação e rechamada de arquivos do cliente.
Gerar conjuntos de backup	Menos tempo é gasto na procura de entradas de banco de dados e são necessárias menos operações de montagem.	Mais tempo é gasto na procura de entradas de banco de dados e são necessárias menos operações de montagem.
Copiando conjuntos de retenção para a fita **Importante:** Sua configuração de disposição pode aumentar significativamente o número de volumes de fita necessários para o conjunto de retenção.	O servidor tenta manter os arquivos da mesma entidade disposta no menor número de volumes de fita possível. O tempo de processamento para gravar um conjunto de retenção para fita pode aumentar.	O servidor tenta usar todo o espaço disponível em cada volume da fita antes do servidor usar outro volume da fita. Se os dados precisarem ser restaurados por meio de um conjunto de retenção, mais montagens da fita poderão ser necessárias para um único usuário do conjunto de retenção porque os arquivos podem ser difundidos em diversos volumes.

Quando a disposição é ativada para um grupo, nó cliente único ou espaço no arquivo, todos os dados que pertencem ao grupo, nó ou espaço no arquivo são movidos ou copiados por um processo do servidor. Por exemplo, se os dados forem dispostos por grupo, todos os dados para todos os nós que pertencem ao mesmo grupo de disposição serão migrados pelo mesmo processo.

Ao dispor dados, o servidor IBM Spectrum Protect tenta manter os arquivos juntos em um número mínimo de volumes de armazenamento de acesso sequencial. No entanto, quando o servidor está fazendo backup de dados para volumes em um conjunto de armazenamentos de acesso sequencial, o processo de backup tem prioridade sobre as configurações de disposição. Como resultado, o servidor conclui a operação de backup, mas pode não ser capaz de dispor os dados.

Por exemplo, suponha que você esteja dispondo por nó e especifique que um nó pode usar dois pontos de montagem no servidor. Suponha também que os dados que são submetidos a backup a partir do nó podem facilmente caber em um volume da fita. Durante o backup, o servidor pode montar dois volumes de fita, e os dados do nó podem ser distribuídos em duas fitas, em vez de uma. Se você ativar a disposição, as seguintes operações do servidor usarão um processo do servidor:

- Mover dados de volumes de acesso aleatório e de acesso sequencial
- Mover dados do nó de volumes de acesso sequencial
- Fazer backup de um conjunto de armazenamentos de acesso aleatório ou de acesso sequencial
- Restaurar um conjunto de armazenamentos de acesso sequencial
- Recuperar espaço em um conjunto de armazenamentos de acesso sequencial ou volumes externos
- Migrar dados de um conjunto de armazenamentos de acesso aleatório

Ao migrar dados de um conjunto de armazenamentos em disco de acesso aleatório para um conjunto de armazenamentos de acesso sequencial, e se a disposição for por nó ou espaço no arquivo, os nós ou espaços no arquivo serão selecionados automaticamente para migração com base na quantidade de dados a serem migrados. O nó ou espaço no arquivo com a maior parte dos dados será migrado primeiro. Se a disposição for por grupo, todos os nós no conjunto de armazenamentos serão avaliados para determinar qual nó tem a maior parte dos dados. O nó com a maior parte dos dados é migrado primeiro junto com todos os dados para todos os nós que pertencem a esse grupo de disposição. Esse processo ocorre, independentemente da quantidade de dados que são armazenados nos espaços no arquivo de nós e independentemente do limite baixo de migração ter sido atingido.

No entanto, ao migrar dados dispostos de um conjunto de armazenamentos de acesso sequencial para outro conjunto de armazenamentos de acesso sequencial, o servidor ordena os volumes de acordo com a data do último acesso ao volume. O volume com a data de acesso mais antiga é migrado primeiro e o volume com a data de acesso mais recente é migrado por último.

Uma razão para dispor por grupo é que os nós clientes individuais geralmente não têm dados suficientes para preencher volumes de fita de alta capacidade. Dispor dados por grupos de nós pode reduzir a capacidade de fita não utilizada, colocando mais dados dispostos em fitas individuais. Além disso, dispor dados por grupos de espaços no arquivo reduz a fita não utilizada a um grau maior.

Os dados que pertencem a todos os nós no mesmo grupo de disposição são migrados pelo mesmo processo. Portanto, a disposição por grupo pode reduzir o número de vezes que um volume a ser migrado deve ser montado. A disposição por grupo também podem minimizar a varredura de banco de dados e reduzir as transmissões de fita durante a transferência de dados de um conjunto de armazenamentos de acesso sequencial para outro.

Selecionando volumes com a disposição ativada

A seleção de volume depende se a disposição é por grupo, nó ou espaço no arquivo.

A Tabela 31 na página 171 mostra como o servidor IBM Spectrum Protect seleciona o primeiro volume quando a disposição é ativada para um conjunto de armazenamentos no nó cliente, grupo de disposição e nível de espaço no arquivo.

Tabela 31. Como o servidor seleciona volumes quando a disposição está ativada

Ordem de seleção de volume	Quando a disposição é por grupo	Quando a disposição é por nó	Quando a disposição é por espaço no arquivo
1	Um volume que já contém arquivos do grupo de disposição ao qual o cliente pertence	Um volume que já contém arquivos do mesmo nó cliente	Um volume que já contém arquivos do mesmo espaço no arquivo desse nó cliente
2	Um volume predefinido vazio	Um volume predefinido vazio	Um volume predefinido vazio
3	Um volume utilizável vazio	Um volume utilizável vazio	Um volume utilizável vazio
4	Um volume com a maior parte do espaço livre disponível entre volumes que já contêm dados	Um volume com a maior parte do espaço livre disponível entre volumes que já contêm dados	Um volume que contém dados do mesmo nó cliente
5	Não aplicável	Não aplicável	Um volume com a maior parte do espaço livre disponível entre volumes que já contêm dados

Quando o servidor precisar continuar armazenando dados em um segundo volume, ele usa a seguinte ordem de seleção para adquirir mais espaço:

1. Um volume predefinido vazio
2. Um volume utilizável vazio
3. Um volume com a maior parte do espaço livre disponível entre volumes que já contêm dados
4. Qualquer volume disponível no conjunto de armazenamentos

Quando a disposição é por nó cliente ou espaço no arquivo, o servidor tenta fornecer o melhor uso de volumes individuais e minimiza a combinação de arquivos de diferentes clientes ou espaços no arquivo em volumes. Essa configuração é descrita em Figura 11 na página 171, que mostra que a seleção de volume é *horizontal*, em que todos os volumes disponíveis são usados antes do uso de todo o espaço disponível em cada volume. A, B, C e D representam arquivos de quatro nós clientes diferentes.

Dicas:

1. Se a disposição for por nó e o nó tiver vários espaços no arquivo, o servidor não tentará dispor esses espaços no arquivo.
2. Se a disposição for espaço no arquivo e um nó tiver vários espaços no arquivo, o servidor tentará colocar dados para diferentes espaços no arquivo em diferentes volumes.

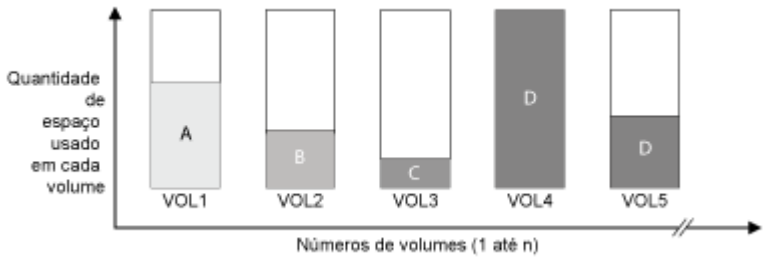


Figura 11. Usando todos os volumes de armazenamento de acesso sequencial disponíveis com a disposição ativada no nível do nó ou do espaço no arquivo

A disposição pode ser por grupo de espaço no arquivo ou por grupo de nós. Quando a disposição é por grupo de nós (grupo de disposição do nó), o servidor tenta dispor dados de nós que pertencem ao mesmo grupo de disposição. Um grupo de disposição de espaço no arquivo usa os mesmos métodos que um grupo de disposição do nó, mas pode usar mais espaço devido à granularidade de tamanhos de espaço no arquivo. Conforme mostrado na Figura 12 na página 172, os dados para os seguintes grupos de nós foram dispostos:

- O Grupo 1 consiste nos nós A, B e C
- O Grupo 2 consiste nos nós D e E
- O Grupo 3 consiste nos nós F, G, H e I

Sempre que possível, o servidor IBM Spectrum Protect dispõe dados que pertencem a um grupo de nós em uma única fita, conforme representado pelo Grupo 2 na figura. Os dados para um único nó também podem ser difundidos entre várias fitas que estão associadas a um grupo (Grupos 1 e 2). Se os nós no grupo de disposição tiverem vários espaços de arquivo, o servidor não fará nenhuma tentativa de co-alocar esses espaços de arquivos.

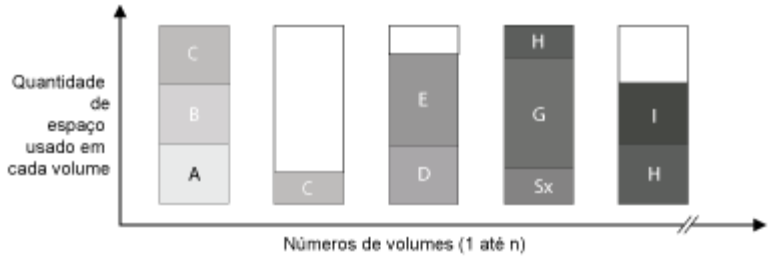


Figura 12. Usando todos os volumes de armazenamento de acesso sequencial disponíveis com a disposição ativada no nível do grupo

Normalmente, o servidor IBM Spectrum Protect sempre grava dados no volume de preenchimento atual para a operação que está sendo executada. No entanto, ocasionalmente, é possível notar mais de um volume de preenchimento em um conjunto de armazenamentos disposto. Ter mais de um volume de preenchimento em um conjunto de armazenamentos disposto pode ocorrer se diferentes processos do servidor ou sessões do cliente tentarem armazenar dados no conjunto disposto ao mesmo tempo. Nessa situação, o IBM Spectrum Protect aloca um volume para cada processo ou sessão que precisa de um volume para que ambas as operações sejam concluídas o mais rápido possível.

Selecionando volumes com a disposição desativada

Quando a disposição está desativada, o servidor tenta usar todo o espaço disponível em um volume de armazenamento antes de acessar outro volume.

Ao armazenar arquivos do cliente em um conjunto de armazenamentos de acesso sequencial no qual a disposição está desativada, o servidor seleciona um volume usando a seguinte ordem de seleção:

1. Um volume sequencial usado anteriormente com espaço disponível (um volume com a maior quantidade de dados é selecionado primeiro)
2. Um volume nulo

Quando o servidor precisar continuar armazenando dados em um segundo volume, ele tentará selecionar um volume nulo. Se não existir nenhum volume nulo, o servidor tentará selecionar qualquer volume disponível restante no conjunto de armazenamentos.

A Figura 13 na página 173 mostra que o uso do volume é vertical quando a disposição está desativada. Nesse exemplo, menos volumes são usados porque o servidor tenta usar todo o espaço disponível combinando arquivos do cliente em volumes individuais. A, B, C e D representam arquivos de quatro nós clientes diferentes.

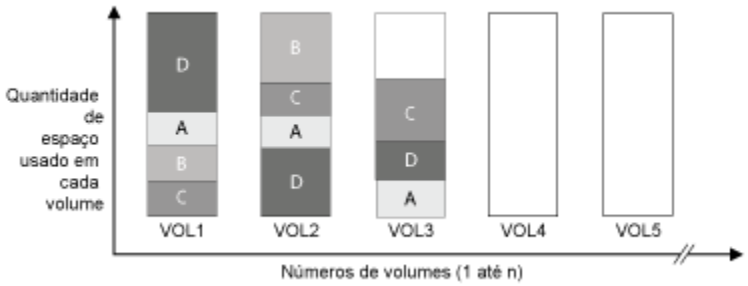


Figura 13. Usando todo o espaço disponível em volumes de acesso sequencial com a disposição desativada

Configurações de disposição

Depois de definir um conjunto de armazenamentos, é possível mudar a configuração de disposição atualizando o conjunto de armazenamentos. A mudança na disposição para o conjunto não afeta os arquivos que já estão armazenados no conjunto.

Por exemplo, se a disposição estiver desativada para um conjunto de armazenamentos e você ativá-la, desse ponto em diante, os arquivos do cliente que estão armazenados no conjunto serão dispostos. Os arquivos que foram armazenados anteriormente no conjunto de armazenamentos não são movidos para serem dispostos. Conforme os volumes são recuperados ou restaurados, os dados no conjunto tendem a se tornar mais dispostos. Também é possível usar os comandos **MOVE DATA** ou **MOVE NODEDATA** para mover dados para novos volumes para aumentar a disposição. Mover dados para novos volumes causa um aumento no tempo de processamento e na atividade da montagem do volume.

Dica: Uma espera de montagem pode ocorrer ou demorar mais que o normal quando a disposição por espaço no arquivo está ativada e um nó tem um volume que contém vários espaços no arquivo. Se um volume for elegível para receber dados, o IBM Spectrum Protect espera esse volume.

Disposição de conjuntos de armazenamento de cópia

O uso de disposição em conjuntos de armazenamento de cópia requer consideração especial. A disposição de conjuntos de armazenamento de cópia, especialmente por nó ou espaço no arquivo, resulta em mais volumes parcialmente preenchidos e em atividade de recuperação externa potencialmente desnecessária.

Os conjuntos de armazenamentos primários desempenham um papel de recuperação diferente dos conjuntos de armazenamento de cópia. Normalmente, você usa conjuntos de armazenamentos primários para recuperar dados diretamente para clientes. Em um desastre, quando os clientes e o servidor são perdidos, você pode usar volumes do conjunto de armazenamentos de cópia externos para recuperar os conjuntos de armazenamentos primários. Os tipos de cenários de recuperação podem ajudá-lo a determinar se usar disposição em seus conjuntos de armazenamento de cópia.

A disposição geralmente resulta em volumes parcialmente preenchidos ao dispor por nó ou por espaço no arquivo. No entanto, os volumes parcialmente preenchidos são menos prevalentes ao dispor por grupo. Os volumes parcialmente preenchidos podem ser aceitáveis para conjuntos de armazenamentos primários, porque os volumes permanecem disponíveis e podem ser preenchidos durante o próximo processo de migração. No entanto, os volumes parcialmente preenchidos podem ser inaceitáveis para conjuntos de armazenamento de cópia cujos volumes do conjunto de armazenamentos são obtidos externamente de forma imediata. Se você usar a disposição para conjuntos de armazenamento de cópia, deverá tomar as seguintes decisões:

- Obter mais volumes parcialmente preenchidos externos, o que aumenta a atividade de recuperação quando o limite de recuperação é reduzido ou atingido.
- Deixar esses volumes parcialmente preenchidos no local até que eles sejam preenchidos e arrisquem não ter uma cópia externa dos dados nesses volumes.
- Se dispor por grupo para usar a capacidade de fita máxima possível.

Quando a disposição for desativada para um conjunto de armazenamento de cópia, geralmente apenas alguns volumes parcialmente preenchidos permanecem após o backup dos dados para o conjunto de armazenamento de cópia.

Considere suas opções com cuidado antes de usar a disposição para conjuntos de armazenamento de cópia e se usar a gravação simultânea. Se você não usar a gravação simultânea e usar a disposição para seus conjuntos de armazenamentos primários, talvez queira desativar a disposição para conjuntos de armazenamento de cópia. A disposição de conjuntos de armazenamento de cópia pode ser desejável se você tiver alguns clientes com cada um deles tendo grandes quantidades de dados de backup incremental todos os dias. Para disposição com gravação simultânea, você deve assegurar que as configurações de disposição sejam idênticas para os conjuntos de armazenamentos primários e os conjuntos de armazenamento de cópia.

Disposição de conjuntos de armazenamentos de retenção

O valor que você seleciona para a propriedade de disposição afeta como os dados de um conjunto de retenção são difundidos entre os volumes da fita. Em geral, para usar o menor número de volumes de fita, a disposição deve ser desativada. Por padrão, a configuração de disposição para conjuntos de armazenamentos de retenção está desativada.

Com a configuração de disposição desativada, durante a seleção de volume para processos de cópia de conjuntos de retenção, o servidor tenta usar todo o espaço disponível em cada volume de fita antes de selecionar um novo volume. Embora esse processo faça um uso mais eficiente dos volumes de fita individuais, os dados de cada conjunto de retenção não são dispostos em conjunto e podem ser distribuídos por muitos volumes de fita.

Suas configurações de disposição podem ter um impacto significativo no desempenho do sistema quando os dados do conjunto de retenção estão sendo gravados na fita e durante as operações de restauração de dados do conjunto de retenção. Antes de considerar a possibilidade de ativar as configurações de disposição para os conjuntos de armazenamento de retenção, considere seus requisitos e as compensações de desempenho.

- Se a disposição estiver ativada, o servidor tentará manter aos arquivos para cada entidade em um número mínimo de volumes da fita. No entanto, essa opção aumenta o tempo de processamento do servidor necessário para dispor os arquivos para o armazenamento e o número de volumes necessários. A configuração do parâmetro **STACK** definida para o conjunto de retenção também é relevante.

  Dica: Se o empilhamento de volume estiver ativado para o conjunto de retenção, os dados do conjunto de retenção poderão compartilhar volumes da fita com os dados copiados de outros conjuntos de retenção. A seleção de volume primeiro procura volumes que estão em um estado FILLING que já contêm dados, mas somente se esses volumes já não estiverem em uso por conjuntos de retenção que requerem um volume separado. Se o empilhamento de volume não estiver ativado para o conjunto de retenção, o conjunto de retenção será disposto em um ou mais volumes de fita e os dados de outros conjuntos de retenção não serão dispostos nesses volumes. A seleção de volume procurará volumes vazios, mas os dados também poderão ser copiados para volumes FILLING somente se os volumes já contiverem dados para o conjunto de retenção que estiver sendo copiado.
- Com a disposição desativada, como os dados para os conjuntos de retenção individuais podem ser distribuídos por muitos volumes, mais montagens de fita poderão ser necessárias se os dados precisarem ser restaurados do conjunto de retenção. Se mais montagens de fita forem necessárias, o tempo de processamento necessário para as operações de restauração pode aumentar.

Dica: É possível ativar a disposição ou mudar as configurações de disposição especificando o parâmetro **COLLOCATE** nos comandos **DEFINE STGPOOL** ou **UPDATE STGPOOL**.

Mudando a configuração de disposição, somente os dados que forem subsequentemente gravados no conjunto de armazenamentos de retenção serão afetados. Os arquivos que já estão armazenados no conjunto não são afetados.

Conceitos relacionados

“Selecionando volumes com a disposição desativada” na página 172

Quando a disposição está desativada, o servidor tenta usar todo o espaço disponível em um volume de armazenamento antes de acessar outro volume.

"Efeitos de disposição em operações" na página 168
O efeito da disposição em recursos e no desempenho do sistema depende do tipo de operação que está sendo executado.

Planejando e ativando a disposição

Entender os efeitos de disposição pode ajudar a reduzir o número de montagens de mídia, fazer melhor uso do espaço em volumes sequenciais e melhorar a eficiência de operações do servidor.

Sobre Esta Tarefa

A Tabela 32 na página 175 lista as quatro opções de disposição que podem ser especificadas nos comandos **DEFINE STGPOOL** e **UPDATE STGPOOL**. A tabela também mostra os efeitos de disposição em dados que pertencem a nós que são e não são membros de grupos de disposição.

Tabela 32. Opções de disposição e os efeitos em dados do nó

Opção de disposição	Se um nó não estiver definido como um membro de um grupo de disposição	Se um nó estiver definido como um membro de um grupo de disposição
Sim	Os dados para o nó não são dispostos.	Os dados para o nó não são dispostos.
Grupo	O servidor armazena os dados para o nó no menor número de volumes possível no conjunto de armazenamentos.	O servidor armazena os dados para o nó e para outros nós que pertencem ao mesmo grupo de disposição no menor número de volumes possível.
Nó	O servidor armazena os dados para o nó no menor número de volumes possível.	O servidor armazena os dados para o nó no menor número de volumes possível.
Espaço no arquivo	O servidor armazena os dados para o espaço no arquivo do nó no menor número de volumes possível. Se um nó tiver vários espaços no arquivo, o servidor armazena os dados para diferentes espaços no arquivo em diferentes volumes no conjunto de armazenamentos.	O servidor armazena os dados para o espaço no arquivo do nó no menor número de volumes possível. Se um nó tiver vários espaços no arquivo, o servidor armazena os dados para diferentes espaços no arquivo em diferentes volumes no conjunto de armazenamentos.

Tabela 33. Opções do grupo de disposição e efeitos em dados do espaço no arquivo

Opção de disposição	Se um espaço no arquivo não estiver definido como um membro de um grupo de disposição	Se um espaço no arquivo estiver definido como um membro de um grupo de disposição
Sim	Os dados para o espaço no arquivo não são dispostos.	Os dados para o espaço no arquivo não são dispostos.
Grupo	O servidor armazena os dados para o espaço no arquivo no menor número de volumes possível no conjunto de armazenamentos.	O servidor armazena os dados para o espaço no arquivo e outros espaços no arquivo que pertencem ao mesmo grupo de disposição no menor número de volumes possível.
Nó	O servidor armazena os dados para o nó no menor número de volumes possível.	O servidor armazena os dados para o nó no menor número de volumes possível.

Tabela 33. Opções do grupo de disposição e efeitos em dados do espaço no arquivo (continuação)

Opção de disposição	Se um espaço no arquivo não estiver definido como um membro de um grupo de disposição	Se um espaço no arquivo estiver definido como um membro de um grupo de disposição
Espaço no arquivo	O servidor armazena os dados para o espaço no arquivo do nó no menor número de volumes possível. Se um nó tiver vários espaços no arquivo, o servidor armazena os dados para diferentes espaços no arquivo em diferentes volumes no conjunto de armazenamentos.	O servidor armazena os dados para os espaços no arquivo no menor número de volumes possível. Se um nó tiver vários espaços no arquivo, o servidor armazena os dados para diferentes espaços no arquivo em diferentes volumes no conjunto de armazenamentos.

Procedimento

Para determinar se e como dispor os dados, conclua as seguintes etapas:

1. Determine como organizar os dados, se por nó cliente, grupo de nós clientes ou espaço no arquivo. Para dispor por grupo, você deve decidir como agrupar nós:
   - Se o objetivo for economizar espaço, talvez você queira agrupar pequenos nós para melhor uso das fitas.
   - Se o objetivo for restaurações do cliente potencialmente mais rápidas, agrupe os nós para que eles preencham o maior número de fitas possível. Ao agrupar nós, os dados do nó individual são distribuídos entre duas ou mais fitas e mais fitas podem ser montadas simultaneamente durante uma operação de restauração sem consulta de múltiplas sessões.
   - Se o objetivo for dividir os dados em departamentos, é possível agrupar nós por departamento.
2. Para dispor os grupos, conclua as seguintes etapas:
   a) Defina grupos de disposição com o comando **DEFINE COLLOCGROUP**.
   b) Inclua nós clientes nos grupos de disposição com o comando **DEFINE COLLOCMEMBER**.

   Os seguintes comandos de consulta estão disponíveis para ajudar em grupos de disposição:

   QUERY COLLOCGROUP
   Exibe os grupos de disposição definidos no servidor.

   QUERY NODE
   Exibe o grupo de disposição, se houver, ao qual um nó pertence.

   QUERY NODEDATA
   Exibe informações sobre os dados para um ou mais nós em um conjunto de armazenamentos de acesso sequencial.

   QUERY STGPOOL
   Exibe informações sobre o local de dados do cliente em um conjunto de armazenamentos de acesso sequencial e a quantidade de espaço que um nó ocupa em um volume.

   Também é possível usar scripts do servidor IBM Spectrum Protect ou scripts PerlL para exibir informações que podem ser úteis na definição de grupos de disposição.
3. Especifique como os dados devem ser dispostos em um conjunto de armazenamentos, emitindo o comando **DEFINE STGPOOL** ou **UPDATE STGPOOL** e especificando o parâmetro **COLLOCATE**.

O que Fazer Depois

Dica: Para reduzir o número de montagens de mídia, usar o espaço em volumes sequenciais de forma mais eficiente e ativar a disposição, conclua as seguintes etapas:

- Defina uma hierarquia e política do conjunto de armazenamentos para requerer que arquivos de backup, arquivados ou gerenciados por espaço sejam armazenados inicialmente em conjuntos de armazenamentos em disco.

Quando os arquivos forem migrados de um conjunto de armazenamentos em disco, o servidor tentará migrar todos os arquivos que pertencem ao nó cliente ou grupo de disposição que está usando a maior parte do espaço em disco no conjunto de armazenamentos. Esse processo funciona bem com a opção de disposição, porque o servidor tenta colocar todos os arquivos de um determinado cliente no mesmo volume de armazenamento de acesso sequencial.

- Use volumes utilizáveis para conjuntos de armazenamentos de acesso sequencial para permitir que o servidor selecione novos volumes para disposição.
- Especifique a opção de cliente `COLLOCATEBYFILESPEC` para limitar o número de fitas onde serão gravados os objetos associados com uma especificação de arquivo. Essa opção de disposição torna a disposição pelo servidor mais eficiente; ela não substitui a disposição por espaço no arquivo ou a disposição por nó.

Gerenciando dispositivos de fita

As operações de fita de rotina incluem a preparação de volumes de fita para uso, o controle de como e quando os volumes são reutilizados e a certeza de que volumes suficientes estão disponíveis. Deve-se também responder às solicitações do operador e gerenciar bibliotecas, unidades, discos, caminhos e movedores de dados.

Preparando mídia removível

Deve-se preparar mídia removível antes que ela possa ser usada para armazenar dados. As tarefas típicas de preparação incluem etiquetagem e check-in de volumes.

Sobre Esta Tarefa

Quando o IBM Spectrum Protect acessa um volume de mídia removível, ele verifica o nome do volume no cabeçalho do rótulo para assegurar que o volume correto seja acessado.

Os volumes da fita devem ser identificados antes que o servidor possa usá-los.

Procedimento

Para preparar um volume para uso, conclua as etapas a seguir:

1. Etiquete o volume emitindo o comando **LABEL LIBVOLUME**.
2. Para bibliotecas automatizadas, efetue check-in do volume na biblioteca. Para obter instruções, consulte “Efetuando check-in de volumes em uma biblioteca automatizada” na página 179.

   Dica: Ao usar o comando **LABEL LIBVOLUME** com unidades em uma biblioteca automatizada, será possível etiquetar e efetuar check-in dos volumes com um comando.
3. Se o conjunto de armazenamentos não puder conter volumes utilizáveis (`MAXSCRATCH=0`), identifique o volume para o IBM Spectrum Protect por nome para que o volume possa ser acessado posteriormente.

   Se o conjunto de armazenamento puder conter volumes utilizáveis (**MAXSCRATCH** é configurado para um valor diferente de zero), ignore esta etapa.

Etiquetando volumes de fita

Deve-se etiquetar volumes de fita antes que o servidor possa usá-los.

Sobre Esta Tarefa

Para bibliotecas automatizadas, você é solicitado a inserir o volume no slot de entrada/saída da biblioteca. Se nenhuma estação de entrada/saída (E/S) de conveniência estiver disponível, insira o volume em um slot vazio. É possível rotular os volumes ao efetuar check-in deles ou antes de efetuar check-in dos mesmos.

Procedimento

Para rotular volumes de fita antes de efetuar check-in deles, conclua as seguintes etapas:

1. Etiquete os volumes de fita emitindo o comando **LABEL LIBVOLUME**.
   Por exemplo, para nomear um volume de biblioteca VOLUME1 em uma biblioteca que é denominada LIBRARY 1, emita o comando a seguir:

   ```
   label libvolume library1 volume1
   ```

   Exigência: Pelo menos uma unidade deve estar disponível. A unidade não pode ser usada por outro processo do IBM Spectrum Protect. Se uma unidade estiver inativa, ela será considerada indisponível.
2. Para sobrescrever uma etiqueta existente, especifique o parâmetro OVERWRITE=YES. Por padrão, o comando **LABEL LIBVOLUME** não sobrescreve um rótulo existente.

Tarefas relacionadas

Etiquetando novos volumes usando AUTOLABEL
Usar o parâmetro **AUTOLABEL** no comando **DEFINE LIBRARY** ou **UPDATE LIBRARY** é mais eficiente do que usar o comando **LABEL LIBVOLUME**, que requer a montagem dos volumes separadamente.

Informações relacionadas

LABEL LIBVOLUME (Rotular um volume de biblioteca)

Rotulando volumes em uma biblioteca biblioteca

É possível rotular volumes individualmente ou usar o IBM Spectrum Protect para procurar na biblioteca por volumes e rotular os volumes localizados.

Rotulando volumes individualmente

Ao rotular volumes individualmente usando o comando **LABEL LIBVOLUME**, deve-se especificar um nome de volume.

Procedimento

1. Insira os volumes no slot de entrada/saída da biblioteca quando o servidor solicitar. A biblioteca monta cada volume inserido em uma unidade.
2. Para uma biblioteca SCSI, insira um nome de volume quando solicitado. Um rótulo com o nome especificado é gravado no volume.

   Dica: Para solicitar o nome do volume para uma biblioteca SCSI, emita o comando **LABEL LIBVOLUME** e especifique o parâmetro **LABELSOURCE=PROMPT**.
3. Se a biblioteca não tiver uma porta de entrada/saída, será solicitado a remover a fita de um número de slot especificado. Remova a fita do slot especificado.

   Se a biblioteca tiver uma porta de entrada/saída, o comando retornará, por padrão, cada volume rotulado para a porta de entrada/saída da biblioteca.

Sobrescrevendo rótulos de volume em uma biblioteca SCSI

Será possível usar o comando **LABEL LIBVOLUME** para sobrescrever rótulos de volume existentes se nenhum dado válido existir nos volumes de armazenamento.

Sobre Esta Tarefa

Será possível rotular volumes em uma biblioteca SCSI, mesmo se eles não tiverem uma porta de entrada/saída. Deve-se inserir manualmente cada novo volume na biblioteca e colocá-los em slots de armazenamento dentro da biblioteca após seus rótulos serem gravados.

Procedimento

Sobrescreva os rótulos de volume existentes emitindo o comando **LABEL LIBVOLUME**. Por exemplo, se o nome da biblioteca for LIB1 e o nome do volume for VOLNAME, emita o comando a seguir:

```
label libvolume lib1 volname overwrite=yes
```

Etiquetando novos volumes usando AUTOLABEL

Usar o parâmetro **AUTOLABEL** no comando **DEFINE LIBRARY** ou **UPDATE LIBRARY** é mais eficiente do que usar o comando **LABEL LIBVOLUME**, que requer a montagem dos volumes separadamente.

Procedimento

Emita o comando **DEFINE LIBRARY** ou **UPDATE LIBRARY** e especifique o parâmetro **AUTOLABEL**.

Dica: Se usar o parâmetro **AUTOLABEL** com uma biblioteca SCSI, você deverá efetuar check-in das fitas especificando o parâmetro **CHECKLABEL=BARCODE** no comando **CHECKIN LIBVOLUME**. O parâmetro **AUTOLABEL** está padronizado como YES para todas as bibliotecas não-SCSI e NO para as bibliotecas SCSI. O parâmetro **CHECKLABEL=BARCODE** será respeitado apenas se a biblioteca tiver um leitor de código de barras.

Informações relacionadas

CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)

DEFINE LIBRARY (Definir uma biblioteca)

LABEL LIBVOLUME (Rotular um volume de biblioteca)

Procurando em uma biblioteca e etiquetando volumes

O IBM Spectrum Protect pode procurar volumes em todos os slots de armazenamento de uma biblioteca e pode tentar etiquetar cada volume que localizar.

Procedimento

Para procurar em uma biblioteca e etiquetar volumes, emita o comando **LABEL LIBVOLUME** e especifique o parâmetro **SEARCH=YES**.

Dica: Se você usar uma biblioteca SCSI e ela tiver um leitor de código de barras, o comando **LABEL LIBVOLUME** poderá usar o leitor para obter nomes de volumes em vez de solicitar a você os nomes dos volumes. O parâmetro **LABELSOURCE=BARCODE** é válido somente para bibliotecas SCSI.

Por exemplo, para etiquetar todos os volumes em uma biblioteca SCSI, emita o comando a seguir:

```
label libvolume library_name search=yes labelsource=barcode
```

O IBM Spectrum Protect seleciona a próxima unidade disponível para que você possa continuar sua procura.

Resultados

Após um volume ser etiquetado, o volume será retornado para seu local original na biblioteca.

Informações relacionadas

LABEL LIBVOLUME (Rotular um volume de biblioteca)

Efetuando check-in de volumes em uma biblioteca automatizada

É possível efetuar check-in de um volume em uma biblioteca automatizada usando o comando **CHECKIN LIBVOLUME**.

Antes de Iniciar

Para etiquetar fitas automaticamente antes de efetuar check-in das mesmas, emita o comando **DEFINE LIBRARY** e especifique o parâmetro **AUTOLABEL=YES**. Ao usar o parâmetro **AUTOLABEL**, você elimina a necessidade de pré-etiquetar um conjunto de fitas.

Sobre Esta Tarefa

Cada volume que for usado por um servidor com qualquer propósito deve ter um nome exclusivo. Esse requisito se aplica a todos os volumes, independentemente de serem usados para conjuntos de armazenamento ou para operações como backup e exportação de banco de dados. O requisito também se aplica a volumes que estão em bibliotecas diferentes, mas que são usados pelo mesmo servidor.

Dicas:

- Não use uma única biblioteca para volumes que tenham etiquetas de código de barras e volumes que não tenham etiquetas de código de barras. A varredura de código de barras pode levar um longo tempo para volumes não etiquetados.
- O servidor aceita apenas fitas etiquetadas com rótulos padrão IBM.
- Qualquer volume que tenha um código de barras iniciado por CLN será tratado como uma fita de limpeza.
- Se um volume possuir uma entrada no histórico do volume, não será possível verificar como volume de trabalho.

Procedimento

1. Para efetuar check-in de um volume de armazenamento em uma biblioteca, emita o comando **CHECKIN LIBVOLUME**.

   Dica: O comando sempre é executado como um processo de segundo plano. Espere a conclusão do processamento do processo **CHECKIN LIBVOLUME** antes de definir volumes, caso contrário, o processo de definição falhará. É possível economizar tempo efetuando check-in de volumes como parte da operação de etiquetagem.
2. Nomeie a biblioteca e especifique se o volume é um volume privado ou um volume utilizável. Dependendo se você usa volumes utilizáveis ou volumes privados, conclua uma das etapas a seguir:
   - Se você usar somente volumes utilizáveis, assegure que haja volumes utilizáveis suficientes disponíveis. Por exemplo, você pode precisar etiquetar mais volumes. À medida que os volumes são usados, você também poderá precisar aumentar o número de volumes utilizáveis permitidos no conjunto de armazenamentos definido para essa biblioteca.
   - Se você deseja usar volumes privados, além de ou em vez de volumes utilizáveis na biblioteca, defina volumes para o conjunto de armazenamentos usando o comando **DEFINE VOLUME**. Deve-se etiquetar e efetuar check-in dos volumes definidos.

Tarefas relacionadas

Etiquetando volumes de fita
Deve-se etiquetar volumes de fita antes que o servidor possa usá-los.

Verificando um volume único em uma biblioteca SCSI

É possível efetuar check-in de um único volume emitindo o comando **CHECKIN LIBVOLUME** e especificando o parâmetro **SEARCH=NO**. O IBM Spectrum Protect solicita que o operador de montagem carregue o volume na porta de entrada/saída da biblioteca.

Procedimento

1. Emita o comando **CHECKIN LIBVOLUME**.

   Por exemplo, para efetuar check-in do volume VOL001, insira o comando a seguir:

   ```
   checkin libvolume tapelib vol001 search=no status=scratch
   ```
2. Responda ao prompt do servidor.
   - Se a biblioteca tiver uma porta de entrada/saída, será solicitado a inserir uma fita na porta de entrada/saída.
   - Se a biblioteca não tiver uma porta de entrada/saída, será solicitado a inserir uma fita em um dos slots na biblioteca. Os endereços de elemento identificam esses slots. Por exemplo, o servidor localiza o primeiro slot vazio no endereço do elemento 5. A mensagem a seguir é retornada:

     ```
     ANR8306I 001: Insert 8MM volume VOL001 R/W in slot with element
     address 5 of library TAPELIB within 60 minutes; issue 'REPLY' along
     with the request ID when ready.
     ```

Se você não souber o local de endereço do elemento 5 na biblioteca, verifique a planilha para o dispositivo. Para localizar a planilha, revise a documentação para sua biblioteca. Depois de inserir o volume conforme solicitado, responda à mensagem de um cliente administrativo do IBM Spectrum Protect. Emita o comando **REPLY**, seguido pelo número da solicitação (o número no início da solicitação de montagem), por exemplo:

```
reply 1
```

Dica: Os endereços de elemento às vezes são numerados começando com um número diferente de 1. Verifique a planilha para ter certeza. Se nenhuma planilha estiver listada para seu dispositivo no IBM Support Portal for IBM Spectrum Protect, consulte a documentação de sua biblioteca.

Se você especificar um tempo de espera de 0 usando o parâmetro **WAITTIME** opcional no comando **CHECKIN LIBVOLUME**, um comando **REPLY** não será necessário. O tempo de espera padrão é de 60 minutos.

Efetuando check-in de volumes a partir de slots de armazenamento da biblioteca
Quando você tem muitos volumes para efetuar check-in e deseja evitar a emissão de um comando **CHECKIN LIBVOLUME** para cada volume, é possível procurar por slots de armazenamento para novos volumes. O servidor localiza volumes que ainda não foram incluídos no inventário de volume.

Procedimento

1. Abra a biblioteca e coloque os novos volumes em slots não utilizados.
   Por exemplo, para um dispositivo SCSI, abra a porta de acesso à biblioteca, coloque todos os novos volumes em slots não utilizados e feche a porta.
2. Se os volumes não estiverem rotulados, use o comando **LABEL LIBVOLUME** para rotular o volume.
3. Emita o comando **CHECKIN LIBVOLUME** com o parâmetro **SEARCH=YES**.

Informações relacionadas
CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)

Efetuando check-in de volumes em portas de entrada/saída da biblioteca
É possível procurar por todos os slots de portas de entrada/saída em massa para volumes rotulados e o servidor pode efetuar check-in deles automaticamente.

Antes de Iniciar
Emita o comando **LABEL LIBVOLUME** para rotular volumes que não estiverem rotulados.

Sobre Esta Tarefa
Para bibliotecas SCSI, o servidor varre todas as portas de entrada/saída na biblioteca em busca de volumes. Se um volume for localizado contendo um rótulo de volume válido, ele será registrado automaticamente.

Procedimento

Emita o comando **CHECKIN LIBVOLUME** e especifique o parâmetro **SEARCH=BULK**.

- Para carregar uma fita em uma unidade e ler o rótulo, especifique o parâmetro **CHECKLABEL=YES**. Após o servidor ler o rótulo, o servidor moverá a fita da unidade para um slot de armazenamento.
- Para que o servidor use o leitor de código de barras para verificar rótulos externos nas fitas, especifique o parâmetro **CHECKLABEL=BARCODE**. Quando a leitura de código de barras é ativada, o servidor lê o rótulo e move a fita da porta de entrada/saída para um slot de armazenamento.

Efetuando check-in de volumes usando leitores de código de barras da biblioteca
É possível economizar tempo ao efetuar check-in de volumes para bibliotecas que possuírem leitores de código de barras utilizando os caracteres nos rótulos de código de barras como nomes para os volumes.

Sobre Esta Tarefa

O servidor lê os rótulos de código de barras e usa as informações para gravar os rótulos de mídia interna. Para volumes que não tiverem rótulos de código de barras, o servidor monta os volumes em uma unidade e tenta ler o rótulo interno registrado.

Procedimento

Emita o comando **CHECKIN LIBVOLUME** com o parâmetro **CHECKLABEL=BARCODE**.
Por exemplo, para usar um leitor de código de barras para procurar por uma biblioteca que seja denominada TAPELIB e efetuar check-in de uma fita inicial, emita o comando a seguir:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

Efetuando check-in de volumes usando um leitor de código de barras

É possível economizar tempo ao efetuar check-in de volumes usando um leitor de código de barras, se sua biblioteca tiver um.

Sobre Esta Tarefa

Ao efetuar check-in de um volume, é possível especificar se os rótulos de mídia são lidos durante o processamento de check-in. Quando a verificação de rótulo está ligada, o IBM Spectrum Protect monta cada volume para ler o rótulo interno e efetuará check-in de um volume apenas se ele estiver rotulado corretamente. A verificação de rótulo pode evitar erros futuros quando os volumes são usados em conjuntos de armazenamentos, mas também aumenta o tempo de processamento no check-in.

Se um volume não tiver etiqueta de código de barras, o IBM Spectrum Protect montará os volumes em uma unidade e tentará ler a etiqueta registrada.

Procedimento

Para efetuar check-in de volumes usando um leitor de código de barras, emita o comando **CHECKIN LIBVOLUME** e especifique **CHECKLABEL=BARCODE**. Por exemplo, para usar o leitor de código de barras para efetuar check-in de todos os volumes como volumes utilizáveis em uma biblioteca que é denominada TAPELIB, emita o comando a seguir:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

Tarefas relacionadas

Preparando mídia removível
Deve-se preparar mídia removível antes que ela possa ser usada para armazenar dados. As tarefas típicas de preparação incluem etiquetagem e check-in de volumes.

Informações relacionadas

CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)

Efetuando check-in de volumes em uma biblioteca cheia com troca

Se nenhum slot vazio estiver disponível na biblioteca quando você estiver efetuando check-in de volumes, a operação de check-in falhará, a menos que você ative *troca*. Se você ativar troca e a biblioteca estiver cheia, o servidor selecionará um volume para ejetar e, em seguida, efetuará check-in do volume solicitado.

Sobre Esta Tarefa

O servidor seleciona o volume a ejetar verificando primeiramente se há qualquer volume utilizável disponível e, em seguida, o volume que é montado com menor frequência. O servidor ejeta o volume selecionado para a operação de troca na biblioteca e substitui o volume ejetado por um volume do qual está sendo efetuado check-in.

Procedimento

- Para trocar volumes se um slot de biblioteca vazio não estiver disponível para efetuar check-in de um volume, emita o comando **CHECKIN LIBVOLUME** e especifique o parâmetro **SWAP=YES**.
  Por exemplo, para efetuar check-in de um volume denominado VOL1 em uma biblioteca denominada AUTO e especificar troca, emita o comando a seguir:

```
checkin libvolume auto vol1 swap=yes
```

Tarefas relacionadas

Gerenciando uma biblioteca cheia com um local para excesso
À medida que a demanda por armazenamento cresce, o número de volumes que você precisa para um conjunto de armazenamentos pode exceder a capacidade física de uma biblioteca automatizada. Para disponibilizar espaço para novos volumes e monitorar os volumes existentes, é possível definir um local para excesso para um conjunto de armazenamentos.

Informações relacionadas

CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)

Volumes privados e volumes utilizáveis

Para otimizar o armazenamento em fita, revise as informações sobre volumes privados e volumes utilizáveis. Use volumes privados e volumes utilizáveis de forma apropriada.

Volumes privados não podem ser sobrescritos quando uma montagem utilizável é solicitada. Não é possível efetuar check-in de um volume com status utilizável quando esse volume é usado por um conjunto de armazenamentos, para exportar dados, fazer backup de um banco de dados ou fazer backup para um volume do conjunto de backup.

Os volumes parcialmente gravados são sempre volumes privados. Os volumes têm um status inicial ou privado, mas quando o IBM Spectrum Protect armazena dados neles, o status se torna privado.

Tabela 34. Usos de um volume privado e de um volume utilizável

Tipo de volume	**Quando Usar**
Volumes privados	Use volumes privados para regular os volumes usados por conjuntos de armazenamentos individuais e para controlar manualmente os volumes. Para definir volumes privados, emita o comando **DEFINE VOLUME**. Para operações de restauração do banco de dados, dumps de memória ou carregamentos, ou importação do servidor, você deve especificar volumes privados.
Volumes Livres	Em alguns casos, é possível simplificar o gerenciamento de volumes usando volumes utilizáveis. É possível usar volumes utilizáveis nas seguintes circunstâncias: • Quando não precisar definir cada volume do conjunto de armazenamentos. • Quando desejar aproveitar a automação de dispositivos robóticos. • Quando conjuntos de armazenamentos diferentes compartilham uma biblioteca automatizada e quando conjuntos de armazenamentos podem adquirir volumes dinamicamente por meio dos volumes utilizáveis na biblioteca. Os volumes não precisam ser pré-alocados para os conjuntos de armazenamentos.

Tarefas relacionadas

Mudando o status de um volume em uma biblioteca automatizada
É possível mudar o status de um volume de privado para inicial ou de inicial para privado.

Informações relacionadas

CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)
DELETE VOLUME (Excluir um volume do conjunto de armazenamento)

Endereços de elementos para slots de armazenamento da biblioteca

Um endereço do elemento é um número que indica o local físico de um slot de armazenamento ou de uma unidade dentro de uma biblioteca automatizada.

Se uma biblioteca tiver portas de entrada/saída, será possível incluir e remover mídia usando as portas. Se nenhuma porta de entrada/saída existir, as fitas deverão ser carregadas nos slots de armazenamento.

Se você carregar as fitas nos slots de armazenamento, deve-se responder a solicitações de montagem que identificam slots de armazenamento com endereços de elementos. Se especificar um tempo de espera de 0 no comando **CHECKIN LIBVOLUME** ou no comando **LABEL LIBVOLUME**, não será necessário responder a uma solicitação de montagem.

Para endereços do elemento, consulte a documentação do fabricante do dispositivo ou acesse o IBM Support Portal for IBM Spectrum Protect e procure pelos endereços de elemento.

Informações relacionadas

CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)
LABEL LIBVOLUME (Rotular um volume de biblioteca)

Gerenciando o inventário de volume

É possível gerenciar o inventário de volumes controlando o acesso do servidor aos volumes reutilizando fitas e reutilizando volumes que são usados para operações de backup e de exportação de banco de dados. Também é possível gerenciar o inventário mantendo um suprimento de volumes utilizáveis.

Sobre Esta Tarefa

Cada volume que for usado por um servidor deve ter um nome exclusivo, independentemente se os volumes forem usados para conjuntos de armazenamentos ou usados para operações, como backup e exportação de banco de dados. Os volumes que estiverem em bibliotecas diferentes, mas que forem usados pelo mesmo servidor, também devem ter um nome exclusivo.

Controlando acesso a volumes

É possível utilizar métodos diferentes para controlar o acesso aos volumes.

Procedimento

Para controlar o acesso aos volumes, execute qualquer uma das ações a seguir:

- Para evitar que o servidor monte um volume, emita o comando **UPDATE VOLUME** e especifique o parâmetro **ACCESS=UNAVAILABLE**.
- Para tornar os volumes indisponíveis e enviá-los externamente para proteção, use um conjunto de armazenamentos de cópia ou um conjunto de armazenamentos de dados ativos.
- É possível fazer backup de conjuntos de armazenamentos primários para um conjunto de armazenamentos de cópia e, em seguida, enviar os volumes do conjunto de armazenamentos de cópias externamente.
- É possível copiar versões ativas de dados de backup do cliente para conjuntos de armazenamentos de dados ativos e, em seguida, enviar os volumes externamente.
- É possível rastrear volumes do conjunto de armazenamentos de cópia e volumes do conjunto de dados ativos mudando o modo de acesso para externo e atualizando o histórico de volume para identificar seu local.

Informações relacionadas

UPDATE VOLUME (Atualizar um volume do conjunto de armazenamentos)

Reutilizando fitas

Para assegurar um fornecimento de fitas adequado, é possível expirar arquivos antigos, recuperar volumes e excluir volumes que atingirem o término de vida. Também é possível manter um fornecimento de volumes utilizáveis.

Sobre Esta Tarefa

Com o tempo e dependendo da idade da mídia, talvez você não precise de alguns dos dados de backup que estiverem armazenados na mídia. É possível definir políticas do servidor para determinar quantas versões de backup são retidas e por quanto tempo são retidas. É possível usar o processo de expiração para excluir arquivos que não são mais necessários. É possível manter os dados que você precisa na mídia. Quando você não precisa mais dos dados, é possível recuperar e reutilizar a mídia.

Procedimento

1. Exclua dados do cliente desnecessários executando regularmente o processo de expiração. O processamento de expiração exclui dados que não forem mais válidos, porque eles excedem as especificações de retenção na política ou porque os usuários ou administradores excluíram as versões ativas dos dados.
2. Reutilize volumes em conjuntos de armazenamentos executando o processamento de recuperação.

   O processamento de recuperação consolida quaisquer dados não expirados movendo-os de vários volumes para menos volumes. A mídia poderá então ser retornada ao conjunto de armazenamentos e reutilizada.
3. Reutilize volumes que contenham backups de banco de dados desatualizados ou dados exportados que não forem mais necessários excluindo histórico do volume.

   Antes que o servidor possa reutilizar volumes controlados no histórico do volume, deve-se excluir as informações do volume do arquivo do histórico de volume emitindo o comando **DELETE VOLHISTORY**.

   Dica: Se o seu servidor usar a função gerenciador de recuperação de desastre (DRM), as informações do volume serão excluídas automaticamente durante o processamento do comando **MOVE DRMEDIA**.
4. Determine quando os volumes de fita atingem o término de vida. É possível usar o servidor para exibir estatísticas sobre volumes, incluindo o número de operações de gravação concluídas na mídia e o número de erros de gravação. Os volumes privados e volumes utilizáveis exibem os seguintes dados estatísticos:

   Volumes privados
   Para mídia inicialmente definida como volumes privados, o servidor mantém esses dados estatísticos, mesmo quando o volume é recuperado. É possível comparar as informações com o número de operações de gravação e de erros de gravação recomendado pelo fabricante.

   Volumes Livres
   Para mídia definida inicialmente como volumes utilizáveis, o servidor sobrescreve esses dados estatísticos toda vez que os volumes são recuperados.
5. Recupere quaisquer dados válidos de volumes que atinjam o término de vida. Se os volumes estiverem em bibliotecas automatizadas, efetue check-out dos mesmos do inventário de volume. Exclua volumes privados do banco de dados com o comando **DELETE VOLUME**.
6. Assegure que os volumes estejam disponíveis para rotação de fita para que o conjunto de armazenamentos não fique sem espaço. É possível usar o Operations Center para monitorar a disponibilidade de volumes utilizáveis. Assegure-se de que o número de volumes utilizáveis seja alto o suficiente para atender à demanda. Para obter informações adicionais, consulte “Mantendo um suprimento de volumes em uma biblioteca que contém mídia WORM” na página 187.

mídia WORM: As unidades Write Once Read Many (WORM) podem desperdiçar mídia quando o servidor cancela transações, já que os volumes ficam indisponíveis para concluir a operação de backup. Após o servidor gravar em volumes WORM, o espaço nos volumes não poderá ser reutilizado, mesmo se as transações forem canceladas (por exemplo, se um backup for cancelado devido a uma escassez de mídia no dispositivo). Para minimizar mídia WORM desperdiçada, conclua as ações a seguir:

a. Assegure que o número máximo de volumes utilizáveis para o conjunto de armazenamentos de dispositivo seja pelo menos igual ao número de slots de armazenamento na biblioteca.
b. Verificar volumes suficientes no inventário de volume do dispositivo para a carga esperada.

Se a maioria das operações de backup for para arquivos pequenos, o controle do tamanho da transação poderá afetar o modo com que as lâminas WORM são usadas. Transações menores significam que menos espaço é gasto quando uma transação, como uma operação de backup, tiver que ser cancelada. O tamanho da transação é controlado por uma opção do servidor, TXNGROUPMAX, e uma opção do cliente, TXNBYTELIMIT.

Tarefas relacionadas

Migrando dados para unidades com upgrade
Se você fizer upgrade de todas as unidades de fita em uma biblioteca, será possível preservar suas definições de política existentes para migrar e expirar dados existentes e também usar as novas unidades para armazenar dados.

Gerenciando solicitações do servidor para volumes
O IBM Spectrum Protect exibe as solicitações e as mensagens de status para todos os clientes administrativos da linha de comandos que forem iniciados no modo do console. Essas mensagens de solicitação frequentemente têm um limite de tempo. As operações do servidor bem-sucedidas devem ser concluídas dentro do limite de tempo que for especificado; caso contrário, a operação atingirá o tempo limite.

Informações relacionadas

DELETE VOLHISTORY (Excluir informações de histórico de volume sequencial)
DELETE VOLUME (Excluir um volume do conjunto de armazenamento)
EXPIRE INVENTORY (Iniciar manualmente o processo de expiração de inventário)
RECLAIM STGPOOL (Recuperar volumes em um conjunto de armazenamentos de acesso sequencial)
Opção Txnbytelimit
opção do servidor TXNGROUPMAX

Mantendo um fornecimento de volumes utilizáveis

Deve-se configurar o número máximo de volumes utilizáveis para um conjunto de armazenamentos grande o suficiente para o uso esperado.

Sobre Esta Tarefa

Quando se define um conjunto de armazenamentos, é preciso especificar o número máximo de volumes livres que o conjunto de armazenamentos pode utilizar. O servidor solicita automaticamente um volume utilizável quando necessário. Quando o número de volumes utilizáveis que o servidor está usando para o conjunto de armazenamentos excede o máximo especificado, o conjunto de armazenamentos pode ficar sem espaço.

Procedimento

Quando um conjunto de armazenamentos precisa de mais do que o número máximo de volumes utilizáveis, é possível executar uma ou as duas ações a seguir:

1. Aumente o número máximo de volumes utilizáveis emitindo o comando **UPDATE STGPOOL** e especificando o parâmetro **MAXSCRATCH**.
2. Disponibilize volumes para reutilização executando o processamento de expiração e a recuperação para consolidar dados em menos volumes.

a) Emita o comando **EXPIRE INVENTORY** para executar o processamento de expiração.

Dica: Por padrão, esse processo é executado automaticamente todos os dias. Também é possível especificar a opção do servidor **EXPINTERVAL** no arquivo de opções do servidor, `dsmserv.opt`, para executar o processamento de expiração automaticamente. Um valor de 0 significa que o comando **EXPIRE INVENTORY** deve ser usado para executar o processamento de expiração.

b) Emita o comando **RECLAIM STGPOOL** para executar o processamento de recuperação.

Dica: Também é possível especificar limites de recuperação ao definir o conjunto de armazenamentos usando o comando **DEFINE STGPOOL** e especificando o parâmetro **RECLAIMPROCESS**.

O que Fazer Depois

Se você precisar de mais volumes para operações de backup futuras, rotule mais volumes utilizáveis usando o comando **LABEL LIBVOLUME**.

Tarefas relacionadas

Mantendo um fornecimento de volumes utilizáveis em uma biblioteca automatizada

Ao definir um conjunto de armazenamentos associado a uma biblioteca automatizada, será possível especificar um número máximo de volumes utilizáveis igual à capacidade física da biblioteca. Se o servidor estiver usando um número maior de volumes utilizáveis para o conjunto de armazenamentos, assegure-se de que volumes suficientes estejam disponíveis.

Informações relacionadas

EXPIRE INVENTORY (Iniciar manualmente o processo de expiração de inventário)

LABEL LIBVOLUME (Rotular um volume de biblioteca)

RECLAIM STGPOOL (Recuperar volumes em um conjunto de armazenamentos de acesso sequencial)

UPDATE STGPOOL (Atualizar um conjunto de armazenamentos)

Mantendo um suprimento de volumes em uma biblioteca que contém mídia WORM

Para bibliotecas que contêm mídia Write Once Read Many (WORM), é possível evitar o cancelamento de transações de armazenamento de dados mantendo um suprimento de volumes utilizáveis ou novos privados na biblioteca. As transações canceladas podem fazer com que a mídia WORM seja desperdiçada.

Sobre Esta Tarefa

O IBM Spectrum Protect cancela uma transação se volumes, privados ou utilizáveis, estiverem indisponíveis para concluir a operação de armazenamento de dados. Após o IBM Spectrum Protect iniciar uma transação gravando em um volume WORM, o espaço gravado no volume não poderá ser reutilizado, mesmo se a transação for cancelada.

Por exemplo, se você tiver volumes WORM retendo 2,6 GB cada e um cliente iniciar backup de um arquivo de 12 GB. Se o IBM Spectrum Protect não puder adquirir um quinto volume utilizável após quatro volumes estarem cheios, o IBM Spectrum Protect cancela a operação de backup. Os quatro volumes que o IBM Spectrum Protect já preencheu não poderão ser reutilizados.

Para minimizar o cancelamento de transações, deve-se ter volumes suficientes disponíveis na biblioteca para gerenciar operações esperadas do cliente, como backups.

Procedimento

1. Assegure que o conjunto de armazenamentos associado à biblioteca tenha volumes utilizáveis suficientes. Emita o comando **UPDATE STGPOOL** e especifique o parâmetro **MAXSCRATCH**.
2. Para gerenciar a carga esperada, efetue check-in de um número suficiente de volumes utilizáveis ou privados na biblioteca emitindo o comando **CHECKIN LIBVOLUME**.
3. Para controlar o tamanho da transação, especifique a opção do servidor TXNGROUPMAX e a opção do cliente TXNBYTELIMIT. Se seus clientes tendem a armazenar arquivos pequenos, controlar o tamanho da transação pode afetar como os volumes WORM são usados. Transações menores desperdiçam menos espaço quando uma transação, como um backup, deve ser cancelada.

Informações relacionadas

CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)
UPDATE STGPOOL (Atualizar um conjunto de armazenamentos)
Opção Txnbytelimit
opção do servidor TXNGROUPMAX

Gerenciar o inventário de volume em bibliotecas automatizadas

O servidor IBM Spectrum Protect usa um inventário do volume de biblioteca para rastrear volumes utilizáveis e privados que estão disponíveis em uma biblioteca automatizada. Deve-se assegurar que o inventário seja consistente com os volumes que estão fisicamente na biblioteca.

O inventário de volumes de biblioteca é separado do inventário de volumes para cada conjunto de armazenamentos. Para incluir um volume em um inventário do volume de biblioteca, você efetua check-in de um volume nessa biblioteca do IBM Spectrum Protect.

Uma lista de volumes no inventário do volume de biblioteca pode não ser idêntica a uma lista de volumes no inventário do conjunto de armazenamentos para o dispositivo. Por exemplo, é possível efetuar check-in de volumes utilizáveis na biblioteca, mas não é possível defini-los para um conjunto de armazenamentos. Se volumes utilizáveis não forem selecionados para operações de backup, será possível definir volumes privados para um conjunto de armazenamentos, mas não será possível vê-los no inventário de volume para o dispositivo.

Para assegurar que o inventário de volume da biblioteca do servidor permaneça preciso, efetue check-out de volumes para remover fisicamente os volumes de uma biblioteca SCSI. Ao efetuar check-out de um volume que é usado por um conjunto de armazenamentos, o volume permanece no conjunto de armazenamentos. Se você tiver que montar o volume quando ele for retirado, uma mensagem para o console do operador de montagem será exibida com uma solicitação para verificar no volume. Se a operação de check-in for mal sucedida, o servidor marcará o volume como indisponível.

Quando um volume está no inventário do volume de biblioteca, é possível mudar o status do volume de zero para privado.

Para verificar se o inventário de volume da biblioteca do servidor está consistente com os volumes que estão fisicamente na biblioteca, é possível auditar a biblioteca. O inventário pode se tornar inexato se volumes forem movidos para dentro e para fora da biblioteca sem informar o servidor usando operações de check-in ou de check-out de volume.

Tarefas relacionadas

Efetuando check-in de volumes em uma biblioteca automatizada
É possível efetuar check-in de um volume em uma biblioteca automatizada usando o comando **CHECKIN LIBVOLUME**.

Informações relacionadas

AUDIT LIBRARY (Auditar inventários de volume em uma biblioteca automatizada)

Mudando o status de um volume em uma biblioteca automatizada

É possível mudar o status de um volume de privado para inicial ou de inicial para privado.

Procedimento

Para mudar o status de um volume, emita o comando **UPDATE LIBVOLUME**.
Por exemplo, para mudar o status de um volume que é denominado VOL1 para um volume privado, emita o comando a seguir:

```
update libvolume lib1 vol1 status=private
```

Restrições:

- Não é possível alterar o status de um volume de privado para utilizável se o volume pertencer a um conjunto de armazenamentos ou estiver definido no arquivo do histórico de volume.

- Os volumes privados devem ser volumes definidos pelo administrador sem dados ou com dados inválidos. Eles não podem ser volumes parcialmente gravados que contêm dados ativos. Estatísticas de volume são perdidas quando os status de volume são modificados.

Removendo volumes de uma biblioteca automatizada
É possível remover volumes de uma biblioteca automatizada se você tiver exportado dados para um volume e deseja importar os dados para outro sistema. Você também pode querer remover volumes para criar espaço para novos volumes.

Sobre Esta Tarefa
Por padrão, o servidor monta o volume do qual você efetuou check-out e verifica a etiqueta interna. Quando a etiqueta é verificada, o servidor remove o volume do inventário de volumes de biblioteca e, em seguida, o move para a porta de entrada/saída ou estação de E/S De conveniência da biblioteca. Se a biblioteca não tiver uma porta de entrada/saída, o servidor solicita que o operador de montagem remova o volume de um slot ou dispositivo dentro da biblioteca.

Procedimento

- Para remover um volume de uma biblioteca automatizada, emita o comando **CHECKOUT LIBVOLUME**.
- Para bibliotecas automatizadas com múltiplas portas de entrada/saída, emita o comando **CHECKOUT LIBVOLUME** e especifique o parâmetro **REMOVE=BULK**. O servidor ejeta o volume para a próxima porta de entrada/saída disponível.

O que Fazer Depois
Se efetuar check-out de um volume que estiver definido em um conjunto de armazenamentos e o servidor tiver que acessar o volume posteriormente, o servidor solicitará que esse volume seja registrado. Para retornar volumes a uma biblioteca, emita o comando **CHECKIN LIBVOLUME**.
Informações relacionadas
CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)
CHECKOUT LIBVOLUME (Verificar um Volume de Armazenamento Fora de uma Biblioteca)

Mantendo um fornecimento de volumes utilizáveis em uma biblioteca automatizada
Ao definir um conjunto de armazenamentos associado a uma biblioteca automatizada, será possível especificar um número máximo de volumes utilizáveis igual à capacidade física da biblioteca. Se o servidor estiver usando um número maior de volumes utilizáveis para o conjunto de armazenamentos, assegure-se de que volumes suficientes estejam disponíveis.

Procedimento

Se o número de volumes utilizáveis que o servidor está usando para o conjunto de armazenamentos exceder o número especificado na definição do conjunto de armazenamentos, conclua as etapas a seguir:

1. Inclua volumes utilizáveis na biblioteca emitindo o comando **CHECKIN LIBVOLUME**.

   Dica: Poderá ser necessário usar um local para excesso para mover volumes para fora da biblioteca para liberar espaço para esses volumes utilizáveis. Para obter informações adicionais, consulte “Gerenciando uma biblioteca cheia com um local para excesso” na página 190.
2. Aumente o número máximo de volumes utilizáveis que podem ser incluídos em um conjunto de armazenamentos, emitindo o comando **UPDATE STGPOOL** e especificando o parâmetro **MAXSCRATCH**.

O que Fazer Depois

Você pode precisar de mais volumes para operações de recuperação futura, portanto, considere etiquetar e separar volumes utilizáveis adicionais.

Tarefas relacionadas
Mantendo um fornecimento de volumes utilizáveis
Deve-se configurar o número máximo de volumes utilizáveis para um conjunto de armazenamentos grande o suficiente para o uso esperado.

Gerenciando uma biblioteca cheia com um local para excesso

À medida que a demanda por armazenamento cresce, o número de volumes que você precisa para um conjunto de armazenamentos pode exceder a capacidade física de uma biblioteca automatizada. Para disponibilizar espaço para novos volumes e monitorar os volumes existentes, é possível definir um local para excesso para um conjunto de armazenamentos.

Sobre Esta Tarefa

O servidor controla os volumes que são movidos para a área de estouro e disponibiliza slots de armazenamento para novos volumes.

Procedimento

1. Crie um local para excesso de volume. Defina ou atualize o conjunto de armazenamentos associado à biblioteca automatizada emitindo o comando **DEFINE STGPOOL** ou **UPDATE STGPOOL** e especificando o parâmetro **OVFLOCATION**.
   Por exemplo, para criar um local para excesso denominado ROOM2948 para um conjunto de armazenamentos denominado ARCHIVEPOOL, emita o comando a seguir:

   ```
   update stgpool archivepool ovflocation=Room2948
   ```

2. Quando precisar criar espaço na biblioteca para volumes utilizáveis, mova volumes completos para o local para excesso emitindo o comando **MOVE MEDIA**.
   Por exemplo, para mover todos os volumes cheios do conjunto de armazenamentos especificado para fora da biblioteca, emita o comando a seguir:

   ```
   move media * stgpool=archivepool
   ```

3. Efetue check-in de volumes utilizáveis conforme necessário.

   Restrição: Se um volume tiver uma entrada no arquivo do histórico de volume, não será possível efetuar seu check-in como um volume utilizável. Para obter informações adicionais, consulte “Efetuando check-in de volumes em uma biblioteca automatizada” na página 179.

4. Identifique as fitas utilizáveis vazias no local para excesso emitindo o comando **QUERY MEDIA**.
   Por exemplo, emita o seguinte comando:

   ```
   query media * stg=* whereovflocation=Room2948 wherestatus=empty
   ```

5. Se o servidor solicitar volumes adicionais, localize e efetue check-in de volumes do local para excesso.

   Para localizar volumes em um local para excesso, emita o comando **QUERY MEDIA**. Também é possível utilizar o comando **QUERY MEDIA** para gerar comandos efetuando check-in dos volumes.

   Por exemplo, para listar os volumes no local para excesso e, ao mesmo tempo, gerar os comandos para efetuar check-in desses volumes na biblioteca, emita um comando que seja semelhante ao exemplo a seguir:

   ```
   query media format=cmd stgpool=archivepool whereovflocation=Room2948
   cmd="checkin libvol autolib &vol status=private"
   cmdfilename="\storage\move\media\checkin.vols"
   ```

   Dicas:

   - As solicitações de montagem do servidor incluem o local dos volumes.
   - Para especificar o número de dias que devem decorrer antes que os volumes estejam elegíveis para processamento, emita o comando **UPDATE STGPOOL** e especifique o parâmetro **REUSEDELAY**.
   - O arquivo que contém os comandos gerados pode ser executado usando o comando IBM Spectrum Protect **MACRO**.

Informações relacionadas

MOVE MEDIA (Mover a mídia de conjunto de armazenamentos de acesso sequencial)
QUERY MEDIA (Consultar mídia de conjunto de armazenamentos de acesso sequencial)

UPDATE STGPOOL (Atualizar um conjunto de armazenamentos)

Auditando o inventário de volume em uma biblioteca

É possível auditar uma biblioteca automatizada para assegurar que o inventário do volume de biblioteca seja consistente com os volumes que estão fisicamente na biblioteca. Talvez você deseja auditar uma biblioteca se o inventário de volume da biblioteca estiver distorcido devido ao movimento manual de volumes na biblioteca ou a problemas do banco de dados.

Procedimento

1. Assegure que nenhum volume seja montado nas unidades de biblioteca. Se quaisquer volumes forem montados no estado IDLE, emita o comando **DISMOUNT VOLUME** para desmontá-los.
2. Audite o inventário de volume emitindo o comando **AUDIT LIBRARY**. Execute uma das seguintes ações:
   - Se a biblioteca tiver um leitor de código de barras, será possível economizar tempo usando o leitor de código de barras para identificar volumes. Por exemplo, para auditar a biblioteca TAPELIB usando seu leitor de código de barras, emita o comando a seguir:

     ```
     audit library tapelib checklabel=barcode
     ```

   - Se a biblioteca não tiver um leitor de código de barras, emita o comando **AUDIT LIBRARY** sem especificar **CHECKLABEL=BARCODE**. O servidor monta cada volume para verificar o rótulo. Após o rótulo ser verificado, o servidor conclui a auditoria de quaisquer volumes restantes.

Resultados

O servidor exclui os volumes ausentes do inventário e atualiza os locais de volumes que foram movidos desde a última auditoria.

Restrição: O servidor não pode incluir novos volumes no inventário durante uma operação de auditoria.

Tarefas relacionadas

Etiquetando volumes de fita
Deve-se etiquetar volumes de fita antes que o servidor possa usá-los.

Informações relacionadas

AUDIT LIBRARY (Auditar inventários de volume em uma biblioteca automatizada)
DISMOUNT VOLUME (Desmontar um volume por nome de volume)

Volumes parcialmente gravados

Os volumes parcialmente gravados são sempre volumes privados, mesmo se seu status era inicial antes do servidor tê-los montado. O servidor controla o status original de volumes utilizáveis e os retorna para o status inicial quando eles estão vazios.

Exceto para volumes em bibliotecas automatizadas, o servidor não está ciente de um volume utilizável até após a montagem do volume. Então, o status do volume muda para privado e o volume é automaticamente definido como parte do conjunto de armazenamentos ao qual a solicitação de montagem foi feita.

Tarefas relacionadas

Mudando o status de um volume em uma biblioteca automatizada
É possível mudar o status de um volume de privado para inicial ou de inicial para privado.

Operações com bibliotecas compartilhadas

Bibliotecas compartilhadas são bibliotecas lógicas que são representadas fisicamente por bibliotecas SCSI . A biblioteca física é controlada pelo servidor do IBM Spectrum Protect que estiver configurado como um gerenciador de biblioteca. Os servidores do IBM Spectrum Protect que usam o tipo de

biblioteca SHARED são clientes de biblioteca para o servidor do gerenciador de bibliotecas do IBM Spectrum Protect.

O cliente da biblioteca entra em contato com o gerenciador de biblioteca quando o gerenciador de biblioteca inicia e o dispositivo de armazenamento inicializa ou após um gerenciador de biblioteca ser definido para um cliente de biblioteca. O cliente de biblioteca confirma que o servidor contatado é o gerenciador de bibliotecas para o dispositivo de biblioteca nomeado. O cliente de biblioteca também compara as definições da unidade com o gerenciador de biblioteca para garantir a consistência. O cliente de biblioteca entra em contato com o gerenciador de biblioteca para cada uma das seguintes operações:

Montagem do volume
Um cliente de biblioteca envia uma solicitação para o gerenciador de bibliotecas para acesso a um volume específico no dispositivo de biblioteca compartilhada. Para um volume utilizável, o cliente da biblioteca não especifica um nome de volume. Se o gerenciador de biblioteca não puder acessar o volume solicitado ou se os volumes utilizáveis estiverem indisponíveis, o gerenciador de biblioteca negará a solicitação de montagem. Se a montagem for bem-sucedida, o gerenciador de biblioteca retornará o nome da unidade em que o volume estiver montado.

Liberação do volume
Quando um cliente de biblioteca não precisa mais acessar um volume, ele notifica o gerenciador de biblioteca que o volume pode ser retornado para um volume utilizável. O banco de dados do gerenciador de biblioteca é atualizado com o novo local para o volume, que agora está no inventário do servidor de bibliotecas. O volume é excluído do inventário de volume do cliente de biblioteca.

O Tabela 35 na página 192 mostra a interação entre os clientes de biblioteca e o gerenciador de biblioteca no processamento das operações do IBM Spectrum Protect.

Tabela 35. Como servidores ativados para SAN processam operações do IBM Spectrum Protect

Operação **(Comando)**	**Gerenciador de biblioteca**	**Cliente de biblioteca**
Consultar volumes da biblioteca (**QUERY LIBVOLUME**)	Exibe os volumes que estiverem registrados na biblioteca. Para volumes privados, o servidor proprietário também é exibido.	Não aplicável.
Check-in e check-out de volumes da biblioteca (**CHECKIN LIBVOLUME**, **CHECKOUT LIBVOLUME**)	Envia os comandos para o dispositivo de biblioteca.	Não aplicável. Quando uma operação de check-in é necessária devido a uma operação de restauração do cliente, uma solicitação é enviada para o servidor do gerenciador de bibliotecas.
Mover a mídia e mover a mídia DRM (**MOVE MEDIA**, **MOVE DRMEDIA**)	Válido apenas para volumes que forem usados pelo servidor do gerenciador de bibliotecas.	Solicita que o servidor do gerenciador de bibliotecas conclua a operação. Gera um processo de check-out no servidor do gerenciador de bibliotecas.
Inventário de biblioteca de auditoria (**AUDIT LIBRARY**)	Sincroniza o inventário com o dispositivo de biblioteca.	Sincroniza o inventário com o servidor do gerenciador de bibliotecas.
Rotular um volume de biblioteca (**LABEL LIBVOLUME**)	Rotula e faz check-in dos volumes.	Não aplicável.

Tabela 35. Como servidores ativados para SAN processam operações do IBM Spectrum Protect (continuação)

Operação **(Comando)**	**Gerenciador de biblioteca**	**Cliente de biblioteca**
Desmontar um volume (**DISMOUNT VOLUME**)	Envia a solicitação para o dispositivo de biblioteca.	Solicita que o servidor do gerenciador de bibliotecas conclua a operação.
Consulta um volume (**QUERY VOLUME**)	Verifica se o volume é de propriedade do cliente da biblioteca de solicitação e verifica se o volume está no dispositivo de biblioteca.	Solicita que o servidor do gerenciador de bibliotecas conclua a operação.

Gerenciando solicitações do servidor para volumes

O IBM Spectrum Protect exibe as solicitações e as mensagens de status para todos os clientes administrativos da linha de comandos que forem iniciados no modo do console. Essas mensagens de solicitação frequentemente têm um limite de tempo. As operações do servidor bem-sucedidas devem ser concluídas dentro do limite de tempo que for especificado; caso contrário, a operação atingirá o tempo limite.

Sobre Esta Tarefa

Para bibliotecas automatizadas, use os comandos **CHECKIN LIBVOLUME** e **LABEL LIBVOLUME** para inserir cartuchos nos slots. Se especificar um valor para o parâmetro **WAITTIME**, uma mensagem de resposta será exibida. Se o valor do parâmetro for 0, nenhuma resposta será necessária. Ao emitir o comando **CHECKOUT LIBVOLUME**, os cartuchos deverão ser inseridos em slots e, em todos os casos, uma mensagem de resposta será exibida.

Procedimento

- A tabela a seguir fornece informações sobre como manipular diferentes tarefas de mídia do servidor.

Tarefa	**Detalhes**
Usar o cliente administrador para mensagens de montagem	O servidor envia mensagens de status de solicitação de montagem para o console do servidor e para todos os clientes administrativos da linha de comandos no modo de montagem ou no modo do console. Para iniciar um cliente administrativo da linha de comandos no modo de montagem, emita o comando **dsmadmc -mountmode** no cliente administrativo da linha de comandos.
Receber mensagens sobre bibliotecas automatizadas	É possível visualizar mensagens de montagem e mensagens de erro sobre bibliotecas automatizadas em clientes administrativos da linha de comandos no modo de montagem ou no modo do console. As mensagens de montagem são enviadas para a biblioteca e não a um operador. As mensagens sobre problemas com a biblioteca são enviadas à fila de mensagens de montagem.
Obter informações sobre solicitações pendentes do operador	Para obter informações sobre solicitações pendentes do operador, emita o comando **QUERY REQUEST** ou visualize a fila de mensagens de montagem em um cliente administrativo da linha de comandos que for iniciado no modo de montagem. Quando você emite o comando **QUERY REQUEST**, o servidor exibe ações solicitadas e a quantia de tempo restante antes de a solicitação atingir o tempo limite.

Tarefa	Detalhes
Responder a solicitações do operador	Quando o servidor requer uma resposta explícita a uma solicitação de montagem concluída, use o comando **REPLY**. O parâmetro *request_number* especifica o número de identificação da solicitação que informa ao servidor qual solicitação pendente do operador é concluída. Este número de três dígitos é sempre exibido como parte da mensagem de solicitação.
Cancelar uma solicitação do operador	Para cancelar uma solicitação de montagem para uma biblioteca, emita o comando **CANCEL REQUEST**. Para a maioria das solicitações associadas às bibliotecas SCSI automatizadas, um operador deve concluir uma ação de hardware ou do sistema para cancelar a montagem solicitada. Para essas solicitações, o comando **CANCEL REQUEST** não é aceito pelo servidor. O comando **CANCEL REQUEST** deve incluir o número de identificação da solicitação. Este número é incluído na mensagem de solicitação. Se desejar marcar o volume solicitado como **UNAVAILABLE**, emita o comando **CANCEL REQUEST** e especifique o parâmetro **PERMANENT**. Se especificar o parâmetro **PERMANENT**, o servidor não tentará montar o volume solicitado novamente. Isso é útil se, por exemplo, o volume estiver em um site remoto ou estiver indisponível de outra forma.
Responder a uma solicitação de check-in de volume	Se o servidor não conseguir localizar um volume em particular para montar em uma biblioteca automatizada, o servidor solicitará que o operador efetue check-in do volume. Se o volume solicitado estiver disponível, coloque o volume na biblioteca e efetue check-in dele. Para obter informações adicionais, consulte “Efetuando check-in de volumes em uma biblioteca automatizada” na página 179. Se o volume solicitado estiver indisponível, atualize o modo de acesso do volume emitindo o comando **UPDATE VOLUME** e especificando o parâmetro **ACCESS=UNAVAILABLE**. Em seguida, cancele a solicitação de check-in usando o comando **CANCEL REQUEST**. Não cancele o processo do cliente que causou a solicitação. Use o comando **QUERY REQUEST** para obter o ID da solicitação que você deseja cancelar. Se você não responder à solicitação de check-in a partir do servidor dentro do período de espera de montagem especificado para a classe de dispositivo do conjunto de armazenamentos, o servidor marcará o volume como indisponível.
Determinar quais volumes estão montados	Para obter um relatório de todos os volumes que estiverem atualmente montados para uso pelo servidor, emita o comando **QUERY MOUNT**. O relatório mostra quais volumes estão montados, quais unidades os acessaram e se os volumes estão em uso.
Desmontar volumes inativos	Quando um volume está inativo, o servidor o mantém montado durante o tempo especificado pelo parâmetro de retenção de montagem para a classe do dispositivo. O uso de um valor de retenção de montagem pode reduzir o tempo de acesso quando os volumes são usados repetidamente. Para desmontar um volume inativo da unidade na qual está montado, emita o comando **DISMOUNT VOLUME**. Para obter informações sobre como configurar tempos de retenção de montagem, consulte “Controlando a quantia de tempo que um volume permanece montado” na página 125.

Informações relacionadas

QUERY REQUEST (Consultar um ou mais pedidos de montagem pendentes)

Gerenciando unidades de fita

É possível consultar, atualizar e excluir unidades de fita. Também é possível limpar unidades de fita e configurar a criptografia de unidade de fita e os dados de validação.

Atualizando unidades

É possível mudar os atributos de uma definição de unidade para colocar uma unidade off-line ou reconfigurá-la.

Sobre Esta Tarefa

É possível mudar os seguintes atributos de uma unidade:

- O endereço de elemento, se a unidade estiver em um SCSI
- A frequência de limpeza
- O status da unidade: on-line ou off-line

Restrição: Se uma unidade estiver em uso, não será possível mudar o número do elemento ou o nome do dispositivo. Para obter instruções sobre como colocar unidades off-line, consulte “Colocando unidades de fita off-line” na página 195.

Se um volume estiver montado na unidade, mas estiver inativo, ele poderá ser desmontado explicitamente. Para obter instruções sobre como desmontar volumes inativos, consulte “Gerenciando solicitações do servidor para volumes” na página 193.

Procedimento

- Mude o endereço do elemento de uma unidade emitindo o comando **UPDATE DRIVE**.
  Por exemplo, em uma biblioteca que é denominada AUTO, mude o endereço do elemento de DRIVE3 para 119 emitindo o comando a seguir:

```
update drive auto drive3 element=119
```

- Mude o nome do dispositivo de uma unidade emitindo o comando **UPDATE PATH**.
  Por exemplo, para mudar o nome do dispositivo de uma unidade que é denominada DRIVE3, emita o comando a seguir:

AIX
```
update path server1 drive3 srctype=server desttype=drive library=scsilib
device=/dev/rmt0
```

Linux
```
update path server1 drive3 srctype=server desttype=drive library=scsilib
device=/dev/IBMtape0
```

Windows
```
update path server1 drive3 srctype=server desttype=drive library=scsilib
  device=mt3.0.0.0
```

Informações relacionadas

UPDATE DRIVE (Atualizar uma Unidade)

UPDATE PATH (Alterar um caminho)

Colocando unidades de fita off-line

É possível colocar uma unidade de fita off-line enquanto ela estiver em uso. Por exemplo, é possível colocar uma unidade off-line para concluir a manutenção.

Sobre Esta Tarefa

Se mudar o status de uma unidade para off-line enquanto a unidade estiver em uso, o servidor concluirá o processamento da fita que estiver na unidade e, em seguida, interromperá o uso da unidade. No entanto, se a fita que estava em uso fazia parte de uma série de fitas para uma única transação, a unidade estará indisponível para concluir a série. Se nenhuma outra unidade estiver disponível, a transação poderá falhar.

Procedimento

- Para mudar o status de uma unidade, emita o comando **UPDATE DRIVE** e especifique o parâmetro **ONLINE**. Por exemplo, para atualizar a unidade DRIVE3 na biblioteca MANLIB e colocar a unidade off-line, emita o comando a seguir:

  ```
  update drive manlib drive3 online=no
  ```

  Restrição: Não especifique outros parâmetros opcionais ao especificar o parâmetro **ONLINE**. Se fizer isso, a unidade não será atualizada e o comando falhará quando a unidade estiver em uso.

Resultados

Se você atualizar todas as unidades em uma biblioteca para um status off-line, os processos que requerem um ponto de montagem de biblioteca falharão.

O estado atualizado da unidade é retido, mesmo quando o servidor é interrompido e reiniciado. Se uma unidade estiver marcada como off-line quando o servidor for reiniciado, um aviso será emitido informando que a unidade deve ser colocada on-line manualmente.

Informações relacionadas

UPDATE DRIVE (Atualizar uma Unidade)

Validação de Dados Durante Operações de Leitura/Gravação para Fita

Para validar dados e identificar aqueles que estiverem corrompidos, é possível usar um recurso chamado proteção de bloco lógico. Se usar a proteção de bloco lógico, o IBM Spectrum Protect inserirá um valor de verificação de redundância cíclica (CRC) no término de cada bloco lógico de dados enquanto eles são gravados na fita.

Com a proteção de bloco lógico, é possível identificar erros que ocorrem quando os dados são gravados em fita e durante a transferência de dados da unidade de fita para o IBM Spectrum Protect por meio da rede de área de armazenamento. Unidades que suportam proteção de bloco lógico validam dados durante operações de leitura e gravação. O servidor IBM Spectrum Protect valida dados durante operações de leitura.

Se a validação pela unidade falhar durante as operações de gravação, a falha poderá indicar que os dados foram corrompidos durante transferência para fita. Neste caso, o servidor do IBM Spectrum Protect falha a operação de gravação. Você deve reiniciar a operação para continuar. Se a validação pela unidade falhar durante as operações de leitura, a falha poderá indicar que a mídia de fita está corrompida. Se a validação pelo servidor IBM Spectrum Protect falhar durante as operações de leitura, a falha poderá indicar que os dados foram corrompidos durante a transferência da unidade de fita e o servidor tentará executar a operação novamente. Se a validação falhar consistentemente, o servidor IBM Spectrum Protect emitirá uma mensagem de erro que indicará problemas de hardware ou conexão.

Se a proteção de bloco lógico estiver desativada em uma unidade de fita, ou a unidade não suportar proteção de bloco lógico, o servidor IBM Spectrum Protect poderá ler dados protegidos. Porém, os dados não serão validados.

A proteção de bloco lógico é superior à validação de CRC que pode ser especificada ao definir ou atualizar um conjunto de armazenamentos. Ao especificar validação CRC para um conjunto de armazenamentos, os dados são validados somente durante operações de auditoria de volume. Os erros são identificados após os dados serem gravados na fita.

Restrições:

- Não é possível usar proteção de bloco lógico para dados sequenciais como conjuntos de backup e backups de banco de dados.
- A verificação CRC afeta o desempenho porque é necessário um maior uso do processador no cliente e no servidor para calcular e comparar valores CRC.
- Para um volume utilizável, se você especificar a proteção de bloco lógico para operações de leitura/gravação, (**LBPROTECT=READWRITE**), não mude o valor de parâmetro em nenhum momento após a gravação dos dados no volume. A mudança do valor de parâmetro durante a existência do volume no servidor IBM Spectrum Protect não é suportada.

Unidades que Suportam Proteção do Bloco Lógico

A proteção do bloco lógico está disponível apenas para 3592, LTO, e tipos de dispositivo ECARTRIDGE. Unidades 3592 capazes incluem IBM TS1130, TS1140, e gerações mais recentes. As unidades LTO compatíveis incluem as unidades IBM LTO-5 e LTO-6 suportadas. As unidades Oracle StorageTek suportadas incluem unidades com o formato T10000C e T10000D.

A tabela a seguir mostra a mídia e o formato que você pode usar com unidades que suportam proteção de bloco lógico.

Unidade	Mídia de Fita	Formatos de unidade
IBM TS1130	3592 Generation 2	3592-3 e 3592-3C
IBM TS1140	3592 Generation 2 3592 Geração 3	Geração 2: 3592-3 e 3592-3C Geração 3: 3592-4 e 3592-4C
IBM TS1150	3592 Geração 3 3592 Geração 4	Geração 4: 3592-5 e 3592-5C
IBM LTO-5	LTO-5	Ultrium 5 e Ultrium 5C
IBM LTO-6	LTO-6 LTO-5	Ultrium 6 e Ultrium 6C Ultrium 5 e Ultrium 5C
IBM LTO-7	LTO-7 LTO-6	Ultrium 7 e Ultrium 7C Ultrium 6 e Ultrium 6C
Oracle T10000C	Oracle StorageTek T10000 T2	T10000C e T10000C-C
Oracle T10000D	Oracle StorageTek T10000 T2	T10000D e T10000D-C

Dicas:

- Para ativar a proteção de bloco lógico para um volume de fita e, em seguida, reutilizar o volume para o backup de dados, deve-se ativar a proteção de bloco lógico para a classe de dispositivo e a unidade.
- Se você tiver uma unidade 3592, LTO, ou Oracle StorageTek que não seja capaz de proteção de bloco lógico, é possível atualizar a unidade com firmware que forneça proteção de bloco lógico.

A proteção de bloco lógico está disponível para unidades que estão em bibliotecas SCSI . Para obter as informações mais atuais sobre suporte para proteção de bloco lógico, consulte a nota técnica 1568108.

Para usar a proteção de bloco lógico para operações de gravação, todas as unidades na biblioteca deverão suportar proteção de bloco lógico. Se uma unidade não for capaz de proteção de bloco lógico, volumes que têm acesso de leitura/gravação não serão montados. Porém, o servidor pode usar a unidade para montar volumes que tenham acesso de leitura-gravação. Os dados protegidos são lidos e validados pelo servidor IBM Spectrum Protect se a proteção de bloco lógico for ativada para operações de leitura/gravação.

Ativando e Desativando Proteção de Bloco Lógico

É possível especificar proteção de bloco lógico para operações de leitura e gravação, ou somente durante operações de gravação. Também é possível desativar a proteção de bloco lógico. Por padrão, a proteção do bloco lógico está desativada devido a efeitos de desempenho resultantes da validação de verificação de redundância cíclica (CRC) no servidor e na unidade de fita.

Sobre Esta Tarefa

Operações de leitura/gravação para esvaziar ou preencher volumes dependem de se os volumes têm proteção de bloco lógico. Blocos de dados protegidos e desprotegidos não podem ser combinados no mesmo volume. Se você mudar a configuração para proteção de bloco lógico, a mudança se aplicará somente a volumes nulos. Volumes de preenchimento e completos mantêm seus status de proteção de bloco lógico até estarem vazios e prontos para serem preenchidos novamente. Por exemplo, se você desativar a proteção de bloco lógico e o servidor selecionar um volume que estiver associado a uma classe de dispositivo que tenha a proteção de bloco lógico, o servidor continuará gravando dados protegidos no volume.

Restrição: A proteção de bloco lógico está disponível apenas para certos tipos de dispositivo. Para obter informações adicionais, consulte “Unidades que Suportam Proteção do Bloco Lógico” na página 197.

Procedimento

1. Para ativar a proteção do bloco lógico para os tipos de dispositivos 3592, LTO e ECARTRIDGE, emita o comando **DEFINE DEVCLASS** ou **UPDATE DEVCLASS** e especifique o parâmetro **LBPROTECT**.
   Por exemplo, para especificar a proteção de bloco lógico durante operações de leitura e gravação para uma classe de dispositivo 3592 que é denominada 3592_lbprotect, emita o comando a seguir:

   ```
   define devclass 3592_lbprotect library=3594 lbprotect=readwrite
   ```

   Dicas:

   - Se atualizar o valor do parâmetro **LBPROTECT** de NO para READWRITE ou WRITEONLY e o servidor selecionar um volume de preenchimento sem proteção de bloco lógico para as operações de gravação, o servidor emitirá uma mensagem toda vez que o volume for montado. A mensagem indica que os dados são gravados no volume sem a proteção de bloco lógico. Para evitar que essa mensagem seja exibida ou fazer com que o IBM Spectrum Protect grave dados apenas com a proteção de bloco lógico, atualize o acesso de volumes de preenchimento sem proteção de bloco lógico para somente leitura.
   - Para melhorar o desempenho, não especifique o parâmetro **CRCDATA** no comando **DEFINE STGPOOL** ou **UPDATE STGPOOL**.
   - Quando os dados são validados durante as operações de leitura pela unidade e pelo servidor do IBM Spectrum Protect, eles podem diminuir o desempenho do servidor durante as operações de restauração e de recuperação. Para reduzir o tempo que é necessário para as operações de restauração e de recuperação, mude a configuração do parâmetro **LBPROTECT** de READWRITE para WRITEONLY. Após os dados serem restaurados ou recuperados, é possível reconfigurar o parâmetro **LBPROTECT** para READWRITE.

2. Para desativar a proteção de bloco lógico, emita o comando **DEFINE DEVCLASS** ou **UPDATE DEVCLASS** e especifique o parâmetro **LBPROTECT=NO**.

   Restrição: Se a proteção de bloco lógico estiver desativada, o servidor não gravará em uma fita vazia com proteção de bloco lógico. Porém, se um volume de preenchimento com proteção de bloco estiver selecionado, o servidor continuará a gravar no volume com proteção de bloco lógico. Para evitar que o servidor grave em fitas com proteção de bloco lógico, mude o acesso de volumes de preenchimento com proteção de bloco lógico para somente leitura. Quando os dados são lidos, os resultados do CRC não são verificados pela unidade ou pelo servidor.

   Se ocorrer um desastre e o site de recuperação de desastre não tiver unidades que suportem a proteção de bloco lógico, o parâmetro **LBPROTECT=NO** deverá ser especificado. Se as unidades de fita forem usadas para operações de gravação, você deverá mudar o acesso ao volume para volumes com dados protegidos para somente leitura para evitar que o servidor use os volumes.

Se o servidor tiver que ativar a proteção do bloco lógico, o servidor emitirá uma mensagem de erro indicando que a unidade não suporta proteção de bloco lógico.

O que Fazer Depois

Para determinar se um volume possui proteção de bloco lógico, emita o comando **QUERY VOLUME** e revise o valor no campo `Proteção do bloco lógico`.

Informações relacionadas

DEFINE DEVCLASS (Definir uma Classe de Dispositivo)
DEFINE STGPOOL (definir um volume em um conjunto de armazenamentos)
QUERY VOLUME (Consultar volumes do conjunto de armazenamentos)
UPDATE DEVCLASS (atualizar uma classe de dispositivo)
UPDATE STGPOOL (Atualizar um conjunto de armazenamentos)

Operações de Leitura/Gravação para Volumes com Proteção de Bloco Lógico

Operações de leitura/gravação para esvaziar ou preencher volumes dependem de se os volumes têm proteção de bloco lógico. Blocos de dados protegidos e desprotegidos não podem ser combinados no mesmo volume.

Se usar o comando **UPDATE DEVCLASS** para mudar a configuração de proteção de bloco lógico, a mudança será aplicada somente a volumes nulos. Volumes de preenchimento e completos mantêm seus status de proteção de bloco lógico até estarem vazios e prontos para serem preenchidos novamente.

Por exemplo, suponha que você mude o valor do parâmetro **LBPROTECT** de `READWRITE` para `NO`. Se o servidor selecionar um volume que está associado com uma classe de dispositivo e que tem proteção de bloco lógico, o servidor continuará gravando dados protegidos no volume.

Dicas:

- Se uma unidade não suportar proteção de bloco lógico, os volumes com proteção de bloco lógico para operações de gravação não poderão ser montados. Para evitar que o servidor monte volumes protegidos para operações de gravação, mude o acesso do volume para somente leitura. Além disso, desative a proteção de bloco lógico para evitar que o servidor ative o recurso na unidade de fita.
- Se uma unidade não suportar proteção de bloco lógico e a proteção de bloco lógico estiver desativada, o servidor lerá dados de volumes protegidos. Porém, os dados não são validados pelo servidor e a unidade de fita.

Informações relacionadas

QUERY VOLUME (Consultar volumes do conjunto de armazenamentos)
UPDATE DEVCLASS (atualizar uma classe de dispositivo)

Gerenciamento do conjunto de armazenamentos em uma biblioteca de fitas

Para combinar dados protegidos e não protegidos em uma biblioteca, você deve criar classes de dispositivo diferentes e conjuntos de armazenamentos diferentes para separar os dados. Se uma classe de dispositivo estiver associada a dados protegidos, será possível especificar uma proteção de bloco lógico para operações de leitura e gravação ou apenas para operações de gravação.

Para definir classes de dispositivo e conjuntos de armazenamentos para uma biblioteca TS3500 que tem unidades LTO-5, para dados protegidos e desprotegidos, é possível emitir uma série de comandos, conforme mostrado no exemplo a seguir:

```
define library 3584 libtype=scsi
define devclass lbprotect library=3584 devicetype=lto lbprotect=readwrite
define devclass normal library=3584 devicetype=lto lbprotect=no
define stgpool lbprotect_pool lbprotect maxscratch=10
define stgpool normal_pool normal maxscratch=10
```

Informações relacionadas

DEFINE DEVCLASS (Definir uma Classe de Dispositivo)

DEFINE LIBRARY (Definir uma biblioteca)
DEFINE STGPOOL (definir um volume em um conjunto de armazenamentos)

Limpando Unidades de Fita

É possível usar o servidor para gerenciar a limpeza da unidade de fita. O servidor pode controlar como unidades de fita em bibliotecas SCSI são limpas.

Sobre Esta Tarefa

Deve-se ter privilégio no sistema ou privilégio de armazenamento irrestrito para limpeza de unidades de fita. Para bibliotecas automatizadas, é possível automatizar a limpeza especificando a frequência das operações de limpeza e efetuar check-in de um cartucho de limpeza no inventário de volume da biblioteca. O IBM Spectrum Protect monta o cartucho de limpeza, conforme especificado. Haverá considerações especiais, se planejar usar a limpeza da unidade controlada pelo servidor com uma biblioteca SCSI que fornece suporte para limpeza automática da unidade no seu dispositivo de hardware.

Dica: Se uma biblioteca de fitas automatizada suportar a limpeza de unidade da biblioteca, certifique-se de que o recurso esteja ativado.

É possível evitar desgaste prematuro dos cabeçotes de leitura/gravação de unidades usando as funções de limpeza de biblioteca que estiverem disponíveis com seu fabricante do dispositivo.

As unidades e as bibliotecas de fabricantes diferem no modo com que os cartuchos de limpeza são gerenciados e no modo com que a presença de um cartucho de limpeza em uma unidade é relatada. O driver de dispositivo pode não conseguir abrir uma unidade que contém um cartucho de limpeza. Os códigos de detecção e os códigos de erro emitidos pelos dispositivos para limpeza da unidade variam. A limpeza da unidade de biblioteca não é normalmente conhecida para os aplicativos. Portanto, o IBM Spectrum Protect nem sempre pode detectar os cartuchos de limpeza em unidades e podem não ser capazes de determinar quando a limpeza inicia.

Alguns dispositivos requerem um pequeno período de tempo inativo entre os pedidos de montagem para iniciar a limpeza da unidade. No entanto, o IBM Spectrum Protect tenta minimizar o tempo inativo de uma unidade. O resultado poderá ser a impossibilidade de a limpeza da unidade da biblioteca funcionar efetivamente. Se isso acontecer, use o IBM Spectrum Protect para controlar a limpeza da unidade. É possível configurar a frequência para corresponder às recomendações de limpeza do fabricante.

Métodos para limpeza de unidades de fita

Com o tempo, os cabeçotes de leitura das fitas podem ficar sujos, podendo causar falha das operações de leitura e de gravação. Para evitar esses problemas, ative a limpeza de fita. É possível ativar a limpeza de fita na unidade ou no IBM Spectrum Protect.

É possível optar por utilizar o método de limpeza de unidade da biblioteca ou o método de limpeza de unidade do IBM Spectrum Protect, mas não ambos. Algumas bibliotecas SCSI fornecem limpeza automática da unidade. Selecione o método de limpeza de unidade de biblioteca se estiver disponível. Se ele estiver indisponível ou causar problemas, use o IBM Spectrum Protect para controlar a limpeza da unidade da biblioteca.

Método de limpeza de unidade da biblioteca

O método de limpeza de unidade da biblioteca fornece várias vantagens para bibliotecas de fitas automatizadas que usam esta função:

- Reduz a carga para o administrador do IBM Spectrum Protect gerenciar fisicamente a limpeza do cartucho.
- Melhora as taxas de uso do cartucho de limpeza. A maioria das bibliotecas de fitas rastreia o número de vezes em que as unidades podem ser limpas com base nos indicadores de hardware. O IBM Spectrum Protect usa uma contagem bruta.
- Reduz alguma limpeza desnecessária. Unidades de fita modernas não precisam ser limpas em intervalos fixos e podem detectar e solicitar quando a limpeza é necessária.

Os fabricantes que fornecem um método de limpeza de unidade da biblioteca recomendam seu uso para evitar desgaste prematuro dos cabeçotes de leitura/gravação das unidades. As unidades e bibliotecas de vários fabricantes diferem no modo com que os cartuchos de limpeza são gerenciados e no modo com que a presença de um cartucho de limpeza em uma unidade é relatada. O driver de dispositivo pode não conseguir abrir uma unidade que contém um cartucho de limpeza. Os códigos de detecção e os códigos de erro emitidos pelos dispositivos para limpeza da unidade variam. A limpeza da unidade de biblioteca é geralmente transparente para todos os aplicativos. No entanto, o IBM Spectrum Protect nem sempre pode detectar cartuchos de limpeza em unidades e pode não ser capaz de determinar quando a limpeza inicia.

Método de limpeza de unidade do IBM Spectrum Protect

Alguns dispositivos requerem um pequeno período de tempo inativo entre os pedidos de montagem para iniciar a limpeza da unidade. No entanto, o IBM Spectrum Protect tenta minimizar o tempo inativo de uma unidade. O resultado poderá ser a impossibilidade de a limpeza da unidade da biblioteca funcionar efetivamente. Se isso acontecer, tente usar o IBM Spectrum Protect para controlar a limpeza da unidade. Configure a frequência para corresponder às recomendações de limpeza do fabricante.

Se o IBM Spectrum Protect controlar o processo de limpeza, desative a função de limpeza de unidade da biblioteca para evitar problemas. Se a função de limpeza de unidade da biblioteca estiver ativada, alguns dispositivos moverão automaticamente qualquer cartucho de limpeza que for localizado para os slots da biblioteca que estiverem dedicados aos cartuchos de limpeza. Não é possível efetuar check-in de um cartucho de limpeza no inventário de biblioteca do IBM Spectrum Protect até que a função de limpeza de unidade da biblioteca seja desativada.

Para ativar a limpeza da unidade, siga as instruções que são fornecidas pelo fabricante da unidade. Para ativar a limpeza usando o IBM Spectrum Protect, consulte “Configurando o servidor para limpeza da unidade em uma biblioteca automatizada” na página 201.

Configurando o servidor para limpeza da unidade em uma biblioteca automatizada

Ao configurar a limpeza da unidade controlada pelo servidor em uma biblioteca automatizada, é possível especificar a frequência com que deseja que as unidades sejam limpas.

Antes de Iniciar

Determine a frequência com que a unidade deve ser limpa. Esta etapa é necessária para que seja possível especificar um valor apropriado para o parâmetro **CLEANFREQUENCY** no comando **DEFINE DRIVE** ou **UPDATE DRIVE**. Por exemplo, para limpar uma unidade após 100 GB de dados serem processados na unidade, especifique **CLEANFREQUENCY=100**.

Para obter diretrizes sobre a frequência de limpeza, consulte a documentação do fabricante da unidade. Se a documentação fornecer diretrizes para a frequência de limpeza em termos de horas de uso, converta o valor em um valor de gigabyte concluindo as etapas a seguir:

1. Use o valor de bytes por segundo para que a unidade determine um valor de gigabytes por hora.
2. Multiplique o valor de gigabytes por hora pelas horas de uso recomendadas no meio da limpeza.
3. Use o resultado com o valor de limpeza frequente.

É possível especificar um valor para o parâmetro **CLEANFREQUENCY** ou especificar **ASNEEDED** para limpar a unidade conforme necessário.

Restrições:

1. Para unidades IBM 3592, deve-se especificar um valor numérico para o parâmetro **CLEANFREQUENCY**. Usando a frequência de limpeza que é listada na documentação do produto, as unidades não são submetidas a um excesso de limpeza.
2. O valor do parâmetro **CLEANFREQUENCY=ASNEEDED** não funciona para todas as unidades de fita. Para determinar se uma unidade suporta essa função, consulte as informações para seu sistema operacional:

   AIX Windows Dispositivos Suportados para AIX e Windows

Linux Dispositivos Suportados para Linux

Na nota técnica, clique no nome da unidade para visualizar informações detalhadas. Se o valor de ASNEEDED não for suportado, especifique o número de gigabytes.

Procedimento

Defina ou atualize as unidades na biblioteca usando o parâmetro **CLEANFREQUENCY** no comando **DEFINE DRIVE** ou **UPDATE DRIVE**.
Por exemplo, para limpar uma unidade que é denominada DRIVE1 após 100 GB de dados serem processados, emita o comando a seguir:

```
update drive autolib1 drive1 cleanfrequency=100
```

Resultados
Após o cartucho de limpeza ser registrado, o servidor monta o cartucho de limpeza em uma unidade quando a unidade precisa de limpeza. O servidor usa esse cartucho de limpeza para o número de limpezas especificado. Para obter informações adicionais, consulte “Operações com cartuchos de limpeza” na página 152.

O que Fazer Depois
Verifique o cartucho de limpeza no inventário de volume da biblioteca seguindo as instruções em “Efetuando check-in de um cartucho de limpeza em uma biblioteca” na página 202.
Informações relacionadas
DEFINE DRIVE (Definir uma Unidade para uma Biblioteca)
UPDATE DRIVE (Atualizar uma Unidade)

Efetuando check-in de um cartucho de limpeza em uma biblioteca
Para ativar a limpeza automática da unidade de fita, deve-se efetuar check-in de um cartucho de limpeza no inventário de volume da biblioteca automatizada.

Sobre Esta Tarefa

Ao efetuar check-in de um cartucho de limpeza em uma biblioteca, assegure-se de que ele esteja identificado corretamente para o servidor como um cartucho de limpeza. Assegure-se de que um cartucho de limpeza não esteja em um slot que é detectado pelo processo de procura. Erros e atrasos de 15 minutos ou mais podem indicar que um cartucho de limpeza está colocado incorretamente.

O método preferencial é efetuar check-in de cartuchos de limpeza individualmente. Se precisar efetuar check-in de cartuchos de dados e de cartuchos de limpeza, coloque os cartuchos de dados na biblioteca e efetue check-in deles primeiro. Em seguida, efetue check-in do cartucho de limpeza na biblioteca.

Procedimento

Para efetuar check-in de um cartucho de limpeza em uma biblioteca, emita o comando **CHECKIN LIBVOLUME**.
Por exemplo, para efetuar check-in de um cartucho de limpeza que é denominado AUTOLIB1, emita o comando a seguir:

```
checkin libvolume autolib1 cleanv status=cleaner cleanings=10
 checklabel=no
```

O servidor solicita que o cartucho seja colocado na porta de entrada/saída ou em um slot específico.

Informações relacionadas
CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)

Operações com cartuchos de limpeza
Para assegurar que as unidades de fita sejam limpas quando necessário e para evitar problemas com armazenamento em fita, siga estas diretrizes.

Monitorando o processo de limpeza

Se um cartucho de limpeza estiver registrado em uma biblioteca e uma unidade tiver que ser limpa, o servidor desmontará o volume de dados e executará a operação de limpeza. Se a operação de limpeza falhar ou for cancelada ou se nenhum cartucho de limpeza estiver disponível, talvez você não saiba que a unidade precisa de limpeza. Monitore as mensagens de limpeza para esses problemas para assegurar que as unidades sejam limpas, conforme necessário. Se necessário, emita o comando **CLEAN DRIVE** para que o servidor tente a limpeza novamente ou carregue manualmente um cartucho de limpeza na unidade.

Usando múltiplos cartuchos de limpeza

O servidor usa um cartucho de limpeza para o número de limpezas que você especifica ao efetuar check-in do cartucho de limpeza. Se efetuar check-in de dois ou mais cartuchos de limpeza, o servidor usará apenas um dos cartuchos até que o número designado de limpeza para esse cartucho seja atingido. Em seguida, o servidor usa o próximo cartucho de limpeza. Se você efetuar check-in de dois ou mais cartuchos de limpeza e emitir dois ou mais comando **CLEAN DRIVE** simultaneamente, o servidor usará múltiplos cartuchos ao mesmo tempo e diminuirá as limpezas restantes em cada cartucho.

Informações relacionadas

AUDIT LIBRARY (Auditar inventários de volume em uma biblioteca automatizada)

CHECKIN LIBVOLUME (Verificar um volume de armazenamento em uma biblioteca)

CLEAN DRIVE (Limpar uma Unidade)

LABEL LIBVOLUME (Rotular um volume de biblioteca)

QUERY LIBVOLUME (Consultar um volume de biblioteca)

Resolvendo erros que estão relacionados à limpeza da unidade

Ao mover os cartuchos em uma biblioteca, talvez você coloque um cartucho de dados no local em que um cartucho de limpeza deveria estar. Revise o processo que o servidor conclui e as mensagens que são emitidas para que seja possível resolver o problema.

Quando uma unidade precisa de limpeza, o servidor carrega o que o seu banco de dados mostra como um cartucho de limpeza na unidade. Em seguida, a unidade muda para um estado READY e o IBM Spectrum Protect detecta que o cartucho é um cartucho de dados. O servidor conclui as etapas a seguir:

1. O servidor tenta ler o rótulo da fita interno do cartucho de dados.
2. O servidor ejeta o cartucho da unidade e o move de volta ao slot inicial do cartucho de limpeza dentro da biblioteca. Se a operação de ejeção falhar, o servidor marcará a unidade como off-line e emitirá uma mensagem de que o cartucho ainda está na unidade.
3. O servidor efetua o check-out do cartucho de limpeza para evitar que ele seja selecionado por outra solicitação de limpeza da unidade. O cartucho de limpeza permanece na biblioteca, mas não aparece mais no inventário da biblioteca do IBM Spectrum Protect.
4. Usando o rótulo da fita interno, o servidor verifica o nome do volume com relação ao inventário de biblioteca atual, aos volumes do conjunto de armazenamentos e ao arquivo do histórico de volume.
   - Se o nome do volume não for localizado no inventário de biblioteca, um cartucho de dados poderá ser registrado como um cartucho de limpeza por engano. Quando o volume for retirado, não será necessário executar ação adicional.
   - Se o nome do volume for localizado no inventário de biblioteca, o servidor emitirá mensagens que uma intervenção manual e uma auditoria da biblioteca são necessárias. Para resolver o problema, siga as instruções em “Auditando o inventário de volume em uma biblioteca” na página 191.

Substituição da unidade de fita

Se substituir uma unidade em uma biblioteca de fitas que estiver definida para o IBM Spectrum Protect, você deverá excluir as definições de unidade e caminho para a unidade antiga e definir a nova unidade e caminho.

Será necessário substituir as definições de unidade e de caminho mesmo se você estiver trocando uma unidade por outra do mesmo tipo, com o mesmo endereço lógico, endereço físico, ID do SCSI e número da porta. Os nomes de alias de dispositivo poderão mudar quando alterar suas conexões de unidade.

Se a nova unidade for um upgrade que suporta um novo formato de mídia, poderá ser necessário definir uma nova biblioteca lógica, classe de dispositivo e conjunto de armazenamentos. Os procedimentos para configuração de uma política para uma nova unidade em uma biblioteca com múltiplas unidades variam, dependendo dos tipos de unidades e da mídia na biblioteca.

Excluindo unidades de fita

É possível excluir unidades de fita de uma biblioteca. Por exemplo, é possível excluir uma unidade que você não usa mais ou uma unidade que deseja substituir.

Procedimento

1. Pare o servidor IBM Spectrum Protect e encerre o sistema operacional.
2. Remova a unidade antiga e siga as instruções do fabricante para instalar a nova unidade.
3. Reinicie o sistema operacional e o servidor IBM Spectrum Protect.
4. Exclua o caminho do servidor para a unidade.
   Por exemplo, para excluir um caminho de SERVER1 para LIB1, emita o comando a seguir:

   ```
   delete path server1 lib1 srctype=server desttype=drive
   ```

5. Excluir a definição de unidade.
   Por exemplo, emita o comando a seguir para excluir uma unidade denominada DLT1 de um dispositivo de biblioteca denominado LIB1:

   ```
   delete drive lib1 dlt1
   ```

Informações relacionadas

DELETE DRIVE (Excluir uma Unidade de uma Biblioteca)

DELETE PATH (Excluir um caminho)

Substituindo unidades com outras do mesmo tipo

Para incluir uma unidade que suporta os mesmos formatos de mídia que a unidade que a substitui, deve-se definir uma nova unidade e caminho.

Sobre Esta Tarefa

Se uma biblioteca incluir somente um modelo de unidade e você desejar substituir uma unidade, deve substituir a unidade por uma unidade do mesmo modelo. Se uma biblioteca incluir modelos combinados de unidades e você desejar substituir uma unidade, é possível substituí-la por uma unidade de qualquer modelo existente na biblioteca.

Procedimento

1. Exclua as definições de caminho e unidade para a unidade antiga. Por exemplo, para excluir uma unidade que é denominada DRIVE1 de uma biblioteca que é denominada LIB1, insira o comando a seguir:

   ```
   delete path server2 drive1 srctype=server desttype=drive library=lib1
   delete drive lib1 drive1
   ```

2. Desligue a biblioteca, remova a unidade original, substitua-a pela nova unidade e ligue a biblioteca.
3. Atualize o sistema host para assegurar que o sistema detecta a nova unidade.
4. Defina a nova unidade e caminho. Por exemplo, para definir uma nova unidade, DRIVE2, e um caminho para ela de SERVER2, se você estiver usando o driver de dispositivo IBM Spectrum Protect, insira os seguintes comandos:

AIX
```
define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
   device=/dev/mt0
```

Linux
```
define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
   device=/dev/tsmscsi/mt0
```

Windows
```
define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
   device=mt3.0.0.1
```

Dica: É possível usar as definições de sua biblioteca, classe de dispositivo e armazenamento existentes.

Informações relacionadas

DELETE DRIVE (Excluir uma Unidade de uma Biblioteca)

DELETE PATH (Excluir um caminho)

Migrando dados para unidades com upgrade

Se você fizer upgrade de todas as unidades de fita em uma biblioteca, será possível preservar suas definições de política existentes para migrar e expirar dados existentes e também usar as novas unidades para armazenar dados.

Antes de Iniciar

O cenário a seguir supõe que você já possui um conjunto de armazenamentos primário para uma classe de dispositivo DISK que é denominado POOL1.

Procedimento

1. Para migrar dados para um conjunto de armazenamentos que é criado para as novas unidades, especifique o parâmetro **NEXTSTGPOOL**. Por exemplo, para migrar dados de um conjunto de armazenamentos existente, POOL1, para o novo conjunto de armazenamentos, POOL2, emita o comando a seguir:

   ```
   update stgpool pool1 nextstgpool=pool2
   ```

2. Atualize as definições de classe de gerenciamento para armazenar dados no conjunto de armazenamentos DISK usando o comando **UPDATE MGMTCLASS**.

Informações relacionadas

DEFINE STGPOOL (definir um volume em um conjunto de armazenamentos)

UPDATE MGMTCLASS (Atualizar uma classe de gerenciamento)

UPDATE STGPOOL (Atualizar um conjunto de armazenamentos)

Protegendo o servidor do IBM Spectrum Protect

Proteja o servidor do IBM Spectrum Protect e dados controlando o acesso a servidores e nós clientes, criptografando dados e mantendo níveis de acesso e senhas seguros.

Gerenciando administradores

Um administrador que tem autoridade do sistema pode concluir qualquer tarefa com o servidor IBM Spectrum Protect, incluindo designar níveis de autoridade a outros administradores. Para concluir algumas tarefas, deve-se ter recebido autoridade sendo designado a um ou mais níveis de autoridade.

Procedimento

Conclua as seguintes tarefas para modificar as configurações do administrador.

Tarefa	Procedimento

Incluir um administrador.	Para incluir um administrador, ADMIN1, com autoridade do sistema e especificar uma senha, conclua as etapas a seguir:
	a. Registre o administrador e especifique **Pa$# $twO** como a senha emitindo o seguinte comando:
	`register admin admin1 Pa$#$twO`
	b. Conceda autoridade do sistema ao administrador emitindo o seguinte comando:
	`grant authority admin1 classes=system`

Alterar autoridade administrativa.	Altere o nível de autoridade de um administrador, ADMIN1.
	• Conceda autoridade do sistema ao administrador emitindo o seguinte comando:
	`grant authority admin1 classes=system`
	• Revogue a autoridade do sistema para o administrador emitindo o seguinte comando:
	`revogue a autoridade admin1 classes=system`

Remover administradores.	Remova um administrador, ADMIN1, do acesso ao servidor do IBM Spectrum Protect emitindo o seguinte comando: `remove admin admin1`
Impedir temporariamente o acesso ao servidor.	Bloqueie ou desbloqueie um administrador usando o comando **LOCK ADMIN** ou **UNLOCK ADMIN**.

Conceitos relacionados

Planejando funções de administrador
Defina os níveis de autoridade que você deseja designar a administradores que têm acesso à solução do IBM Spectrum Protect.

Alterando requisitos de senha

É possível mudar o limite mínimo de senha, comprimento de senha, expiração de senha e ativar ou desativar a autenticação para o IBM Spectrum Protect.

Sobre Esta Tarefa

Ao aplicar a autenticação de senha e gerenciar restrições de senha, você protege seus dados e seus servidores contra possíveis riscos de segurança.

Procedimento

Conclua as seguintes tarefas para alterar os requisitos de senha para servidores do IBM Spectrum Protect.

Tabela 36. Tarefas de autenticação para servidores do IBM Spectrum Protect

Tarefa	Procedimento
Configurar um limite para tentativas de senha inválida.	a. Na página **Servidores** no Operations Center, selecione o servidor. b. Clique em **Detalhes**, e, em seguida, clique na guia **Propriedades**. c. Configure o número de tentativas inválidas no campo **Limite de tentativas de conexão inválidas**. O valor padrão na instalação é 0.
Configure um comprimento mínimo para senhas.	a. Na página **Servidores** no Operations Center, selecione o servidor. b. Clique em **Detalhes** e, em seguida, clique na guia **Propriedades**. c. Configure o número de caracteres no campo **Comprimento mínimo de senha**.
Configure o período de expiração para senhas.	a. Na página **Servidores** no Operations Center, selecione o servidor. b. Clique em **Detalhes** e, em seguida, clique na guia **Propriedades**. c. Configure o número de dias no campo **Expiração comum de senha**.
Desativar autenticação de senha.	Por padrão, o servidor usa automaticamente a autenticação de senha. Com a autenticação de senha, todos os usuários devem inserir uma senha para acessar o servidor. É possível desativar a autenticação de senha somente para senhas que são autenticadas com o servidor (LOCAL). Desativando a autenticação de senha, aumenta-se o risco de segurança para o servidor.

Configurar um método de autenticação padrão.	Emita o comando **SET DEFAULTAUTHENTICATION**. Por exemplo, para usar o servidor como o método de autenticação padrão, emita o comando a seguir:
	`set defaultauthentication local`
	Para atualizar um nó cliente para ser autenticado com o servidor, inclua AUTHENTICATION=LOCAL no comando **UPDATE NODE**:
	`update node authentication=local`

Protegendo o servidor no sistema

Proteja o sistema em que o servidor do IBM Spectrum Protect é executado para evitar acesso não autorizado.

Procedimento

Certifique-se de que usuários não autorizados não possam acessar os diretórios do banco de dados do servidor e a instância do servidor. Mantenha as configurações de acesso para esses diretórios configurados durante a implementação.

Restringindo o acesso de usuário ao servidor

Os níveis de autoridade determinam o que um administrador pode fazer com o servidor do IBM Spectrum Protect. Um administrador com autoridade do sistema pode concluir qualquer tarefa com o servidor. Os administradores com autoridade de política, de armazenamento ou de operador podem concluir subconjuntos de tarefas.

Procedimento

1. Depois de registrar um administrador usando o comando **REGISTER ADMIN**, use o comando **GRANT AUTHORITY** para configurar o nível de autoridade do administrador.

   Para obter detalhes sobre como configurar e mudar a autoridade, consulte "Gerenciando administradores" na página 205.
2. Para controlar a autoridade de um administrador para concluir algumas tarefas, use as duas seguintes opções do servidor:
   a) É possível selecionar o nível de autoridade que um administrador deve ter para emitir comandos **QUERY** e **SELECT** com a opção do servidor **QUERYAUTH**. Por padrão, o nível de autoridade é obrigatório. É possível alterar o requisito para um dos níveis de autoridade, incluindo o sistema.
   b) É possível especificar que a autoridade do sistema é obrigatória para comandos que fazem o servidor gravar em um arquivo externo com a opção do servidor **REQSYSAUTHOUTFILE**. Por padrão, autoridade do sistema é obrigatória para esses comandos.
3. É possível restringir o backup de dados em um nó de cliente somente a IDs do usuário raiz ou usuários autorizados.
   Por exemplo, para limitar backups ao ID do usuário raiz, emita o comando **REGISTER NODE** ou **UPDATE NODE** e especifique o parâmetro **BACKUPINITIATION=root**:

```
update node backupinitiation=root
```

Parando e iniciando o servidor

Antes de concluir tarefas de manutenção ou reconfiguração, pare o servidor. Em seguida, inicie o servidor no modo de manutenção. Quando concluir as tarefas de manutenção ou reconfiguração, reinicie o servidor no modo de produção.

Antes de Iniciar

Deve-se ter privilégio de sistema ou operador para parar e iniciar o servidor IBM Spectrum Protect.

Parando o Servidor

Antes de parar o servidor, prepare o sistema assegurando que todas as operações de backup de banco de dados sejam concluídas e que todos os outros processos e sessões estejam terminados. Dessa forma, é possível encerrar o servidor com segurança e assegurar que os dados sejam protegidos.

Sobre Esta Tarefa

Ao emitir o comando **HALT** para parar o servidor, ocorrem as seguintes ações:

- Todos os processos e sessões do nó cliente são cancelados.
- Todas as transações atuais são interrompidas. (As transações serão recuperadas quando o servidor for reiniciado.)

Procedimento

Para preparar o sistema e parar o servidor, conclua as etapas a seguir:

1. Evite que novas sessões do nó cliente sejam iniciadas emitindo o comando **DISABLE SESSIONS**:

   ```
   disable sessions all
   ```

2. Determine se os processos ou sessões do nó cliente estão em andamento concluindo as etapas a seguir:

   a. Na página **Visão geral** do Operations Center, visualize a área **Atividade** para o número total de processos e sessões que estão atualmente ativos. Se os números diferirem significativamente dos números comuns que são exibidos durante a rotina diária de gerenciamento de armazenamento, visualize outros indicadores de status no Operations Center para verificar se há um problema.

   b. Visualize o gráfico na área **Atividade** para comparar a quantia de tráfego de rede nos períodos a seguir:

      - O período atual, ou seja, o período mais recente de 24 horas
      - O período anterior, ou seja, as 24 horas antes do período atual

      Se o gráfico para o período anterior representar a quantia esperada de tráfego, as diferenças significativas no gráfico para o período atual poderão indicar um problema.

   c. Na página **Servidores**, selecione um servidor cujos processos e sessões você deseja visualizar e clique em **Detalhes**. Se o servidor não estiver registrado como um servidor do hub ou spoke no Operations Center, obtenha informações sobre processos usando comandos administrativos. Emita o comando **QUERY PROCESS** para os processos de consulta e obtenha informações sobre as sessões emitindo o comando **QUERY SESSION**.

3. Aguarde até que as sessões do nó cliente sejam concluídas ou cancele-as. Para cancelar processos e sessões, conclua as etapas a seguir:

   - Na página **Servidores**, selecione um servidor cujos processos e sessões você deseja visualizar e clique em **Detalhes**.
   - Clique na guia **Tarefas ativas** e selecione um ou mais processos, sessões ou uma combinação de ambos que você deseja cancelar.
   - Clique em **Cancelar**.
   - Se o servidor não estiver registrado como um servidor do hub ou spoke no Operations Center, cancele as sessões usando comandos administrativos. Emita o comando **CANCEL SESSION** para cancelar uma sessão e cancele processos usando o comando **CANCEL PROCESS**.

     Dica: Se o processo que você deseja cancelar estiver aguardando a montagem de um volume da fita, a solicitação de montagem será cancelada. Por exemplo, se você emitir um comando **EXPORT**, **IMPORT** ou **MOVE DATA**, o comando poderá iniciar um processo que requer a montagem de um volume da fita. No entanto, se um volume da fita estiver sendo montado por uma biblioteca automatizada, a operação de cancelamento não poderá entrar em vigor até que o processo de montagem esteja concluído. Dependendo de seu ambiente do sistema, isso pode levar alguns minutos.

4. Pare o servidor emitindo o comando **HALT**:

   ```
   halt
   ```

Iniciando o servidor para tarefas de manutenção ou reconfiguração

Antes de iniciar as tarefas de manutenção ou reconfiguração do servidor, inicie o servidor no modo de manutenção. Ao iniciar o servidor no modo de manutenção, desative as operações que possam interromper suas tarefas de manutenção ou 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, 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. Siga as instruções para o seu sistema operacional:
   - AIX Iniciando a Instância do Servidor
   - Linux Iniciando a Instância do Servidor
   - Windows Iniciando a Instância do Servidor

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

Planejando fazer upgrade do servidor

Quando um fix pack ou correção temporária é disponibilizado, é possível fazer upgrade do servidor IBM Spectrum Protect para aproveitar as melhorias do produto. É possível fazer upgrade de servidores e clientes em momentos diferentes. Certifique-se de concluir as etapas de planejamento antes de fazer upgrade do servidor.

Sobre Esta Tarefa

Siga estas diretrizes:

- O método preferencial é fazer upgrade do servidor usando o assistente de instalação. Depois de iniciar o assistente, na janela **IBM Installation Manager**, clique no ícone **Atualizar**; não clique no ícone **Instalar** ou **Modificar**.
- Se os upgrades estiverem disponíveis para o componente do servidor e o componente Operations Center, selecione as caixas de seleção para fazer upgrade dos dois componentes.

Procedimento

1. Revise a lista de fix packs e de correções temporárias. Consulte IBM Spectrum Protect Downloads - fix packs e correções temporárias mais recentes.
2. Revise as melhorias de produto, que são descritas em arquivos leia-me.

   Dica: Quando obtiver o arquivo de pacote de instalação do Site de suporte do IBM Spectrum Protect, também será possível acessar o arquivo leia-me.
3. Certifique-se de que a versão para a qual você atualizou seu servidor seja compatível com outros componentes, como agentes de armazenamento e clientes de biblioteca. Consulte Compatibilidade do agente de armazenamento e do cliente de biblioteca com um servidor IBM Spectrum Protect .
4. Se sua solução incluir servidores ou clientes em um nível anterior à V7.1, revise as diretrizes para assegurar que as operações de backup e archive do cliente não sejam interrompidas. Consulte Considerações sobre compatibilidade e upgrade do servidor/cliente IBM Spectrum Protect .
5. Revise as instruções de upgrade. Certifique-se de fazer backup do banco de dados do servidor, das informações de configuração do dispositivo e do arquivo do histórico de volume.

O que Fazer Depois

Para instalar um fix pack ou correção temporária, siga as instruções para seu sistema operacional:

- AIX Instalando um fix pack do servidor IBM Spectrum Protect
- Linux Instalando um fix pack do servidor IBM Spectrum Protect
- Windows Instalando um fix pack do servidor IBM Spectrum Protect

Preparando-se para uma indisponibilidade ou atualização do sistema

Prepare o IBM Spectrum Protect para manter seu sistema em um estado consistente durante uma indisponibilidade de energia ou atualização do sistema planejada.

Sobre Esta Tarefa

Certifique-se de planejar atividades regularmente para gerenciar, proteger e manter o servidor. Para obter informações sobre como planejar atividades, como fazer backup do banco de dados, fazer backup do arquivo de configuração de dispositivo e fazer backup do histórico do volume, consulte “Definindo planejamentos para atividades de manutenção de servidor” na página 56.

Procedimento

1. Cancele processos e sessões que estão em andamento concluindo as etapas a seguir:
   a. No Operations Center, na página **Servidores**, selecione um servidor para o qual deseja visualizar processos e sessões e clique em **Detalhes**.
   b. Clique na guia **Tarefas ativas** e selecione um ou mais processos, sessões ou uma combinação de ambos que você deseja cancelar.
   c. Clique em **Cancelar**.
2. Pare o servidor emitindo o comando **HALT**:

```
halt
```

Dica: É possível emitir o comando de parada do Operations Center passando o mouse sobre o ícone **Configurações** e clicando em **Construtor de comando**. Em seguida, selecione o servidor, digite `halt` e pressione **Enter**.

Informações relacionadas

HALT (Encerrar o servidor)

Preparando para um desastre e recuperando-se de um desastre usando o DRM

O IBM Spectrum Protect fornece uma função gerenciador de recuperação de desastre (DRM) para recuperar seus dados do servidor e do cliente durante um desastre.

O DRM rastreia o movimento da mídia externa e registra essas informações no banco de dados do IBM Spectrum Protect. O DRM consolida planos, scripts e outras informações em um arquivo de plano que é necessário para recuperar o servidor do IBM Spectrum Protect quando ocorre um desastre ou uma indisponibilidade não planejada. Se você estiver preocupado com possíveis ataques de malware, incluindo ransomware, considere usar o DRM porque ele pode ajudá-lo a recuperar seus servidores após um ataque.

Restrição: O DRM está disponível apenas no produto IBM Spectrum Protect Extended Edition.

Arquivo de plano de recuperação de desastres

O arquivo de plano de recuperação de desastres contém as informações que são necessárias para recuperar um servidor do IBM Spectrum Protect para o momento em que a última operação de backup do banco de dados foi concluída antes de o plano ser criado.

O plano é organizado em sub-rotinas, que podem ser separadas em múltiplos arquivos. Cada sub-rotina tem uma instrução de início e uma declaração de término.

Tabela 37. Sub-rotinas no arquivo de plano de recuperação de desastres

Sub-rotina	Informações na sub-rotina
SERVER.REQUIREMENTS	Identifica os requisitos de armazenamento do banco de dados e do log de recuperação para o servidor.
RECOVERY.INSTRUCTIONS.GENERAL	Identifica as instruções específicas do site que o administrador insere no arquivo que é identificado pelo prefixo RECOVERY.INSTRUCTIONS.GENERAL. As instruções incluem a estratégia de recuperação, os nomes de contatos chave, uma visão geral dos aplicativos chave que são submetidos a backup por este servidor e outras instruções de recuperação relevantes.
RECOVERY.INSTRUCTIONS.OFFSITE	Contém instruções que o administrador insere no arquivo que é identificado pelo prefixo RECOVERY.INSTRUCTIONS.OFFSITE. As instruções descrevem o nome e o local da área segura externa e como entrar em contato com o administrador da área segura (por exemplo, um nome e um número de telefone).
RECOVERY.INSTRUCTIONS.INSTALL	Contém instruções que o administrador insere no arquivo que é identificado pelo prefixo RECOVERY.INSTRUCTIONS.INSTALL. As instruções descrevem como reconstruir o servidor base e fornecem o local das cópias de backup de imagem do sistema.
RECOVERY.INSTRUCTIONS.DATABASE	Contém instruções que o administrador insere no arquivo que é identificado pelo prefixo RECOVERY.INSTRUCTIONS.DATABASE. As instruções descrevem como preparar para a recuperação do banco de dados. Por exemplo, é possível inserir instruções sobre como inicializar ou carregar os volumes de backup para uma biblioteca automatizada. Nenhuma amostra desta sub-rotina é fornecida.

Tabela 37. Sub-rotinas no arquivo de plano de recuperação de desastres (continuação)

Sub-rotina	Informações na sub-rotina
RECOVERY.INSTRUCTIONS.STGPOOL	Contém instruções que o administrador insere no arquivo que é identificado pelo prefixo RECOVERY.INSTRUCTIONS.STGPOOL. As instruções incluem os nomes de seus aplicativos de software e os nomes do conjunto de armazenamentos de cópia que contêm os backups desses aplicativos. Nenhuma amostra desta sub-rotina é fornecida.
RECOVERY.VOLUMES.REQUIRED	Fornece uma lista de volumes de backup de banco de dados e do conjunto de armazenamentos de cópia que são necessários para recuperar o servidor. Um volume de backup de banco de dados será incluído se ele fizer parte da série de backups de banco de dados mais recente. Um volume do conjunto de armazenamento de cópia será incluído se ele não estiver vazio e não marcado como destruído.
RECOVERY.DEVICES.REQUIRED	Fornece detalhes sobre os dispositivos que são necessários para ler os volumes de backup.
RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE	Contém um script com os comandos que são necessários para recuperar o servidor.
RECOVERY.SCRIPT.NORMAL.MODE	Contém um script com os comandos que são necessários para restaurar os conjuntos de armazenamentos do servidor principal.
DB.STORAGEPATHS	Identifica os diretórios para o banco de dados do IBM Spectrum Protect.
LICENSE.REGISTRATION	Contém uma macro para registrar suas licenças do servidor.
COPYSTGPOOL.VOLUMES.AVAILABLE	Contém uma macro para marcar volumes do conjunto de armazenamentos de cópia que foram movidos externamente e, em seguida, movidos de volta para o local. É possível usar as informações como um guia e emitir os comandos administrativos. Como alternativa, copie, modifique e execute a macro em um arquivo. Esta macro é iniciada pelo script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
COPYSTGPOOL.VOLUMES.DESTROYED	Contém uma macro para marcar volumes do conjunto de armazenamentos de cópia como indisponíveis se os volumes estavam no local no momento do desastre. Estes volumes são considerados externos e não foram destruídos em um desastre. É possível usar as informações como um guia e emitir os comandos administrativos a partir de uma linha de comandos ou copiar, modificar e executar a macro em um arquivo. Esta macro é iniciada pelo script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
PRIMARY.VOLUMES.DESTROYED	Contém uma macro para marcar volumes do conjunto de armazenamentos primário como destruídos se os volumes estavam no local no momento do desastre. É possível usar as informações como um guia e executar os comandos administrativos em uma linha de comandos ou copiar, modificar e executar a macro em um arquivo. Esta macro é iniciada pelo script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
PRIMARY.VOLUMES.REPLACEMENT	Contém uma macro para identificar volumes do conjunto de armazenamentos primário de substituição. É possível usar as informações como um guia e executar os comandos administrativos em uma linha de comandos ou copiar, modificar e executar a macro em um arquivo. Esta macro é iniciada pelo script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
STGPOOLS.RESTORE	Contém uma macro para restaurar os conjuntos de armazenamentos primários. É possível utilizar a sub-rotina como um guia e executar os comandos administrativos em uma linha de comandos. Também é possível copiá-la, modificá-la e executá-la em um arquivo. Esta macro é iniciada pelo script RECOVERY.SCRIPT.NORMAL.MODE.

Tabela 37. Sub-rotinas no arquivo de plano de recuperação de desastres (continuação)	
Sub-rotina	**Informações na sub-rotina**
VOLUME.HISTORY.FILE	Contém uma cópia das informações do histórico de volumes quando o plano de recuperação foi criado. O utilitário **DSMSERV RESTORE DB** usa o arquivo do histórico de volume para determinar quais volumes são necessários para restaurar o banco de dados. O arquivo do histórico de volume é usado pelo script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
DEVICE.CONFIGURATION.FILE	Contém uma cópia das informações de configuração do dispositivo do servidor quando o plano de recuperação foi criado. O utilitário **DSMSERV RESTORE DB** usa o arquivo de configuração do dispositivo para ler os volumes de backup de banco de dados. O arquivo de configuração do dispositivo é usado pelo script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
DSMSERV.OPT.FILE	Contém uma cópia do arquivo de opções do servidor. Esta sub-rotina é usada pelo script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
LICENSE.INFORMATION	Contém uma cópia dos resultados da auditoria de licença e dos termos das licenças do servidor mais recentes.
MACHINE.GENERAL.INFORMATION	Fornece informações para a máquina servidor, como sua localização, que são necessárias para reconstruir a máquina servidor. Esta sub-rotina será incluída no arquivo de plano se as informações da máquina forem salvas no banco de dados usando o comando **DEFINE MACHINE** e especificando o **ADSMSERVER=YES**.
MACHINE.RECOVERY.INSTRUCTIONS	Fornece as instruções de recuperação sobre a máquina servidor. Esta sub-rotina será incluída no arquivo de plano se as instruções de recuperação da máquina forem salvas no banco de dados.
MACHINE.RECOVERY.CHARACTERISTICS	Fornece as características de hardware e software para a máquina servidor. Esta sub-rotina será incluída no arquivo de plano se as características da máquina forem salvas no banco de dados.
MACHINE.RECOVERY.MEDIA	Fornece informações sobre a mídia que são necessárias para reconstruir a máquina que contém o servidor. Esta sub-rotina será incluída no arquivo de plano se as informações da mídia de recuperação forem salvas no banco de dados e estiverem associadas à máquina que contém o servidor.

Recuperando os dados do servidor e do cliente usando o DRM

Use a função gerenciador de recuperação de desastre (DRM) para recuperar os dados do servidor IBM Spectrum Protect e do cliente quando ocorre um desastre.

Antes de Iniciar

O IBM Spectrum Protect é configurado para usar o protocolo Secure Sockets Layer (SSL) para autenticação de cliente/servidor. Ao iniciar o servidor, um arquivo de certificado digital, `cert.kdb`, é criado como parte do processo. Este arquivo inclui a chave pública do servidor, que permite que o cliente criptografe os dados. O arquivo de certificado digital não pode ser armazenado no banco de dados do servidor, porque o Global Security Kit (GSKit) requer um arquivo separado em um determinado formato.

1. Mantenha cópias de backup dos arquivos `cert.kdb`, `cert.sth` e `cert256.arm`.
2. Se os arquivos de certificado originais e quaisquer cópias forem perdidas ou danificadas, gere novos arquivos de certificado.

A chave mestra de criptografia é armazenada em um novo banco de dados de chaves gerenciado por GSKit, `dsmkeydb.kdb`. Se o servidor tiver uma chave mestra de criptografia existente, ela será migrada do arquivo `dsmserv.pwd` para o banco de dados de chaves `dsmkeydb.kdb`. Mantenha cópias de backup dos arquivos `dsmkeydb.kdb` e `dsmkeydb.sth`. É possível configurar o comando **BACKUP DB** para fazer backup da chave mestra de criptografia ou para fazer backup manualmente dos arquivos `dsmkeydb.kdb` e `dsmkeydb.sth`. Não é possível recuperar-se de um desastre sem a chave mestra de criptografia.

1. Mantenha cópias de backup dos arquivos `dsmkeydb.kdb` e `dsmkeydb.sth`.

Procedimento

1. Obtenha o plano de recuperação mais recente.
2. Revise as etapas de recuperação que são descritas na sub-rotina RECOVERY.INSTRUCTIONS.GENERAL do plano.
3. Separe as sub-rotinas do arquivo de plano em arquivos individuais para instruções preliminares gerais, scripts de recuperação do servidor do IBM Spectrum Protect e instrução de recuperação do cliente.
4. Obtenha novamente todos os volumes de recuperação necessários (conforme listado no plano) da área segura.
5. Revise o arquivo de configuração do dispositivo para assegurar que a configuração de hardware no site de recuperação seja a mesma que o site original. Quaisquer diferenças devem ser atualizadas no arquivo de configuração do dispositivo. As seguintes mudanças de configuração de exemplo requerem atualizações nas informações de configuração:
   - Diferentes nomes de dispositivo.
   - Para bibliotecas automatizadas, o requisito de colocar manualmente os volumes de backup de banco de dados na biblioteca automatizada e de atualizar as informações de configuração para identificar o elemento dentro da biblioteca. Isso permite que o servidor localize os volumes de backup de banco de dados necessários.
6. Configure o hardware de substituição para o servidor do IBM Spectrum Protect, incluindo o sistema operacional e a instalação de liberação de base do IBM Spectrum Protect.
7. Execute os scripts de recuperação do servidor do IBM Spectrum Protect no plano de recuperação. As rotinas RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE e RECOVERY.SCRIPT.NORMAL.MODE contêm arquivos de comandos executáveis que podem ser usados para conduzir a recuperação do servidor do IBM Spectrum Protect chamando outros arquivos de comando que foram gerados no plano. O script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE recupera o servidor para o ponto em que os clientes podem iniciar as restaurações diretamente dos volumes do conjunto de armazenamentos de cópia.
8. Restaure os conjuntos de armazenamentos primários usando o script RECOVERY.SCRIPT.NORMAL.MODE.
9. Inicie as operações de restauração do cliente em ordem de prioridade mais alta, conforme definido em seu planejamento de alto nível.

O que Fazer Depois

O servidor IBM Spectrum Protect agora pode ser usado para operações normais do servidor. Certifique-se de que as operações necessárias sejam planejadas. Para obter instruções, consulte “Definindo planejamentos para atividades de manutenção de servidor” na página 56 e Planejando backup e as operações de archive.

Informações relacionadas

PREPARE (Criar um arquivo de plano de recuperação)

Reparando e recuperando dados em conjuntos de armazenamentos de contêiner de diretório

Executando um drill de recuperação de desastre

Planeje drills de recuperação de desastre para preparar-se para auditorias que certificam a recuperabilidade do servidor IBM Spectrum Protect e para assegurar que os dados possam ser restaurados e as operações continuadas após uma indisponibilidade. Um drill também ajuda a assegurar que todos os dados possam ser restaurados e as operações continuadas antes de ocorrer uma situação crítica.

Antes de Iniciar

Execute as seguintes tarefas:

- Planeje atividades regularmente para gerenciar, proteger e manter o servidor. Para obter informações adicionais sobre como planejar atividades, consulte “Definindo planejamentos para atividades de manutenção de servidor” na página 56. Certifique-se de planejar as seguintes tarefas:
  - Fazer backup do banco de dados.
  - Mover mídia externa.
  - Fazer backup do arquivo de configuração de dispositivo, do arquivo do histórico de volume e do arquivo de opções do servidor `dsmserv.opt`.
  - **Opcional:** emitindo o comando **PREPARE** para criar o arquivo de plano de recuperação de desastres.

  Dica:

  Ao emitir o comando **PREPARE**, a função do IBM Spectrum Protectgerenciador de recuperação de desastre (DRM) cria uma cópia do arquivo de plano de recuperação de desastres.

  É possível gerenciar a recuperação de desastre externa sem usar o DRM, no entanto, o DRM ajuda a consolidar planos, scripts e outras informações que são necessárias durante a recuperação de desastre.

  Crie várias cópias do plano para segurança. Por exemplo, mantenha cópias impressas, em uma unidade flash USB, no espaço em disco localizado externamente ou em um servidor remoto. O arquivo de plano de recuperação de desastres é movido externamente todos os dias com as fitas. Para obter mais informações sobre o DRM, consulte “Preparando para um desastre e recuperando-se de um desastre usando o DRM” na página 212.
- Configure os seguintes recursos no site de recuperação de desastre:
  1. Um servidor IBM Spectrum Protect de recuperação. O servidor no site de recuperação de desastre deve estar no mesmo nível que o servidor no site de produção.
  2. Uma biblioteca de fitas para armazenar a mídia que é fornecida no site de produção. Para obter informações adicionais sobre locais de recuperação externos, consulte “Armazenamento de dados externo” na página 24.
  3. Espaço de armazenamento em disco para o banco de dados, o log de archive, logs ativos e conjuntos de armazenamentos.
  4. Clientes para testar operações de restauração.

Sobre Esta Tarefa

Teste o plano de recuperação de desastres e a recuperabilidade do servidor IBM Spectrum Protect com frequência, em um ambiente que seja semelhante ao ambiente de produção.

Procedimento

1. Certifique-se de que as fitas estejam disponíveis no local. Emita o comando **QUERY LIBVOLUME** para identificar volumes que são verificados em uma biblioteca automatizada.
2. Faça backup do banco de dados para as fitas no local concluindo as seguintes etapas:
   a. Na página **Servidores** do Operations Center, selecione o servidor de cujo banco de dados deseja fazer backup.
   b. Clique em **Fazer backup** e siga as instruções na janela **Fazer backup do banco de dados**.
3. Copie os seguintes arquivos para o diretório inicial do servidor no site de recuperação:
   - Arquivo de plano de recuperação de desastres
   - Arquivo de Histórico de Volumes
   - Arquivo de Configuração de Dispositivo
   - Opcional: Arquivo de opções do servidor `dsmserv.opt`
4. Mova a fita para o local de recuperação externo.

5. Restaure o banco de dados do servidor usando o utilitário **DSMSERV RESTORE DB** no servidor de recuperação.
6. Emita o comando **UPDATE VOLUME** e especifique o parâmetro **ACCESS=DESTROYED** para indicar que um volume inteiro deve ser restaurado.
7. No servidor de recuperação, restaure os volumes do conjunto de armazenamentos usando o comando **RESTORE STGPOOL**.

O que Fazer Depois

Certifique-se de que possa acessar os dados na biblioteca auditando um volume da fita no conjunto de armazenamentos restaurados para verificar se os dados estão consistentes. Emita o comando **AUDIT VOLUME** para auditar um volume de fita. Para desempenho mais rápido, audite somente os dados restaurados.

Tarefas relacionadas

Auditando o inventário de volume em uma biblioteca

É possível auditar uma biblioteca automatizada para assegurar que o inventário do volume de biblioteca seja consistente com os volumes que estão fisicamente na biblioteca. Talvez você deseja auditar uma biblioteca se o inventário de volume da biblioteca estiver distorcido devido ao movimento manual de volumes na biblioteca ou a problemas do banco de dados.

Informações relacionadas

AUDIT VOLUME (Verificar informações do banco de dados para um volume do conjunto de armazenamento)

DSMSERV RESTORE DB (Restaurar o banco de dados)

RESTORE STGPOOL (Restaurar dados do conjunto de armazenamentos)

Restaurando o banco de dados

Se você tiver a função do gerenciador de recuperação de desastre (DRM) ativada e tiver seguido o procedimento para preparar-se para um desastre, é possível restaurar o banco de dados após um desastre. Se não tiver o DRM configurado, ainda é possível restaurar o banco de dados, desde que tenha os arquivos de backup necessários.

Antes de Iniciar

Se os diretórios de log do banco de dados e de recuperação forem perdidos, recrie-os antes de executar o utilitário do servidor **DSMSERV RESTORE DB**.

Sobre Esta Tarefa

É possível restaurar o banco de dados para seu estado mais recente ou para um momento especificado. Para recuperar o banco de dados para o momento em que ele foi perdido, recupere o banco de dados para sua versão mais recente.

Restrições:

- Para restaurar o banco de dados para sua versão mais recente, deve-se localizar o diretório de log de archive. Se você não conseguir localizar o diretório, será possível restaurar o banco de dados apenas para um momento.
- Não é possível usar o protocolo Secure Sockets Layer (SSL) para operações de restauração do banco de dados.
- Se o nível da liberação do backup de banco de dados for diferente do nível da liberação do servidor que está sendo restaurado, não será possível restaurar o banco de dados do servidor. Por exemplo, ocorrerá um erro se estiver usando um servidor Versão 8.1 e tentar restaurar um banco de dados V7.1.

Procedimento

Use o utilitário do servidor **DSMSERV RESTORE DB** para restaurar o banco de dados. Dependendo da versão do banco de dados que você deseja restaurar, escolha um dos métodos a seguir:

- Restaurar um banco de dados para sua versão mais recente. Por exemplo, use o seguinte comando:

```
dsmserv restore db
```

- Restaurar um banco de dados para um momento. Por exemplo, para restaurar o banco de dados para uma série de backup que foi criada em 19 de abril de 2017, use o seguinte comando:

```
dsmserv restore db todate=04/19/2017
```

Informações relacionadas

DSMSERV RESTORE DB (Restaurar o banco de dados)

Apêndice A. 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 de 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. _insira 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.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

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.

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 de VMware, Inc. ou suas subsidiárias nos Estados Unidos e/ou em outros países.

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

Caracteres Especiais

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

Número do Programa: 5725-W98
5725-W99
5725-X15