

IBM Spectrum Protect  
Versão 8.1.7

*Introdução a Soluções de Proteção de  
Dados*





IBM Spectrum Protect  
Versão 8.1.7

*Introdução a Soluções de Proteção de  
Dados*



**Observação:**

Antes de utilizar essas informações e o produto que elas suportam, leia as informações em “Aviso” na página 61.

Essa edição se aplica à versão 8, liberação 1, modificação 7 do IBM Spectrum Protect (números de produto 5725-W98, 5725-W99, 5725-X15) e a todas as liberações e modificações subsequentes, até que seja indicado de outra forma em novas edições.

© Copyright IBM Corporation 1993, 2019.

---

# Índice

<b>Sobre esta publicação</b> . . . . .	<b>v</b>
Quem Deve Ler este Guia . . . . .	v
Publicações . . . . .	v

---

## Parte 1. Conceitos do IBM Spectrum Protect . . . . . 1

<b>Capítulo 1. Visão geral do IBM Spectrum Protect</b> . . . . .	<b>3</b>
Componentes de proteção de dados . . . . .	3
Serviços de proteção de dados . . . . .	5
Processos para gerenciar a proteção de dados com o IBM Spectrum Protect . . . . .	7
Interfaces com o usuário para o ambiente do IBM Spectrum Protect . . . . .	11

<b>Capítulo 2. Conceitos de armazenamento de dados no IBM Spectrum Protect</b> . . . . .	<b>15</b>
Tipos de dispositivos de armazenamento . . . . .	15
Armazenamento de dados em conjuntos de armazenamentos. . . . .	20
Transporte de dados para armazenamento em redes . . . . .	27

<b>Capítulo 3. Estratégias de proteção de dados com o IBM Spectrum Protect</b> . . . . .	<b>33</b>
Estratégias para minimizar o uso do espaço de armazenamento para backups . . . . .	33
Estratégias para proteção de desastre. . . . .	35
Estratégias para recuperação de desastre com o IBM Spectrum Protect . . . . .	40

---

## Parte 2. Soluções do IBM Spectrum Protect para proteção de dados . . . 43

<b>Capítulo 4. Implementação baseada em disco de uma solução de proteção de dados para um site único</b> . . . . .	<b>45</b>
--------------------------------------------------------------------------------------------------------------------	-----------

<b>Capítulo 5. Implementação baseada em disco de uma solução de proteção de dados para vários sites</b> . . . . .	<b>47</b>
-------------------------------------------------------------------------------------------------------------------	-----------

<b>Capítulo 6. Implementação baseada em fita de uma solução de proteção de dados</b> . . . . .	<b>49</b>
------------------------------------------------------------------------------------------------	-----------

<b>Capítulo 7. Implementação baseada em dispositivo de uma solução de proteção de dados para vários sites</b> . . . . .	<b>51</b>
-------------------------------------------------------------------------------------------------------------------------	-----------

<b>Capítulo 8. Comparação de soluções de proteção de dados</b> . . . . .	<b>53</b>
--------------------------------------------------------------------------	-----------

<b>Capítulo 9. Roteiro para implementar uma solução de proteção de dados</b> . . . . .	<b>55</b>
----------------------------------------------------------------------------------------	-----------

---

## Parte 3. Apêndices. . . . . 57

<b>Apêndice. Recursos de Acessibilidade para a Família de Produtos IBM Spectrum Protect</b> . . . . .	<b>59</b>
-------------------------------------------------------------------------------------------------------	-----------

<b>Aviso</b> . . . . .	<b>61</b>
------------------------	-----------

<b>Glossário</b> . . . . .	<b>67</b>
----------------------------	-----------

<b>Índice Remissivo</b> . . . . .	<b>69</b>
-----------------------------------	-----------



---

## Sobre esta publicação

Esta publicação fornece uma visão geral de conceitos e soluções de proteção de dados da IBM Spectrum Protect que usam as melhores práticas para o IBM Spectrum Protect. Um gráfico de comparação de recursos ajuda a selecionar a melhor solução para as necessidades de sua organização.

---

## Quem Deve Ler este Guia

Esse guia é 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.

Você deve estar familiarizado com o sistema operacional no qual o servidor reside e os protocolos de comunicação necessários para o ambiente do cliente/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, IBM Spectrum Protect for Virtual Environments, 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.





---

## **Parte 1. Conceitos do IBM Spectrum Protect**

O IBM Spectrum Protect fornece um ambiente de proteção de dados abrangente.



---

## Capítulo 1. Visão geral do IBM Spectrum Protect

O IBM Spectrum Protect fornece proteção de dados centralizada, automatizada que ajuda a reduzir a perda de dados e gerenciar a conformidade com requisitos de retenção de dados e de disponibilidade.

---

### Componentes de proteção de dados

As soluções de proteção de dados que o IBM Spectrum Protect fornece consistem em um servidor, sistemas e aplicativos do cliente e mídia de armazenamento. O IBM Spectrum Protect fornece interfaces de gerenciamento para monitorar e relatar o status de proteção de dados.

#### Servidor

Os sistemas do cliente enviam dados ao servidor para serem armazenados como backups ou dados arquivados. O servidor inclui um *inventário*, que é um repositório de informações sobre dados de cliente.

O inventário inclui os seguintes componentes:

##### Banco de Dados

As informações sobre cada arquivo, volume lógico ou banco de dados que o servidor faz backup, arquiva ou migra estão armazenadas no banco de dados do servidor. O banco de dados do servidor também contém informações sobre a política e planejamentos para serviços de proteção de dados.

##### Log de recuperação

Os registros de transações do banco de dados são mantidos neste log. O banco de dados usa o log de recuperação para assegurar a consistência de dados no banco de dados.

#### Sistemas e aplicativos do cliente

*Clientes* são aplicativos, máquinas virtuais e sistemas que devem ser protegidos. Os clientes enviam dados para o servidor, conforme mostrado na Figura 1 na página 4.

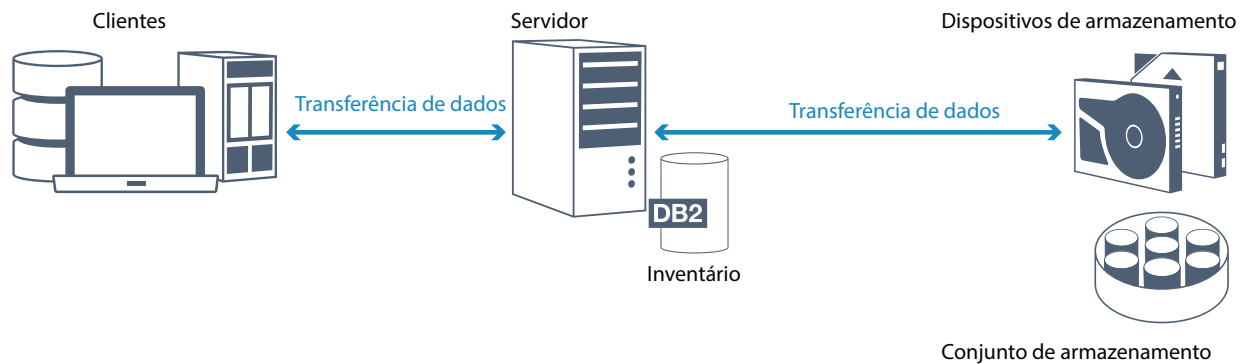


Figura 1. Componentes na solução de proteção de dados

### Software cliente

Para o IBM Spectrum Protect proteger dados de cliente, o software apropriado deve ser instalado no sistema do cliente e o cliente deve ser registrado com o servidor.

### Nós clientes

Um *nó cliente* é equivalente a um computador, máquina virtual ou aplicativo, como um cliente de backup-archive que está instalado em uma estação de trabalho para backups do sistema de arquivos. Cada nó cliente deve ser registrado com o servidor. Vários nós podem ser registrados em um único computador.

## Mídia de armazenamento

O servidor armazena dados do cliente na mídia de armazenamento. Os tipos de mídia a seguir são usados:

### Dispositivos de armazenamento

O servidor pode gravar dados em unidades de disco rígido, matrizes e subsistemas de disco, unidades de fita independentes, bibliotecas de fitas e outros tipos de armazenamento de acesso aleatório e de acesso sequencial. Os dispositivos de armazenamento podem ser conectados diretamente ao servidor ou conectados por meio de uma rede local (LAN) ou de uma rede de área de armazenamento (SAN).

### Conjuntos de armazenamentos

Os dispositivos de armazenamento que estão conectados ao servidor são agrupados em *conjuntos de armazenamentos*. Cada conjunto de armazenamentos representa um conjunto de dispositivos de armazenamento do mesmo tipo de mídia, como unidades de disco ou de fita. O IBM Spectrum Protect armazena todos os dados de cliente em conjuntos de armazenamentos. É possível organizar conjuntos de armazenamentos em uma *hierarquia*, para que o armazenamento de dados possa transferir do armazenamento em disco para um armazenamento de custo mais baixo, como dispositivos de fita.

## Serviços de proteção de dados

O IBM Spectrum Protect fornece serviços de proteção de dados para armazenar e recuperar dados a partir de vários tipos de clientes. Os serviços de proteção de dados são implementados por meio de políticas que estão definidas no servidor. É possível usar o planejamento de cliente para automatizar os serviços de proteção de dados.

### Tipos de serviços de proteção de dados

O IBM Spectrum Protect fornece serviços para armazenar e recuperar dados de cliente, conforme mostrado na Figura 2.

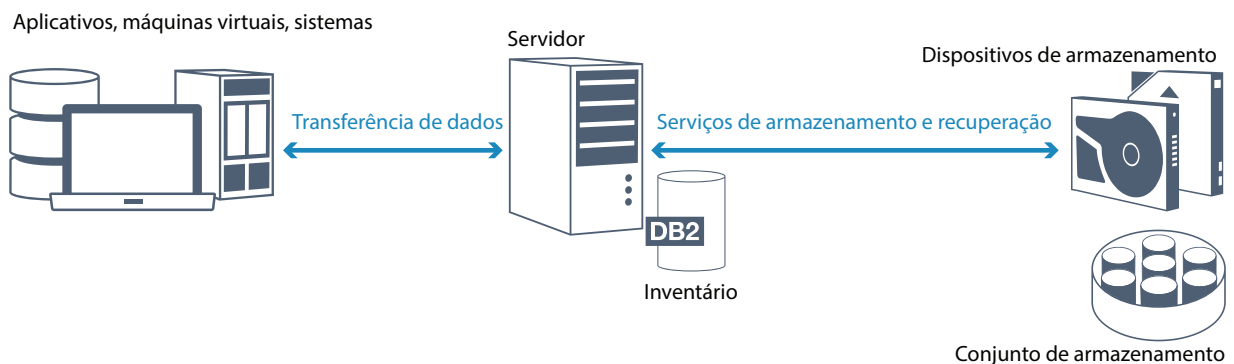


Figura 2. Serviços de proteção de dados

O IBM Spectrum Protect fornece os seguintes tipos de serviços de proteção de dados:

#### Serviços de backup e restauração

Você executa um processo de backup para criar uma cópia de um *objeto de dados* que pode ser usada para recuperação se o objeto de dados original for perdido. Um objeto de dados pode ser um arquivo, um diretório ou um objeto de dados definido pelo usuário, como um banco de dados.

Para reduzir o uso de recursos do sistema durante a operação de backup, o IBM Spectrum Protect usa o método de *backup incremental progressivo*. Para esse método de backup, um primeiro backup completo de todos os objetos de dados é criado e, em operações de backup subsequentes, apenas os dados alterados são movidos para armazenamento. Em comparação com métodos de backup incremental e diferenciado que requerem a execução de backups completos periódicos, o método de backup incremental progressivo fornece os seguintes benefícios:

- Reduz a redundância de dados
- Usa menos largura da banda da rede
- Requer menos espaço do conjunto de armazenamentos

Para reduzir ainda mais os requisitos de capacidade de armazenamento e o uso de largura da banda da rede, o IBM Spectrum Protect inclui *deduplicação de dados* para backups de dados. A técnica de deduplicação de dados remove extensões de dados duplicadas de backups.

Você executa um processo de restauração para copiar um objeto de um conjunto de armazenamentos para o cliente. É possível restaurar um único arquivo, todos os arquivos em um diretório ou todos os dados em um computador.

### Serviços de archive e recuperação

Use o serviço de archive para preservar dados que devem ser armazenados por um longo tempo, por exemplo, para conformidade regulamentar. O serviço de archive fornece os seguintes recursos:

- Ao arquivar dados, especifique por quanto tempo os dados devem ser armazenados.
- É possível solicitar que arquivos e diretórios sejam copiados para armazenamento de longo prazo em mídia. Por exemplo, é possível optar por armazenar esses dados em um dispositivo de fita, que pode reduzir o custo de armazenamento.
- É possível especificar que os arquivos originais sejam apagados do cliente após os arquivos serem arquivados.

O serviço de recuperação fornece os seguintes recursos:

- Ao recuperar dados, os dados são copiados de um conjunto de armazenamentos para um nó cliente.
- A operação de recuperação não afeta a cópia de archive no conjunto de armazenamentos.

### Serviços de migração e rechamada

Use serviços de migração e rechamada para gerenciar o espaço em sistemas do cliente. O objetivo do gerenciamento de espaço é aumentar a capacidade da mídia disponível para novos dados e reduzir o tempo de acesso aos dados. É possível migrar dados para armazenamento do servidor para manter espaço de armazenamento livre suficiente em um sistema de arquivos local. É possível armazenar dados migrados nas maneiras a seguir:

- Em armazenamento em disco para armazenamento de longo prazo
- Em uma *biblioteca de fitas virtual* (VTL) para rechamada rápida de arquivos

É possível rechamar arquivos para o nó cliente sob demanda, automática ou seletivamente.

## Tipos de dados de cliente que podem ser protegidos

É possível proteger os dados para os seguintes tipos de clientes com o IBM Spectrum Protect:

### Aplicativos clientes

O IBM Spectrum Protect pode proteger dados para produtos ou aplicativos específicos. Esses clientes são chamados *aplicativos clientes*. Para proteger os *dados estruturados* para esses clientes, em outras palavras, os dados em campos do banco de dados, deve-se fazer backup de componentes que são específicos do aplicativo. O IBM Spectrum Protect pode proteger os seguintes aplicativos:

- Clientes do IBM Spectrum Protect for Enterprise Resource Planning:
  - Data Protection for SAP HANA
  - Data Protection for SAP for Db2
  - Data Protection for SAP for Oracle

- Clientes do IBM Spectrum Protect for Databases:
  - Data Protection for Microsoft SQL server
  - Data Protection para Oracle
- Clientes do IBM Spectrum Protect for Mail:
  - Data Protection for IBM Domino
  - Data Protection for Microsoft Exchange Server

#### **Máquinas virtuais**

Máquinas virtuais que são submetidas a backup usando o software do aplicativo cliente que está instalado na máquina virtual. No ambiente do IBM Spectrum Protect, uma máquina virtual pode ser protegida pelo IBM Spectrum Protect for Virtual Environments.

#### **Clientes do sistema**

Os clientes do IBM Spectrum Protect a seguir são chamados de *clientes do sistema*:

- Todos os clientes que fazem backup de dados em arquivos e diretórios, em outras palavras, *dados não estruturados*, como clientes de backup-archive e clientes da API que estão instalados em estações de trabalho.
- Um servidor que está incluído em uma configuração de volume virtual de servidor para servidor.
- Uma máquina virtual que é submetida a backup usando o software do cliente de backup-archive que está instalado na máquina virtual.

---

## **Processos para gerenciar a proteção de dados com o IBM Spectrum Protect**

O inventário do servidor IBM Spectrum Protect tem uma função-chave nos processos de proteção de dados. Você define políticas que o servidor usa para gerenciar o armazenamento de dados.

### **Processo de gerenciamento de dados**

A Figura 3 na página 8 mostra o processo de gerenciamento de dados do IBM Spectrum Protect.

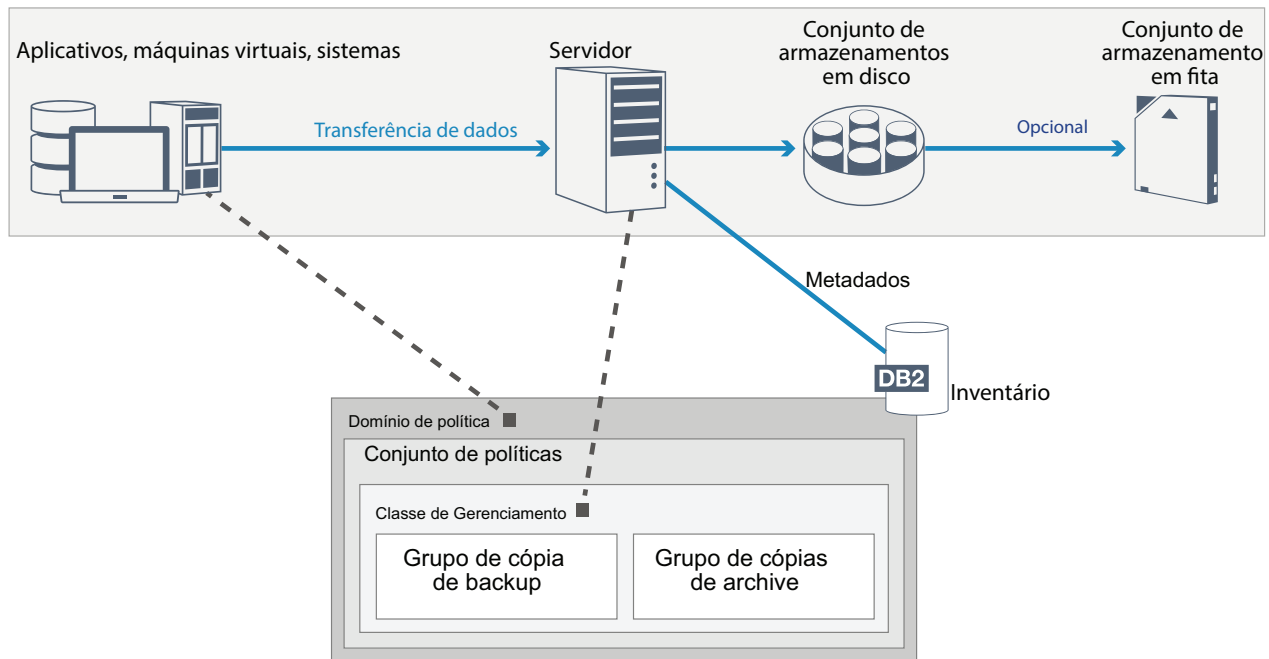


Figura 3. Processo de gerenciamento de dados

O IBM Spectrum Protect usa políticas para controlar como o servidor armazena e gerencia objetos de dados em vários tipos de dispositivos de armazenamento e de mídia. Você associa um cliente a um domínio de política que contém um conjunto de políticas ativas. Quando um cliente faz backup, arquiva ou migra um arquivo, o arquivo é ligado a uma classe de gerenciamento no conjunto de políticas ativas do domínio de política. A classe de gerenciamento e os grupos de cópias de backup e archive especificam onde os arquivos são armazenados e como eles são gerenciados. Se você configurar o armazenamento do servidor em uma hierarquia, será possível migrar os arquivos para diferentes conjuntos de armazenamentos.

## Componentes de inventário

Os componentes de inventário a seguir são chave para a operação do servidor:

### Banco de dados do servidor

O banco de dados do servidor contém informações sobre dados de cliente e operações do servidor. O banco de dados armazena informações sobre dados de cliente, chamados *metadados*. As informações sobre dados de cliente incluem o nome do arquivo, tamanho do arquivo, proprietário do arquivo, classe de gerenciamento, grupo de cópias e local do arquivo no armazenamento do servidor. O banco de dados inclui as informações a seguir necessárias para a operação do servidor:

- Definições de nós clientes e administradores
- Políticas e planejamentos
- Configurações do servidor
- Registros de operações do servidor, como logs de atividades e registros de eventos
- Resultados intermediários para consultas administrativas

### Log de recuperação

O servidor registra transações do banco de dados no log de recuperação. O log de recuperação ajuda a assegurar que uma falha não deixe o banco de



dados em um estado inconsistente. O log de recuperação também é usado para manter a consistência em operações de início do servidor. O log de recuperação consiste nos seguintes logs:

#### **Log ativo**

Este log registra transações atuais no servidor. Estas informações são necessárias para iniciar o servidor e o banco de dados após um desastre.

#### **Espelho de log (opcional)**

O espelho de log ativo é uma cópia do log ativo que pode ser usado se os arquivos de log ativo não puderem ser lidos. Todas as mudanças feitas no log ativo também são gravadas em um espelho de log. É possível configurar um espelho de log ativo.

#### **Log de archive**

O log de archive contém cópias de arquivos de log fechados que estavam no log ativo. O log de archive está incluído nos backups de banco de dados e é usado para recuperação do banco de dados do servidor. Os arquivos de log de archive que estão incluídos em um backup de banco de dados são automaticamente removidos após a conclusão de um ciclo de backup de banco de dados. O log de archive deve ter espaço suficiente para armazenar os arquivos de log para backups de banco de dados.

#### **Log de failover de archive (opcional)**

O log de failover de archive, também chamado de log de archive secundário, é o diretório que o servidor usa para armazenar arquivos de log de archive quando o diretório de log de archive está cheio.

## **Gerenciamento de dados baseado em política**

No ambiente do IBM Spectrum Protect, uma *política* para gerenciamento de proteção de dados contém regras que determinam como os dados de cliente são armazenados e gerenciados. O propósito primário de uma política é implementar os objetivos de gerenciamento de dados a seguir:

- Controle em qual cliente do conjunto de armazenamentos os dados são inicialmente armazenados
- Defina critérios de retenção que controlem quantas cópias de objetos são armazenadas
- Defina por quanto tempo as cópias de objetos são retidas

O gerenciamento de dados baseado em política ajuda a se concentrar nas necessidades de negócios para proteger dados em vez de gerenciar dispositivos de armazenamento e mídia. Os administradores definem políticas e designam nós clientes a um *domínio de política*.

Dependendo de suas necessidades de negócios, é possível ter uma ou muitas políticas. Em uma organização de negócios, por exemplo, diferentes departamentos com diferentes tipos de dados podem ter planos de gerenciamento de armazenamento customizados. As políticas podem ser atualizadas e as atualizações podem ser aplicadas a dados que já são gerenciados.

Ao instalar o IBM Spectrum Protect, uma política padrão chamada STANDARD já está definida. O política STANDARD fornece proteção básica de backup para

estações de trabalho do usuário. Para fornecer diferentes níveis de serviço para diferentes clientes, é possível incluir na política padrão ou criar uma nova política.

Você cria políticas definindo os seguintes componentes de política:

#### **Domínio de política**

O domínio de política é o principal método organizacional de agrupar nós clientes que compartilham regras comuns para gerenciamento de dados. Embora um nó cliente possa ser definido para mais de um servidor, o nó cliente pode ser definido para somente um domínio de política em cada servidor.

#### **Conjunto de políticas**

Um *conjunto de políticas* são várias políticas que são agrupadas para que a política para os nós clientes no domínio possa ser ativada ou desativada conforme necessário. Um administrador usa um conjunto de políticas para implementar diferentes classes de gerenciamento com base nas necessidades de negócios e do usuário. Um domínio de política pode conter vários conjuntos de políticas, mas apenas um conjunto de políticas pode estar ativo no domínio. Cada conjunto de políticas contém uma classe de gerenciamento padrão e qualquer número de classes de gerenciamento extras.

#### **Classe de gerenciamento**

Uma *classe de gerenciamento* é um objeto de política que pode ser ligado a cada categoria de dados para especificar como o servidor gerencia os dados. Pode haver uma ou mais classes de gerenciamento. Uma classe de gerenciamento é designada para ser a classe de gerenciamento padrão que é usada por clientes, a menos que eles substituam especificamente o padrão para usar uma classe de gerenciamento específica.

A classe de gerenciamento pode conter um grupo de cópia de backup, um grupo de cópias de archive e atributos de gerenciamento de espaço. Um grupo de cópias determina como o servidor gerencia versões de backup ou cópias arquivadas do arquivo. Os atributos de gerenciamento de espaço determinam se o arquivo é elegível para migração pelo cliente do gerenciador de espaço para armazenamento do servidor, e em quais condições o arquivo é migrado.

#### **Grupo de cópias**

Um *grupo de cópias* é um conjunto de atributos em uma classe de gerenciamento que controla os seguintes fatores:

- Onde o servidor armazena versões de arquivos de backup ou cópias de archive
- Por quanto tempo o servidor mantém versões de arquivos de backup ou cópias de archive
- Quantas versões de cópias de backup são retidas
- Qual método usar para gerar versões de arquivos de backup ou cópias de archive

### **Gerenciamento da segurança**

O IBM Spectrum Protect inclui recursos de segurança para registro de administradores e usuários. Após os administradores se registrarem, eles devem receber autoridade sendo designados a uma ou mais classes de privilégio administrativo. Um administrador com privilégio do sistema pode executar qualquer função do servidor. Os administradores com privilégios de política,

armazenamento, operador ou de nó podem executar subconjuntos de funções do servidor. O servidor pode ser acessado usando os métodos a seguir, cada um controlado com uma senha:

- Acesso de administrador para gerenciar o servidor
- Acesso de cliente a nós para armazenar e recuperar dados

Também estão incluídos recursos que podem ajudar a garantir segurança quando clientes se conectam ao servidor. Dependendo de necessidades de negócios, como um administrador, você pode escolher um dos métodos de registro de cliente a seguir:

#### **Registro aberto**

Quando o cliente se conecta primeiro ao servidor, é solicitado que o usuário forneça um nome do nó, senha e informações de contato. O registro aberto fornece ao usuário as seguintes configurações padrão:

- O nó cliente é designado ao domínio de política STANDARD.
- O usuário pode definir se os arquivos serão compactados para reduzir a quantidade de dados enviados por redes e o espaço ocupado pelos dados em armazenamento.
- O usuário pode excluir cópias arquivadas de arquivos do armazenamento do servidor, mas não versões de backup de arquivos.

#### **Registro fechado**

Registro fechado é o método padrão para registro de cliente no servidor. Para esse tipo de registro, um administrador registra todos os clientes. O administrador pode implementar as configurações a seguir:

- Designar o nó a qualquer domínio de política
- Determinar se o usuário pode usar compactação ou não, ou se o usuário pode escolher
- Controlar se o usuário pode excluir arquivos de backup ou arquivos arquivados

É possível incluir mais proteção para seus dados e senhas usando o Secure Sockets Layer (SSL). SSL é a tecnologia padrão usada para criar sessões criptografadas para servidores e clientes, e fornece um canal seguro para comunicação por meio de caminhos de comunicação aberta. Com o SSL, a identidade do servidor é verificada usando certificados digitais. Se você autenticar com um servidor Lightweight Directory Access Protocol (LDAP), as senhas entre o servidor e o servidor LDAP serão protegidas por Segurança da Camada de Transporte (TLS). O protocolo de TLS é o sucessor do protocolo de SSL. Quando um servidor e um cliente se comunicam, a TLS assegura que terceiros não possam interceptar mensagens.

---

## **Interfaces com o usuário para o ambiente do IBM Spectrum Protect**

Para tarefas de monitoramento e configuração, o IBM Spectrum Protect fornece várias interfaces, incluindo o Operations Center, uma interface da linha de comandos e uma interface administrativa SQL.

### **Interfaces para gerenciamento de armazenamento de dados**

O Operations Center é a interface primária para os administradores monitorarem e administrarem servidores. Um benefício chave do Operations Center é que é possível monitorar múltiplos servidores, conforme mostrado na Figura 4 na página 12. Também é possível monitorar e administrar o IBM Spectrum Protect a partir de uma interface administrativa de linha de comandos.

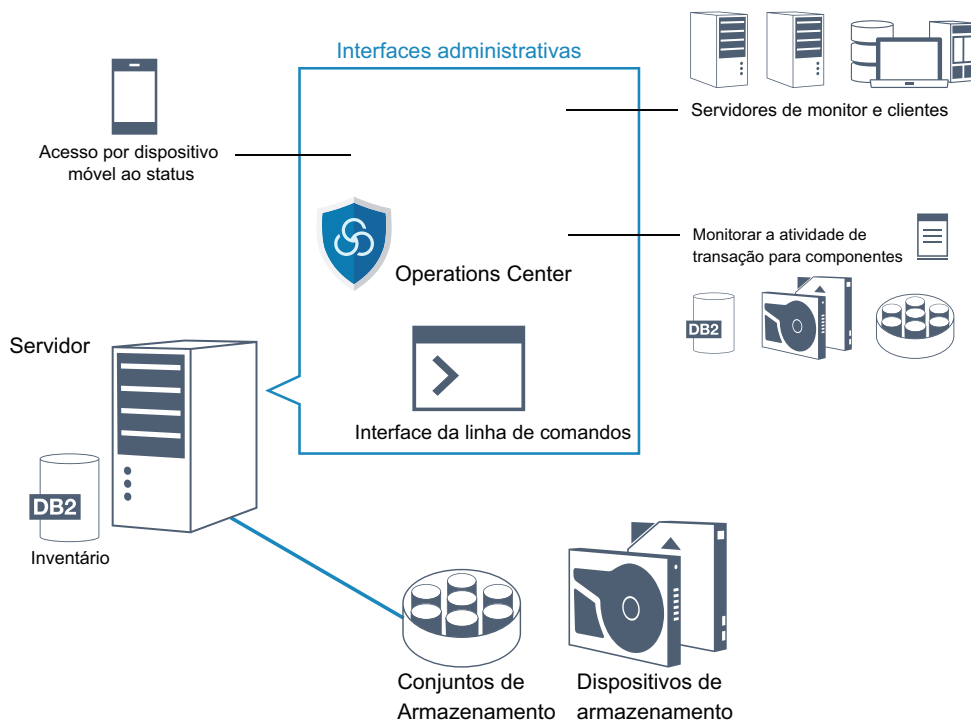


Figura 4. Interfaces com o usuário para gerenciamento de armazenamento de dados

Você usa as interfaces a seguir para interagir com o IBM Spectrum Protect:

### Operations Center

O Operations Center fornece acesso à web e por dispositivo móvel a informações de status sobre o ambiente do IBM Spectrum Protect. É possível usar o Operations Center para concluir algumas tarefas de monitoramento e de administração, por exemplo:

- É possível monitorar múltiplos servidores e clientes.
- É possível monitorar a atividade de transação para componentes específicos no caminho de dados, como o banco de dados do servidor, o log de recuperação, dispositivos de armazenamento e conjuntos de armazenamentos.

### Interface da linha de comandos

É possível usar uma interface da linha de comandos para executar tarefas de administração para servidores. É possível acessar a interface da linha de comandos por meio do cliente administrador do IBM Spectrum Protect ou do Operations Center.

### Acesso a informações no banco de dados do servidor usando instruções SQL

É possível usar instruções SQL SELECT para consultar o banco de dados do servidor e exibir os resultados. As ferramentas de SQL de terceiros estão disponíveis para ajudar os administradores no gerenciamento de banco de dados.

## Interfaces para gerenciamento de atividades de cliente

O IBM Spectrum Protect fornece os seguintes tipos de interfaces para gerenciar a atividade de cliente:

- Uma interface de programação de aplicativos (API)

- Interfaces gráficas com o usuário para clientes
- Interface do navegador para o cliente de backup-archive
- Interfaces da linha de comandos para clientes



---

## Capítulo 2. Conceitos de armazenamento de dados no IBM Spectrum Protect

O IBM Spectrum Protect fornece funções para armazenar dados em um intervalo de armazenamento de dispositivo e de mídia.

Para tornar os dispositivos disponíveis para o servidor, deve-se anexar os dispositivos de armazenamento e mapear conjuntos de armazenamentos para classes de dispositivo, bibliotecas e unidades.

---

### Tipos de dispositivos de armazenamento

É possível usar vários dispositivos de armazenamento com o IBM Spectrum Protect para atender aos objetivos de proteção de dados específicos.

#### Dispositivos de armazenamento e objetos de armazenamento

O servidor do IBM Spectrum Protect pode se conectar a uma combinação de dispositivos de armazenamentos manuais e automatizados. É possível conectar os seguintes tipos de dispositivos de armazenamento ao IBM Spectrum Protect:

- Dispositivos de disco que estão diretamente conectados, conectados por SAN ou conectados à rede
- Dispositivos de fita físicos que são operados manualmente ou automatizados
- Dispositivos de fita virtuais
- Armazenamento de objeto em nuvem

O IBM Spectrum Protect representa dispositivos de armazenamento físico e mídia com objetos de armazenamento definidos no banco de dados do servidor. Os objetos de armazenamento classificam recursos de armazenamento disponíveis e gerenciam a migração de um conjunto de armazenamentos para outro. Tabela 1 descreve os objetos de armazenamento no ambiente de armazenamento do servidor.

*Tabela 1. Objetos de armazenamento e representações*

Objeto de armazenamento	O que o objeto representa
Volume	Uma unidade discreta de armazenamento em disco, em fita ou em outra mídia de armazenamento. Cada volume está associado a um único conjunto de armazenamentos.

Tabela 1. Objetos de armazenamento e representações (continuação)

Objeto de armazenamento	O que o objeto representa
Conjunto de armazenamentos	<p>Um conjunto de volumes de armazenamento ou de contêineres que é o destino usado para armazenar dados de cliente. O IBM Spectrum Protect usa os seguintes tipos de conjunto de armazenamentos:</p> <ul style="list-style-type: none"> <li>• Conjuntos de armazenamentos de contêiner de diretório</li> <li>• Conjuntos de armazenamentos de contêiner em nuvem</li> <li>• Conjuntos de armazenamentos de acesso sequencial que estão associados com uma classe de dispositivo</li> <li>• Conjuntos de armazenamentos de acesso aleatório que estão associados com uma classe de dispositivo</li> </ul>
Contêiner	Um local do armazenamento de dados, por exemplo, um arquivo, diretório ou dispositivo.
Conjunto de armazenamentos de contêiner	Um conjunto de armazenamentos primários que um servidor usa para armazenar dados. Os dados são armazenado em contêineres em diretórios de sistema de arquivos ou em armazenamento em nuvem. Os dados são deduplicados, se necessário, conforme o servidor grava dados no conjunto de armazenamentos.
Classe de dispositivo	O tipo de dispositivo de armazenamento que pode usar os volumes que são definidos em um conjunto de armazenamentos de acesso sequencial ou de acesso aleatório. Cada classe de dispositivo de tipo de mídia removível está associada a uma única biblioteca.
Biblioteca	Um dispositivo de armazenamento. Por exemplo, uma biblioteca pode representar uma unidade independente, um conjunto de unidades independentes, um dispositivo automatizado de várias unidades ou um conjunto de unidades que é controlado por um gerenciador de mídia.
Unidade	Um objeto de um dispositivo de biblioteca de fitas que fornece a capacidade de ler e gravar dados na mídia da biblioteca de fitas. Cada unidade está associada a uma única biblioteca.
Caminho	A especificação da origem de dados e o destino do dispositivo. Antes de um dispositivo de armazenamento ser usado, um caminho deve ser definido entre o dispositivo e o servidor de origem que está movendo dados.



*Tabela 1. Objetos de armazenamento e representações (continuação)*

<b>Objeto de armazenamento</b>	<b>O que o objeto representa</b>
Movedor de dados	Um dispositivo conectado por SAN que é usado para transferir dados de cliente. Um movedor de dados é usado somente em uma transferência de dados em que o servidor não está presente, como em um ambiente do Protocolo de Gerenciamento de Dados de Rede (NDMP). Os movedores de dados transferem dados entre dispositivos de armazenamento sem usar recursos importantes do servidor, do cliente ou de rede.
Servidor	Um servidor que é gerenciado por outro servidor IBM Spectrum Protect.

O administrador define os objetos de armazenamento na camada lógica do servidor, conforme ilustrado na Figura 5 na página 18.

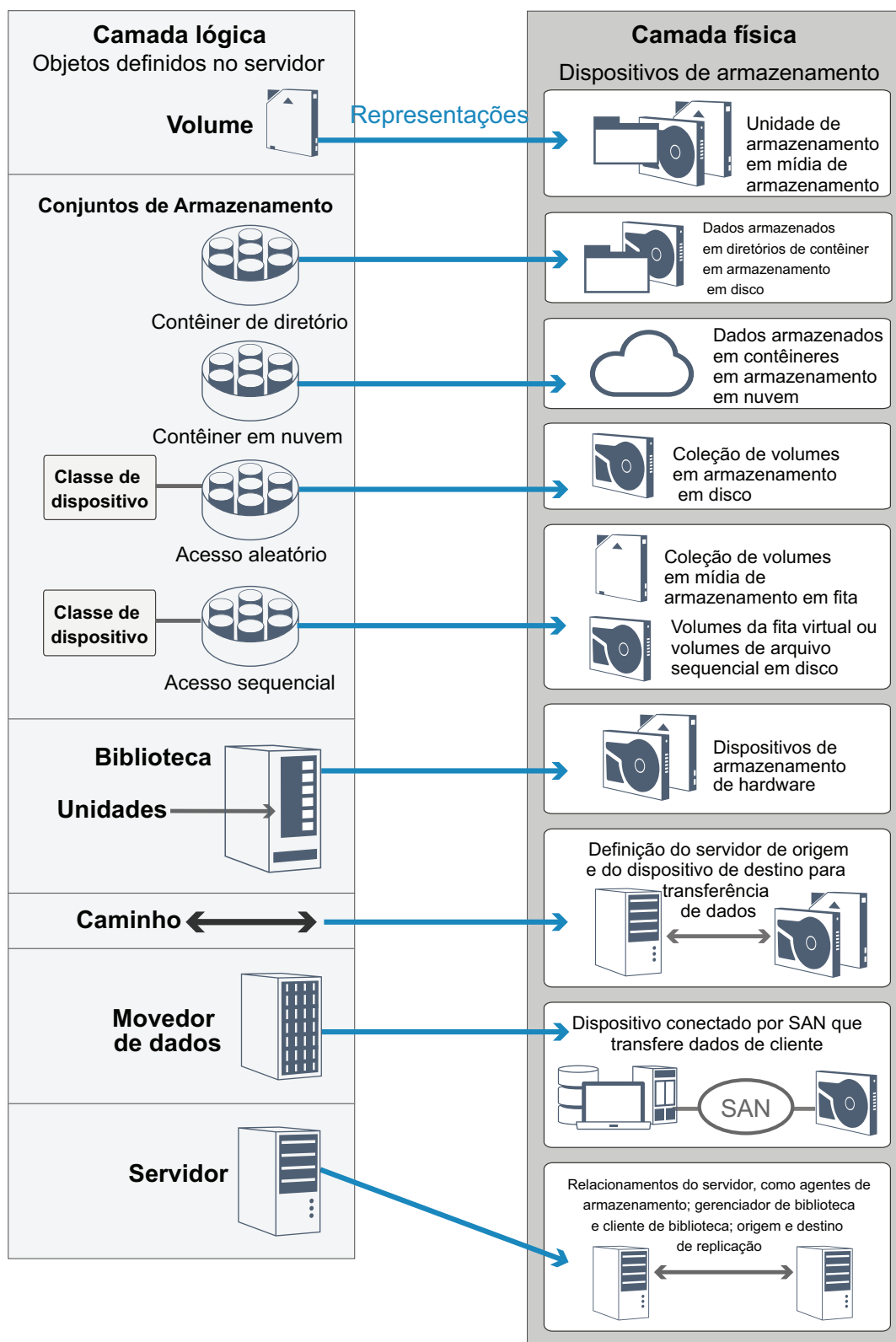


Figura 5. Objetos de armazenamento

## Dispositivos de disco

É possível armazenar dados de cliente em dispositivos de disco com os tipos de volumes a seguir:

- Diretórios em conjuntos de armazenamentos de contêiner de diretório
- Volumes de acesso aleatório de tipo de dispositivo DISK
- Volumes de acesso sequencial de tipo de dispositivo FILE

O IBM Spectrum Protect oferece os seguintes recursos ao usar conjuntos de armazenamentos de contêiner de diretório para armazenamento de dados:

- É possível aplicar técnicas de armazenamento em cache de deduplicação de dados e de disco para aumentar o uso do armazenamento de dados.
- É possível recuperar dados do disco muito mais rapidamente do que é possível recuperar dados de armazenamento em fita.

## Dispositivos de fita físicos

Em uma biblioteca de fitas físicas, a capacidade de armazenamento é definida em termos do número total de volumes na biblioteca. Os dispositivos de fita físicos podem ser usados para as seguintes atividades:

- Armazenar dados de cliente que são submetidos a backup, arquivados ou migrados de nós clientes
- Armazenar backups de banco de dados
- Exportar dados para outro servidor ou armazenamento externo

Mover dados para a fita fornece os seguintes benefícios:

- É possível manter os dados para clientes em um dispositivo de disco ao mesmo tempo em que os dados são movidos para a fita.
- É possível melhorar o desempenho da unidade de fita transferindo a migração de dados do disco para a fita.
- É possível distribuir os tempos em que as unidades estão em uso para melhorar a eficiência das unidades de fita.
- É possível mover dados na fita para áreas seguras externas.
- É possível limitar o consumo de energia porque os dispositivos de fita não consomem energia após os dados serem gravados em fita.
- É possível aplicar a criptografia que é fornecida pelo hardware da unidade de fita para proteger os dados na fita.

Em comparação com o armazenamento em disco e em fita virtual equivalente, o custo unitário para armazenar dados tende a ser muito menos para dispositivos de fita física.

## Bibliotecas de fitas virtual

Um virtual tape library (VTL) não usa mídia de fita física. Ao usar o armazenamento VTL, você emula os mecanismos de acesso de hardware de fita. Em um VTL, é possível definir volumes e unidades para fornecer maior flexibilidade para o ambiente de armazenamento. A capacidade de armazenamento de um VTL é definida em termos do total de espaço em disco disponível. É possível aumentar ou diminuir o número e tamanho de volumes em disco.

A definição de uma VTL para o servidor do IBM Spectrum Protect pode melhorar o desempenho, porque o servidor manipula o processamento de ponto de

montagem para VTLs de forma diferente do que para bibliotecas de fitas reais. Embora as limitações lógicas de dispositivos de fita ainda estejam presentes, as limitações físicas para o hardware de fita não são aplicáveis a uma VTL, dispondo, portanto, de melhor escalabilidade. É possível usar a VTL do IBM Spectrum Protect quando as seguintes condições forem atendidas:

- Apenas um tipo e geração de unidade e mídia são emulados na VTL.
- Cada servidor e agente de armazenamento com acesso à VTL possui caminhos que são definidos para todas as unidades na biblioteca.

---

## Armazenamento de dados em conjuntos de armazenamentos

Os conjuntos de armazenamentos lógicos são os principais componentes no modelo de armazenamento de dados do IBM Spectrum Protect. É possível otimizar o uso de dispositivos de armazenamento manipulando as propriedades de conjuntos e volumes de armazenamentos.

### Tipos de conjuntos de armazenamentos

O grupo de conjuntos de armazenamentos que você configurou para o servidor é chamado de *armazenamento do servidor*. É possível definir os seguintes tipos de conjuntos de armazenamentos em armazenamento do servidor:

#### Conjuntos de armazenamentos primários

Um conjunto nomeado de volumes que o servidor usa para armazenar versões de backup de arquivos, cópias de archive de arquivos e arquivos que são migrados de nós clientes.

#### Conjuntos de armazenamentos de cópia

Um conjunto nomeado de volumes que contém cópias de arquivos que residem em conjuntos de armazenamentos primários. Conjuntos de armazenamentos de cópia são utilizados apenas para backup dos dados que são armazenados nos conjuntos de armazenamentos primários. Um conjunto de armazenamentos de cópias não pode ser um destino para um grupo de cópias de backup, um grupo de cópias de archive ou uma classe de gerenciamento para arquivos gerenciados por espaço.

#### Conjuntos de armazenamentos de cópia de contêiner

Um conjunto nomeado de volumes que contém uma cópia de extensões de dados que residem em conjuntos de armazenamento de contêiner de diretório. Os conjuntos de armazenamento de cópia do contêiner são usados somente para proteger os dados que estão armazenados em conjuntos de armazenamentos de contêiner de diretório.

#### Conjuntos de armazenamentos de dados ativos

Um conjunto nomeado de volumes do conjunto de armazenamentos que contém apenas versões ativas de dados de backup do cliente.

### Conjuntos de armazenamentos primários

Quando você restaura, recupera, faz rechamada ou exporta dados do arquivo, o arquivo solicitado é obtido a partir de um conjunto de armazenamentos primários. Dependendo do tipo de conjunto de armazenamentos primários, os conjuntos de armazenamentos podem estar no local ou ser externos. É possível organizar conjuntos de armazenamentos primários em uma hierarquia de armazenamento de forma que os dados possam ser transferidos de armazenamento em disco para um armazenamento de custo mais baixo, como dispositivos de fita. A Figura 6 na página 21 ilustra o conceito de conjuntos de armazenamentos primários.

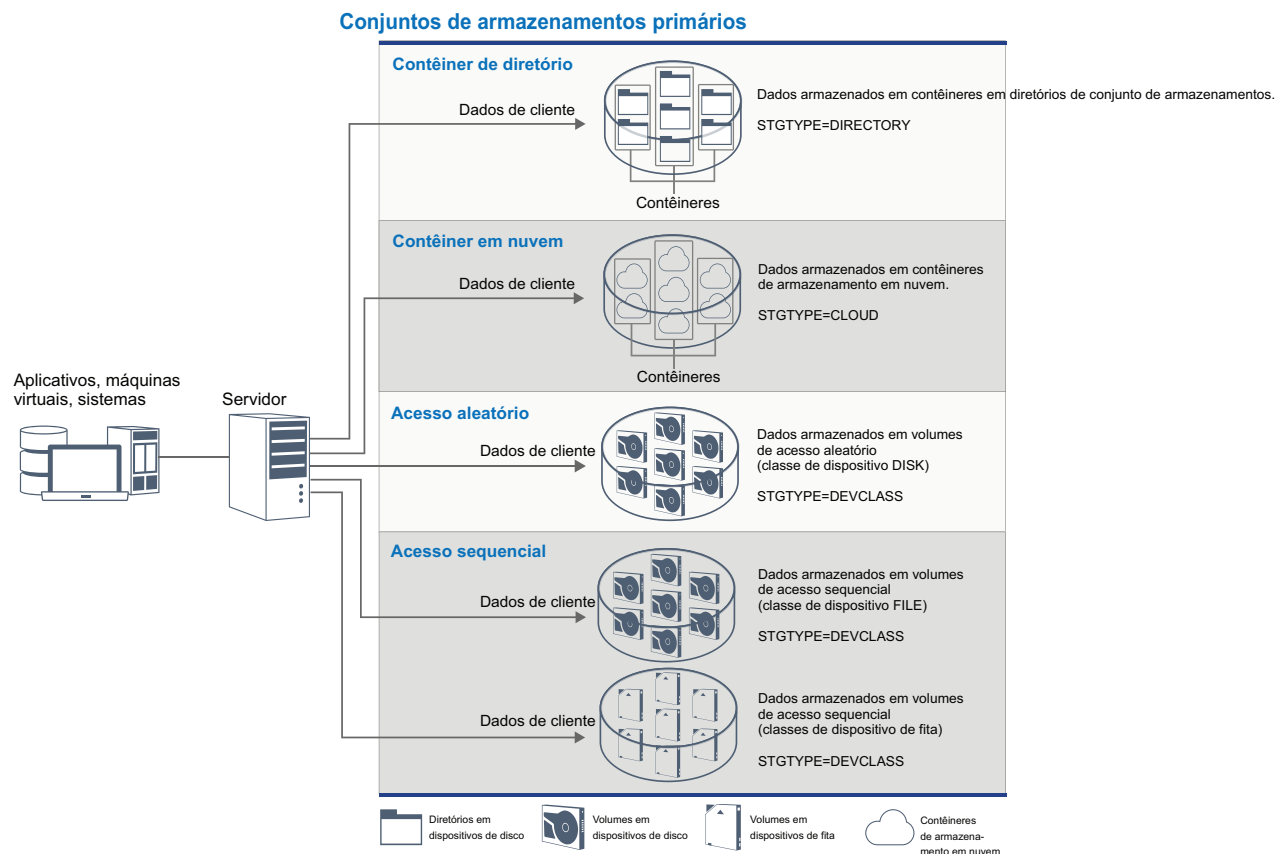


Figura 6. Conjuntos de armazenamentos primários

É possível definir os seguintes tipos de conjunto de armazenamentos primários:

### Conjuntos de armazenamentos de contêiner de diretório

Um conjunto de armazenamentos que o servidor usa para armazenar dados em contêineres em diretórios de conjunto de armazenamentos. Os dados que são armazenados em um conjunto de armazenamentos de contêiner de diretório podem usar a deduplicação de dados sequenciais, a deduplicação de dados do lado do cliente, a compactação sequencial ou a compactação do lado do cliente. A deduplicação de dados sequenciais ou a compactação sequencial reduz os dados no momento em que são armazenados.

**Dica:** Os dados que são compactados primeiro não podem ser deduplicados, entretanto, dados deduplicados podem ser compactados.

Usando conjuntos de armazenamentos de contêiner de diretório, você remove a necessidade de recuperação de volume, o que melhora o desempenho do servidor e reduz o custo de hardware de armazenamento. É possível proteger e reparar dados em conjuntos de armazenamentos de contêiner de diretório no nível do conjunto de armazenamentos. É possível armazenar em camadas os dados que são armazenados em um conjunto de armazenamentos de contêiner de diretório em um conjunto de armazenamentos de contêiner em nuvem.

**Restrição:** Não é possível usar nenhuma das seguintes funções com conjuntos de armazenamentos de contêiner de diretório:

- Migração
- Recuperação
- Agregação
- Disposição
- Gravação simultânea
- Backup do conjunto de armazenamentos
- Volumes virtuais

### **Conjuntos de armazenamentos de contêiner em nuvem**

Um conjunto de armazenamentos que um servidor usa para armazenar dados no armazenamento em nuvem. O armazenamento em nuvem pode ser nas instalações ou fora das instalações. Os conjuntos de armazenamentos de contêiner em nuvem que são fornecidos pelo IBM Spectrum Protect podem armazenar dados em armazenamento em nuvem que é baseado em objeto. Armazenando dados em conjuntos de armazenamentos de contêiner em nuvem, é possível explorar as vantagens de custo por unidade que as nuvens oferecem junto com os recursos de ajuste de escala que o armazenamento em nuvem fornece. É possível usar a definição de camadas em nuvem para reduzir os custos ao mover dados do armazenamento em disco para um conjunto de armazenamentos de contêiner em nuvem. O IBM Spectrum Protect gerencia as credenciais, a segurança, E/Ss de leitura e gravação e o ciclo de vida para dados que são armazenados na nuvem. Quando conjuntos de armazenamentos de contêiner em nuvem são implementados no servidor, é possível gravar diretamente na nuvem configurando um conjunto de armazenamentos de contêiner em nuvem com as credenciais de nuvem. Os dados que são armazenados em um conjunto de armazenamentos de contêiner em nuvem usam a deduplicação de dados sequenciais e a compressão sequencial. O servidor grava dados deduplicados, compactados e criptografados diretamente na nuvem. É possível fazer backup e restaurar dados ou arquivar e recuperar dados diretamente do conjunto de armazenamentos de contêiner em nuvem.

É possível definir os tipos de conjuntos de armazenamentos de contêiner em nuvem a seguir:

#### **No local**

É possível usar o tipo de conjunto de armazenamentos de contêiner em nuvem no local para armazenar dados em uma nuvem particular, para mais segurança e controle máximo sobre os seus dados. As desvantagens de uma nuvem privada são os custos mais altos devido aos requisitos de hardware e manutenção no local.

#### **Fora das instalações**

É possível usar o tipo de conjunto de armazenamentos de contêiner em nuvem fora das instalações para armazenar dados em uma nuvem pública. A vantagem de usar uma nuvem pública em que seja possível diminuir custos em relação a uma nuvem particular, por exemplo, eliminando manutenção. No entanto, deve-se balancear esse benefício com relação a possíveis problemas de desempenho por causa das velocidades da conexão e do controle reduzido sobre os seus dados.

### **Conjuntos de armazenamentos que estão associados a classes de dispositivos**

É possível definir um conjunto de armazenamentos primários para usar os seguintes tipos de dispositivos de armazenamento:

#### **Classe de dispositivo DISK**

Em um tipo de dispositivo DISK do conjunto de armazenamentos, os dados são armazenados em blocos de disco de acesso aleatório. É possível usar o armazenamento em cache em conjuntos de armazenamentos DISK para aumentar o desempenho de restauração do cliente com algumas limitações no processamento do servidor. A alocação de espaço e o rastreamento por blocos usam mais espaço de armazenamento do banco de dados e requer mais energia de processamento do que alocação e rastreamento por volume.

#### **Classe de dispositivo FILE**

Em um tipo de dispositivo FILE do conjunto de armazenamentos, os arquivos são armazenados em volumes sequenciais para melhor desempenho sequencial do que para armazenamento em blocos de disco. Para o servidor, esses arquivos têm as características de um volume da fita para que esse tipo de conjunto de armazenamentos seja mais adequado para migração para a fita. Os volumes FILE são úteis para *transferência eletrônica*, em que os dados são transferidos eletronicamente para um site remoto em vez de por remessa física de fita. Em geral, esse tipo de conjunto de armazenamentos é preferencial sobre conjuntos de armazenamentos DISK.

O servidor usa os conjuntos de armazenamentos primários de acesso aleatório padrão a seguir:

#### **ARCHIVEPOOL**

Na política STANDARD, esse conjunto de armazenamentos é o destino para arquivos que são arquivados de nós clientes.

#### **BACKUPPOOL**

Na política STANDARD, esse conjunto de armazenamentos é o destino para arquivos que são submetidos a backup em nós clientes.

#### **SPACEMGPOOL**

Esse conjunto de armazenamentos é para arquivos gerenciados por espaço que são migrados do IBM Spectrum Protect para nós clientes de Gerenciamento de Espaço.

### **Conjuntos de armazenamentos de cópia**

Os conjuntos de armazenamentos de cópia contêm versões ativas e inativas de dados que são submetidos a backup em conjuntos de armazenamentos primários. Um conjunto de armazenamentos de contêiner de diretório não pode ser usado como um conjunto de armazenamento de cópia. Além disso, os dados de um conjunto de armazenamentos de contêiner de diretório não podem ser copiados para um conjunto de armazenamento de cópia. Para proteger os conjuntos de armazenamentos de contêiner de diretório, copie os dados para um conjunto de armazenamento de cópia do contêiner. A Figura 7 na página 24 ilustra o conceito de conjuntos de armazenamento de cópia.

## Conjuntos de armazenamentos de cópia

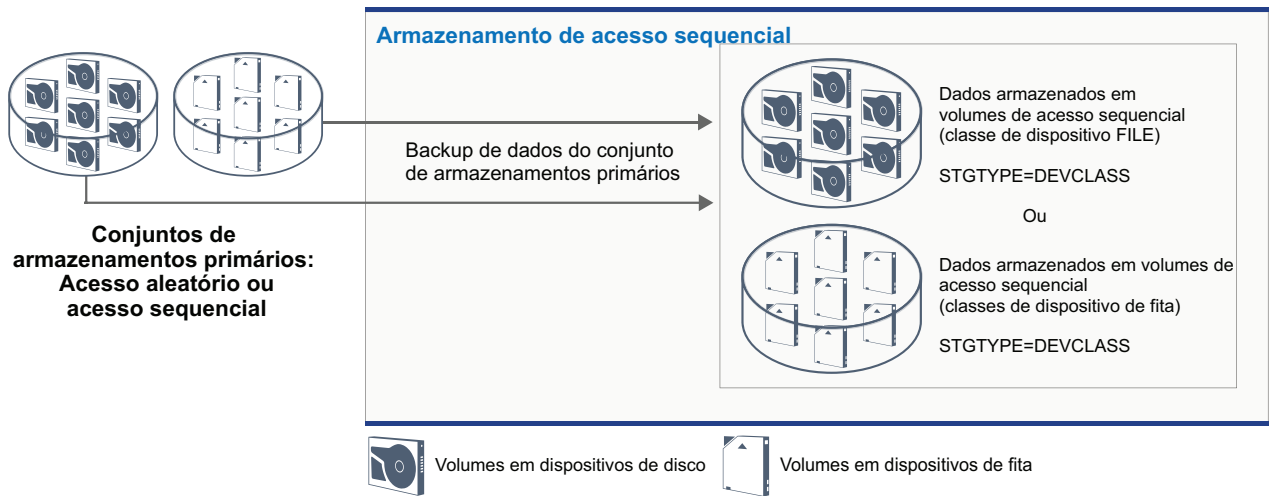


Figura 7. Conjuntos de armazenamentos de cópia

Os conjuntos de armazenamentos de cópias fornecem meios de recuperação de desastres ou de falhas de mídia. Por exemplo, quando um cliente tenta recuperar um arquivo danificado do conjunto de armazenamentos primários e o conjunto de armazenamentos está indisponível ou o arquivo no conjunto de armazenamentos está corrompido, o cliente pode restaurar os dados do conjunto de cópias em armazenamento primário.

É possível mover os volumes de conjuntos de armazenamentos de cópia fora do local e ainda fazer o servidor rastrear os volumes. Mover esses volumes fora do local fornece um meio de recuperação de um desastre no local. Um conjunto de armazenamento de cópia pode usar apenas armazenamento de acesso sequencial, como uma classe de dispositivo de fita ou uma classe de dispositivo FILE.

### Conjuntos de armazenamentos de cópia de contêiner

Um servidor pode proteger um conjunto de armazenamentos de contêiner de diretório armazenando cópias dos dados em um conjunto de armazenamento de cópia do contêiner. Os dados em conjuntos de armazenamento de cópia do contêiner são armazenados em volumes de fita, que podem ser armazenados no local ou externamente. Os dados danificados nos conjuntos de armazenamentos de contêiner de diretório podem ser reparados usando extensões deduplicadas em conjuntos de armazenamento de cópia do contêiner. Os conjuntos de armazenamento de cópia do contêiner fornecem uma alternativa para usar um servidor de replicação para proteger dados em um conjunto de armazenamentos de contêiner de diretório.



**Restrição:** Se todos os dados do servidor forem perdidos, os conjuntos de armazenamento de cópia do contêiner sozinhos não fornecerão o mesmo nível de proteção que a replicação:

- Com a replicação, será possível restaurar os dados de cliente diretamente do servidor de destino se o servidor de origem estiver indisponível.
- Com os conjuntos de armazenamento de cópia do contêiner, deve-se primeiro restaurar o servidor a partir de um backup de banco de dados e, em seguida, reparar os conjuntos de armazenamentos de contêiner de diretório a partir de volumes de fita.

A Figura 8 ilustra o conceito de conjuntos de armazenamento de cópia do contêiner.

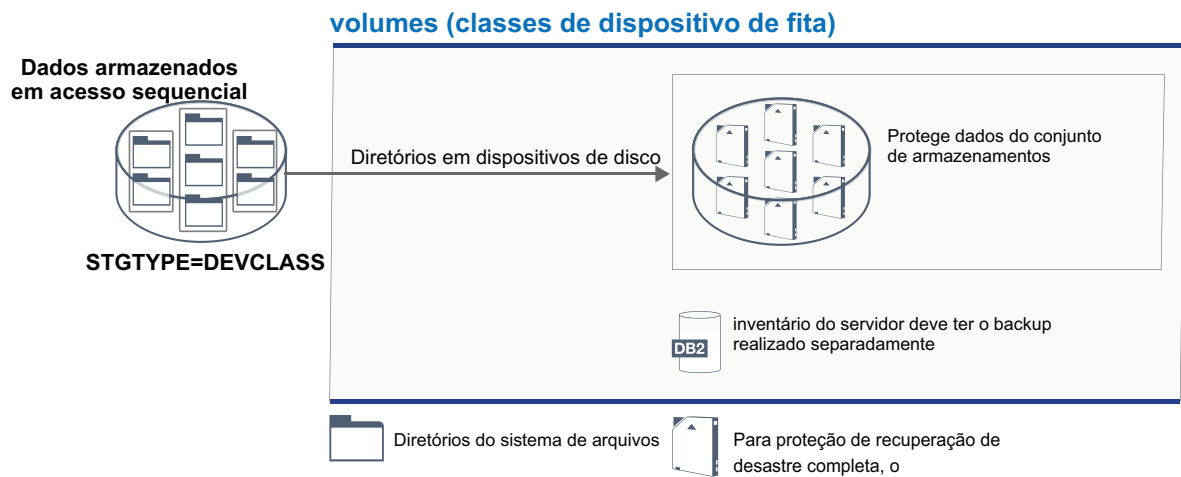


Figura 8. Conjuntos de armazenamentos de cópia de contêiner

Dependendo da configuração do sistema, é possível criar planejamentos de proteção para copiar simultaneamente os dados do conjunto de armazenamentos de contêiner de diretório para os conjuntos de armazenamento de cópia do contêiner no local ou externos para atender a seus requisitos:

- Se a replicação estiver ativada, será possível criar um conjunto de cópias do contêiner externo. A cópia externa pode ser usada para fornecer proteção extra em um ambiente replicado.
- Se a replicação não estiver ativada, será possível criar um conjunto de armazenamento de cópia do contêiner local e um conjunto de armazenamento de cópia do contêiner externo.

Dependendo dos recursos e requisitos de seu site, a capacidade de copiar conjuntos de armazenamentos de contêiner de diretório para fita tem os benefícios a seguir:

- Você evita manter outro servidor e mais espaço de armazenamento em disco.
- Os dados são copiados para conjuntos de armazenamentos que estão definidos no servidor. O desempenho não é dependente da conexão de rede entre os servidores, nem afetado por ela.
- É possível satisfazer os requisitos regulamentares e de negócios para as cópias de fita externas.

## Conjuntos de armazenamentos de dados ativos

Um datapool ativo contém apenas versões ativas de dados de backup do cliente. Nesse caso, o servidor não precisa posicionar arquivos inativos antigos que não precisam ser restaurados. Um conjunto de armazenamentos de contêiner de diretório não pode ser usado como um conjunto de armazenamentos de dados ativos. Você usa conjuntos de dados ativos para melhorar a eficiência de operações de armazenamento e de restauração de dados. Por exemplo, esse tipo de conjunto de armazenamentos pode ajudá-lo a atingir os seguintes objetivos:

- Aumentar a velocidade de operações de restauração de dados do cliente
- Reduzir o número de volumes de armazenamento no local ou fora do local
- Reduzir a quantidade de dados que são transferidos ao copiar ou restaurar arquivos que são transferidos eletronicamente em um local remoto

Os dados que são migrados por clientes de gerenciamento de armazenamento hierárquico (HSM) e dados do archive não são permitidos em data pools ativos. À medida que versões atualizadas de dados de backup são armazenadas em data pools ativos, as versões mais antigas são removidas, pois os dados restantes são consolidados de muitos volumes de acesso sequencial para poucos novos volumes de acesso sequencial. A Figura 9 ilustra o conceito de conjuntos de armazenamentos de dados ativos.

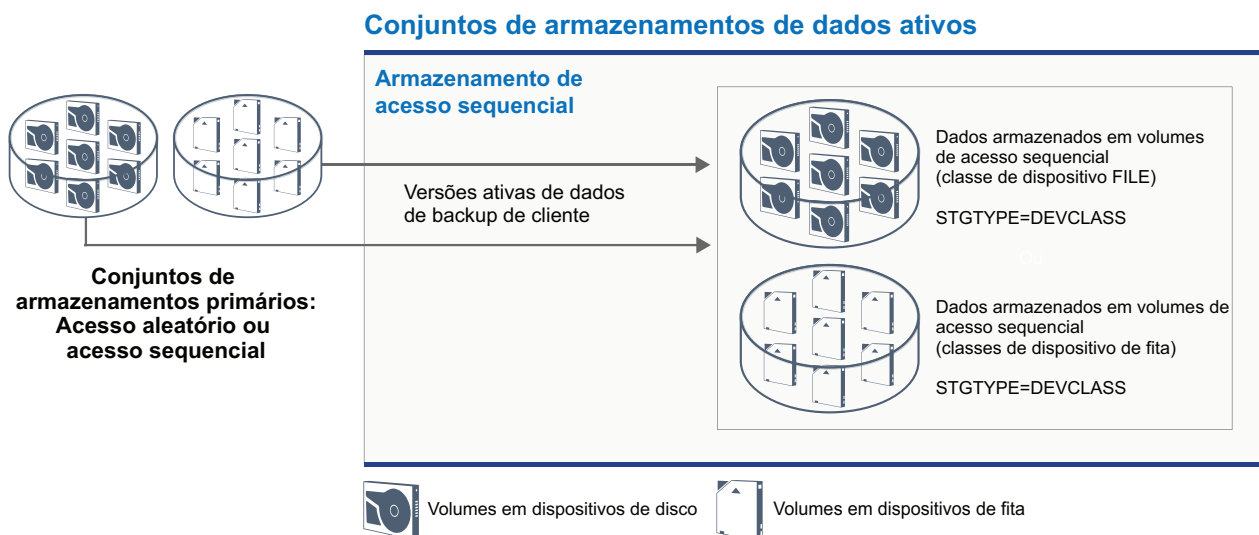


Figura 9. Conjuntos de armazenamentos de dados ativos

Os data pools ativos podem usar qualquer tipo de armazenamento de acesso sequencial. No entanto, os benefícios de um datapool ativo dependem do tipo de

dispositivo que está associado ao conjunto. Por exemplo, os data pools ativos que estão associados a uma classe de dispositivo FILE são ideais para operações rápidas de restauração do cliente pelas seguintes razões:

- Os volumes FILE não precisam ser montados fisicamente
- As sessões do cliente que estão restaurando a partir de volumes FILE em um data pool ativo podem acessar os volumes simultaneamente, o que melhora o desempenho de restauração

---

## Transporte de dados para armazenamento em redes

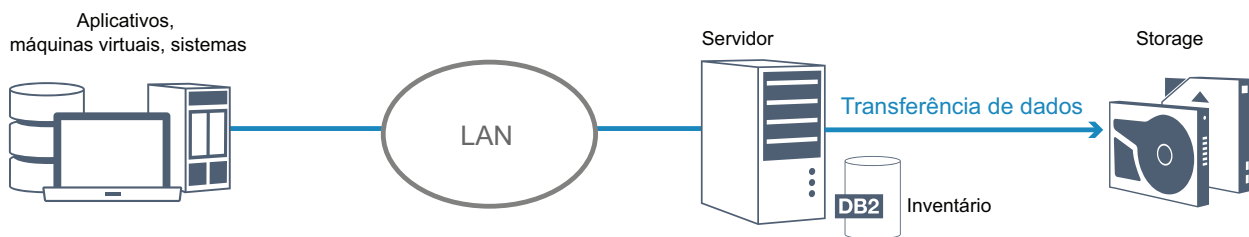
O ambiente do IBM Spectrum Protect fornece maneiras de mover dados com segurança para armazenamento em vários tipos de redes e configurações.

### Configurações de rede para dispositivos de armazenamento

O IBM Spectrum Protect fornece métodos para configurar clientes e servidores em uma rede local (LAN), em uma rede de área de armazenamento (SAN), movimentação de dados sem LAN e como armazenamento conectado à rede.

#### Operações de backup de dados por meio de uma LAN

A Figura 10 mostra o caminho de dados para operações de backup do IBM Spectrum Protect por meio de uma LAN.



*Figura 10. Operações de backup do IBM Spectrum Protect por meio de uma LAN*

Em uma configuração de LAN, uma ou mais bibliotecas de fitas estão associadas a um único servidor do IBM Spectrum Protect. Nesse tipo de configuração, os dados de cliente, correio eletrônico, conexão de terminal, programa de aplicativo e informações de controle de dispositivo devem ser manipulados pela mesma rede. As informações de controle de dispositivo e os dados de backup e restauração do cliente fluem pela LAN.

#### Operações de backup de dados por meio de uma SAN

A Figura 11 na página 28 mostra o caminho de dados para operações de backup do IBM Spectrum Protect por meio de uma SAN.

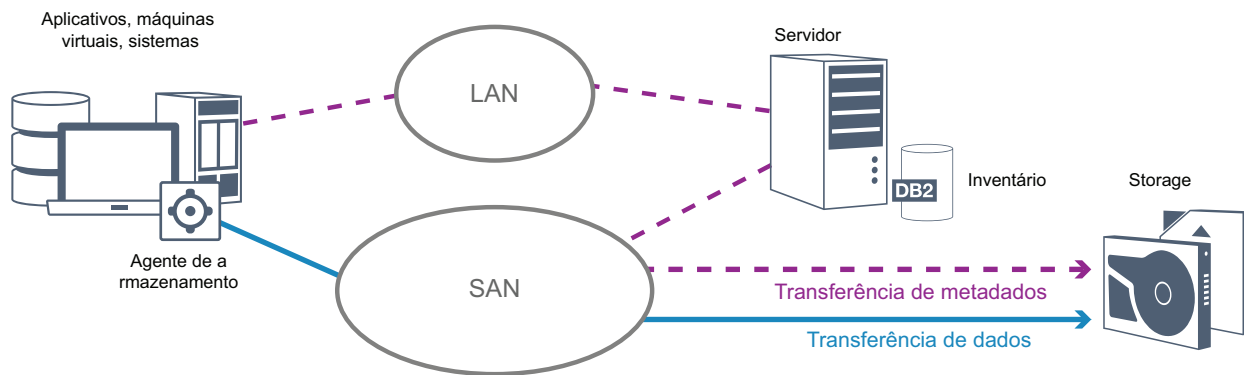


Figura 11. Operações de backup do IBM Spectrum Protect por meio de uma SAN

Uma SAN é uma rede de armazenamento dedicado que pode melhorar o desempenho do sistema. Em uma SAN, é possível consolidar o armazenamento e reduzir a distância, escalabilidade e limitações de largura da banda de LANs e redes de longa distância (WANs). Usando o IBM Spectrum Protect em uma SAN, é possível tirar vantagem das seguintes funções:

- Compartilhar dispositivos de armazenamento entre vários servidores do IBM Spectrum Protect. Os dispositivos que usam o tipo de dispositivo GENERICTAPE não são incluídos.
- Mover dados de um sistema do cliente diretamente para os dispositivos de armazenamento sem usar a LAN. A movimentação de dados sem LAN requer a instalação de um agente de armazenamento no sistema do cliente. O agente de armazenamento está disponível com o produto IBM Spectrum Protect for SAN.

Através do agente de armazenamento, o cliente pode fazer backup e restaurar dados diretamente para uma biblioteca de fitas ou um sistema de arquivos compartilhado como um GPFS. O servidor do IBM Spectrum Protect mantém o banco de dados do servidor e o log de recuperação e age como o gerenciador de biblioteca para controlar operações do dispositivo. O agente de armazenamento no cliente manipula a transferência de dados para o dispositivo na SAN. Essa implementação libera a largura da banda na LAN que, de outra forma, será usada para movimentação de dados do cliente.

- Compartilhar unidades de fita e bibliotecas que são suportadas pelo servidor do IBM Spectrum Protect.
- Consolidar múltiplos clientes sob um nome do nó cliente único em um cluster do General Parallel File System (GPFS).

#### Armazenamento conectado à rede

Os servidores de arquivos de armazenamento conectado à rede (NAS) são servidores de armazenamento dedicado cujos sistemas operacionais são otimizados para funções de entrega de arquivos. Servidores de arquivos com armazenamento conectado à rede interagem com o IBM Spectrum Protect por meio de protocolos de rede padrão de mercado, como Protocolo de Gerenciamento de Dados de Rede (NDMP) ou como armazenamento primário para conjuntos de armazenamentos de acesso aleatório ou de acesso sequencial. O IBM Spectrum Protect fornece os seguintes tipos básicos de configurações que usam o NDMP para fazer backup e gerenciar servidores de arquivos NAS:

- O IBM Spectrum Protect faz backup de um servidor de arquivos NAS para um dispositivo de biblioteca que está diretamente conectado ao servidor de arquivos NAS. O servidor de arquivos NAS, que pode ser remoto a partir do servidor do IBM Spectrum Protect, transfere dados de backup diretamente para uma unidade em uma biblioteca de fitas conectada por SCSI. Os dados são armazenados em conjuntos de armazenamentos formatados por NDMP, que podem ser submetidos a backup para a mídia de armazenamento que pode ser movida para fora do local para proteção, em caso de um desastre no local.
- O IBM Spectrum Protect faz backup de um servidor de arquivos com armazenamento conectado à rede sobre a LAN para uma hierarquia de conjunto de armazenamentos. Nesse tipo de configuração, é possível armazenar dados do NAS diretamente no disco, de acesso aleatório ou acesso sequencial e, em seguida, migrar os dados para a fita. Também é possível usar esse tipo de configuração para replicação de sistema. Os dados também podem ser submetidos a backup em mídia de armazenamento, que pode ser movida para fora do local. A vantagem desse tipo de configuração é que você tem todos os recursos de gerenciamento de dados associados a uma hierarquia do conjunto de armazenamentos.
- O cliente do IBM Spectrum Protect lê os dados a partir do sistema de armazenamento conectado à rede usando protocolos de NFS ou CIFS e envia os dados para o servidor para serem armazenados.

## **Gerenciamento de armazenamento**

Você gerencia os dispositivos e mídia que são usados para armazenar dados de cliente por meio do servidor do IBM Spectrum Protect. O servidor integra gerenciamento de armazenamento com as políticas definidas para gerenciar dados de cliente nas seguintes áreas:

### **Tipos de dispositivos para armazenamento do servidor**

Com o IBM Spectrum Protect, é possível usar dispositivos conectados diretamente e dispositivos conectados à rede para armazenamento do servidor. O IBM Spectrum Protect representa os dispositivos de armazenamento físico e a mídia com objetos de armazenamento definidos pelo administrador.

### **Migração de dados por meio da hierarquia de armazenamento**

Para conjuntos de armazenamentos primários diferentes dos conjuntos de armazenamentos de contêiner de diretório, é possível organizar os conjuntos de armazenamentos em uma ou mais estruturas hierárquicas. Essa hierarquia de armazenamento fornece flexibilidade de várias maneiras. Por exemplo, é possível configurar uma política para fazer backup de dados em discos para operações de backup mais rápidas. O servidor do IBM Spectrum Protect pode então migrar dados automaticamente do disco para a fita.

### **Remoção de dados expirados**

A política definida controla quando os dados de cliente expirarão automaticamente no servidor do IBM Spectrum Protect. Para remover dados que são elegíveis para expiração, um processo de expiração do servidor marca os dados como expirados e exclui metadados para os dados expirados do banco de dados. O espaço que é ocupado pelos dados expirados fica então disponível para novos dados. É possível controlar a frequência do processo de expiração usando uma opção do servidor.

### Reutilização de mídia por recuperação

À medida que as políticas do servidor expiram dados automaticamente, a mídia em que os dados estão armazenados acumula espaço não utilizado. Para mídia de armazenamento diferente dos conjuntos de armazenamentos de contêiner de diretório ou conjuntos de armazenamentos em disco aleatórios, o servidor do IBM Spectrum Protect implementa a *recuperação*, um processo que libera mídia para reutilização sem rotação de fita tradicional. A recuperação desfragmenta automaticamente a mídia, consolidando dados não expirados em outra mídia quando o espaço livre na mídia atinge um nível definido. A mídia recuperada pode então ser usada novamente pelo servidor. A recuperação permite que a mídia circule automaticamente por meio do processo de gerenciamento de armazenamento e reduz o número de mídias necessárias.

### Consolidando dados de cliente de backup

Ao agrupar os dados de cliente que são submetidos a backup, é possível reduzir o número de montagens de mídia necessárias para recuperação do cliente. O servidor do IBM Spectrum Protect fornece os seguintes métodos para agrupar arquivos do cliente em mídia de armazenamento diferente de conjuntos de armazenamentos de contêiner de diretório:

#### Dispondo dados de cliente

O servidor IBM Spectrum Protect pode *colocar* dados de cliente, em outras palavras, armazenar dados de cliente em alguns volumes ao invés de difundir os dados entre muitos volumes. A disposição por cliente reduz o número de volumes necessários para fazer backup e restaurar dados de cliente. A disposição de dados pode aumentar o número de montagens de volume porque cada cliente pode ter um volume dedicado ao invés de armazenamento de dados para vários clientes no mesmo volume.

É possível configurar o servidor para dispor os dados de cliente quando os dados são inicialmente colocados no armazenamento do servidor. Em uma hierarquia de armazenamento, é possível dispor os dados quando o servidor migra os dados do conjunto de armazenamentos inicial para o próximo conjunto de armazenamentos na hierarquia de armazenamento. É possível dispor por cliente, por espaço no arquivo por cliente ou por um grupo de clientes. Sua seleção depende do tamanho dos espaços no arquivo que são armazenados e dos requisitos de restauração.

#### Associando data pools ativos a vários dispositivos

Datapools ativos são úteis para restauração rápida de dados de cliente. Os benefícios incluem uma redução no número de volumes de armazenamento no local ou externo ou a redução de largura da banda quando você copia ou restaura arquivos que são tornados seguros eletronicamente em um local remoto. Os data pools ativos que usam mídia removível, como fita, oferecem benefícios semelhantes. Embora os dispositivos de fita devam ser montados, o servidor não precisa posicionar arquivos inativos antigos. No entanto, o principal benefício de usar mídia removível em data pools ativos é que o número de volumes usados para armazenamento no local e fora do local é reduzido. Se você armazenar dados em um local remoto, será possível reduzir a quantidade de dados que devem ser transferidos copiando e restaurando apenas dados ativos.

#### Criando um conjunto de backup

Um conjunto de backup contém todos os arquivos de backup ativos existentes para esse cliente no armazenamento do servidor. O conjunto de backup é móvel e é mantido pelo tempo especificado. Um conjunto de backup é muito além de backups que já estão armazenados e requer mídia extra.

#### **Movendo dados para um nó cliente**

É possível consolidar dados para um nó cliente movendo os dados no armazenamento do servidor. É possível mover um conjunto de backup para uma mídia diferente, em que o conjunto de backup é mantido até o tempo especificado. A consolidação dos dados pode ajudar a melhorar a eficiência durante operações de restauração ou de recuperação.





---

## Capítulo 3. Estratégias de proteção de dados com o IBM Spectrum Protect

O IBM Spectrum Protect fornece maneiras de você implementar várias estratégias de proteção de dados.

É possível configurar o IBM Spectrum Protect para enviar dados para dispositivos de armazenamento que estão no site local ou em um site remoto. Para aumentar a proteção de dados, é possível configurar a replicação para um servidor remoto.

---

### Estratégias para minimizar o uso do espaço de armazenamento para backups

Para minimizar a quantidade de espaço de armazenamento necessário, o IBM Spectrum Protect faz backup de dados usando as técnicas de deduplicação de dados e de backup incremental progressivo.

#### Deduplicação de dados

Quando o servidor IBM Spectrum Protect recebe dados de um cliente, o servidor identifica extensões de dados duplicadas e armazena instâncias exclusivas das extensões de dados em um conjunto de armazenamentos de contêineres de diretório. A técnica de deduplicação de dados melhora a utilização de armazenamento e elimina a necessidade de um dispositivo de deduplicação de dados dedicado.

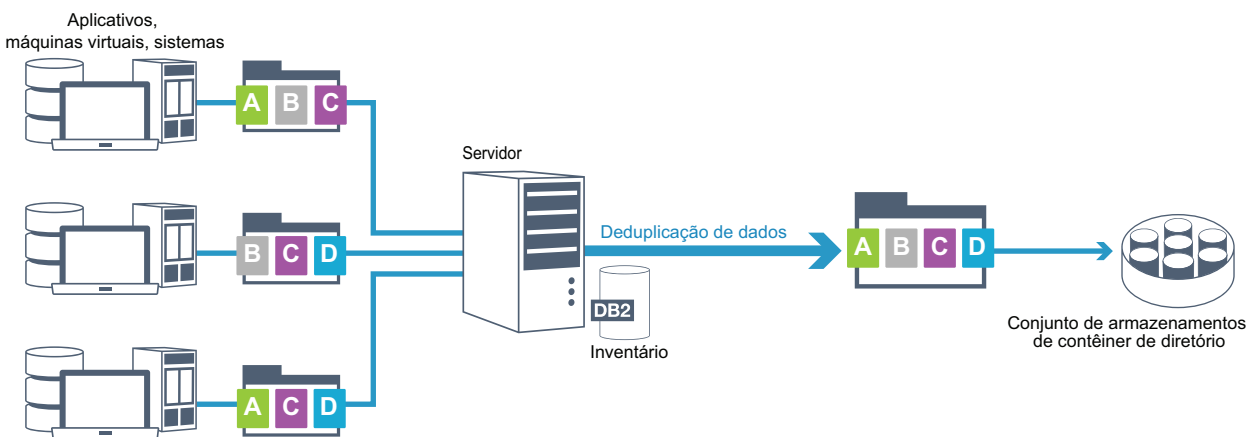


Figura 12. Processo de deduplicação de dados

Se o mesmo padrão de byte ocorrer várias vezes, a deduplicação de dados reduzirá significativamente a quantidade de dados que devem ser armazenados ou transferidos. Além de arquivos inteiros, o IBM Spectrum Protect também pode deduplicar partes de arquivos que são comuns com partes de outros arquivos.

O IBM Spectrum Protect fornece os seguintes tipos de deduplicação de dados:

#### Deduplicação de dados do lado do servidor

O servidor identifica extensões de dados duplicadas e move os dados para um conjunto de armazenamentos de contêiner de diretório. O processo do lado do servidor usa a *deduplicação de dados sequenciais*, em que os dados são deduplicados ao mesmo tempo em que os dados são gravados em um conjunto de armazenamentos de contêiner de diretório. Os dados deduplicados também podem ser armazenados em outros tipos de conjuntos de armazenamentos. A deduplicação de dados sequenciais no servidor fornece os seguintes benefícios:

- Elimina a necessidade de recuperação
- Reduz o espaço que é ocupado pelos dados armazenados

#### **Deduplicação de dados do lado do cliente**

Com esse método, o processamento é distribuído entre o servidor e o cliente durante um processo de backup. O cliente e o servidor identificam e removem dados deduplicados para economizar espaço de armazenamento no servidor. Na deduplicação de dados do lado do cliente, apenas os dados compactados e deduplicados são enviados ao servidor. O servidor armazena os dados no formato compacto que é fornecido pelo cliente. A deduplicação de dados do lado do cliente fornece os seguintes benefícios:

- Reduz a quantidade de dados que são enviados através da rede local (LAN)
- Elimina a energia de processamento extra e o tempo necessário para remover dados duplicados no servidor
- Melhora o desempenho do banco de dados porque a deduplicação de dados do lado do cliente também é sequencial

É possível combinar a deduplicação de dados do lado do cliente e do lado do servidor no mesmo ambiente de produção. A capacidade de deduplicar dados no cliente ou no servidor fornece flexibilidade em termos de utilização de recurso, gerenciamento de política e proteção de dados.

#### **Compactação**

Use a compactação sequencial para reduzir a quantidade de espaço armazenada nos conjuntos de armazenamentos de contêiner. Os dados são compactados conforme são gravados no conjunto de armazenamentos de contêiner.

**Restrição:** O servidor do IBM Spectrum Protect não pode compactar dados criptografados.

#### **Backup incremental progressivo**

Em um processo de backup incremental progressivo, o servidor monitora a atividade de cliente e faz backup de qualquer arquivo que mude desde o backup completo inicial. Arquivos inteiros são submetidos a backup, para que o servidor não precise referenciar versões base dos arquivos. Essa técnica de backup elimina a necessidade de vários backups completos de dados de cliente, economizando, portanto, recursos de rede e espaço de armazenamento.

---

## Estratégias para proteção de desastre

O IBM Spectrum Protect fornece estratégias para proteger dados se ocorrer um desastre. Essas estratégias incluem replicação de nó para um site remoto, proteção do conjunto de armazenamentos, backups de banco de dados, movimentação de fitas de backup externas e replicação de dispositivo para um servidor de espera.

### Replicação para um site remoto

*Replicação de nó* é o processo de copiar dados de forma incremental de um servidor para outro servidor. O servidor a partir do qual os dados de cliente são replicados é chamado de *servidor de replicação de origem*. O servidor para o qual os dados de cliente são replicados é chamado de *servidor de replicação de destino*. Para os propósitos de proteção de desastre, o servidor de replicação de destino está em um site remoto. Um servidor de replicação pode funcionar como um servidor de origem, um servidor de destino ou ambos. Use o processamento de replicação para manter o mesmo nível de arquivos nos servidores e origem e de destino.

A replicação de nó fornece a disponibilidade imediata de dados por meio de failover. Embora a replicação de nó proteja a maioria dos metadados, essa abordagem não fornece proteção adequada para dano de banco de dados. É possível fornecer uma proteção mais abrangente usando conjuntos de armazenamentos para armazenar backups de dados.

#### Vantagens

- Executa failover para que os dados fiquem disponíveis imediatamente se ocorrer um desastre.
- Replicação incremental, que resulta em transmissão rápida de dados.
- Transferência eletrônica
- Protege dados e a maioria dos metadados

#### Desvantagens

- Dados e metadados devem ser recuperados.
- Os dados no servidor de origem devem ser replicados novamente a partir do site remoto.

A Figura 13 na página 36 mostra o processo de replicação de nó para um site remoto.

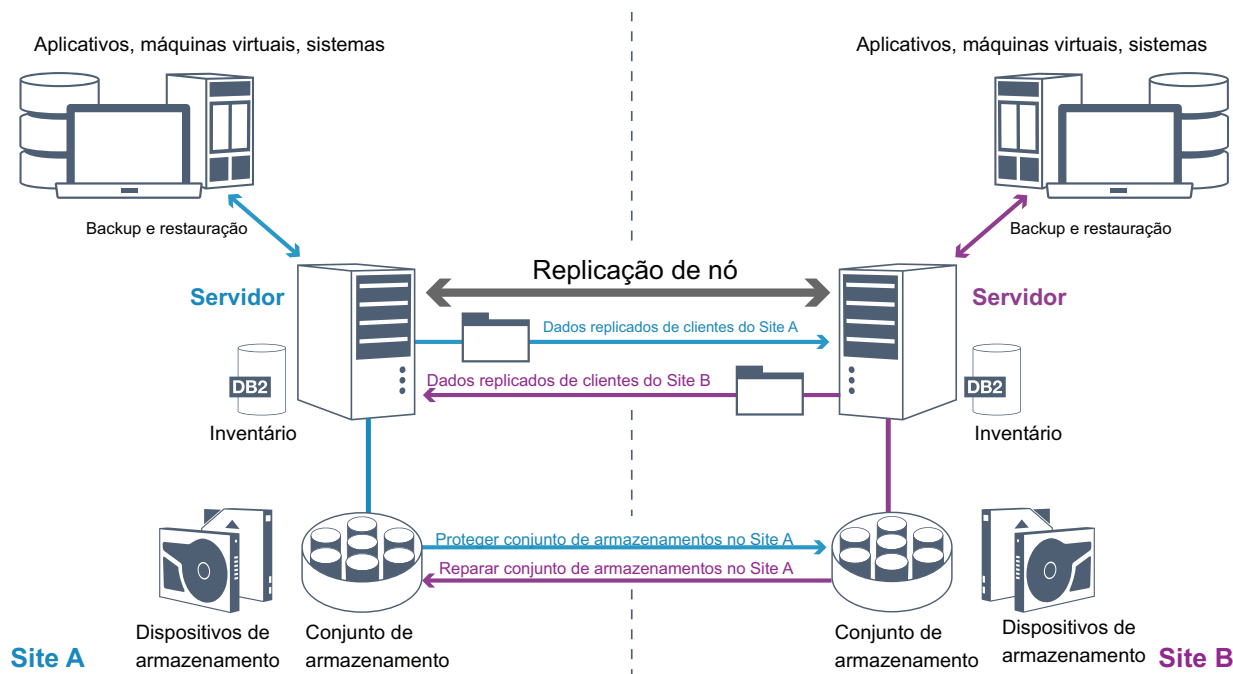


Figura 13. Processo de replicação de nó

Quando dados de cliente são replicados, os dados que não estão no servidor de destino são copiados para o servidor de destino. Quando dados replicados excedem o limite de retenção, o servidor de destino remove automaticamente os dados do servidor de origem. Para aumentar a proteção de dados, você sincroniza o servidor local e o servidor remoto; por exemplo, o Site B replica dados do Site A e o Site A replica dados do Site B. Como parte do processamento de replicação, os dados de cliente que foram excluídos do servidor de origem também são excluídos do servidor de destino.

O IBM Spectrum Protect fornece as seguintes funções de replicação:

- É possível definir políticas para o servidor de destino das seguintes maneiras:
  - Políticas idênticas no servidor de origem e no servidor de destino
  - Políticas diferentes no servidor de origem e no servidor de destino para atender a diferentes necessidades de negócios.

Se ocorrer um desastre e o servidor de origem não estiver disponível, os clientes poderão recuperar dados do servidor de destino. Se o servidor de origem não puder ser recuperado, é possível instruir clientes a armazenarem dados no servidor de destino. Quando ocorre uma indisponibilidade, os clientes dos quais é feito backup no servidor de origem podem executar failover automaticamente para restaurar seus dados do servidor de destino.

- É possível usar o processamento de replicação para recuperar arquivos danificados de conjuntos de armazenamentos. Deve-se replicar os dados de cliente para o servidor de destino antes de ocorrer dano no arquivo. Os processos de replicação subsequentes detectam arquivos danificados no servidor de origem e substituem os arquivos por arquivos não danificados do servidor de destino.

## **Função de replicação em proteção de desastre**

Se ocorrer um desastre, é possível recuperar dados replicados do site remoto e manter o mesmo nível de arquivos nos servidores de origem e de destino. Use a replicação para atingir os seguintes objetivos:

- Controlar o rendimento de rede planejando a replicação de nó em horários específicos
- Recuperar dados após uma perda de site.
- Recuperar arquivos danificados no servidor de origem.

## **Proteção do conjunto de armazenamentos**

Como parte de uma estratégia de recuperação de desastre, certifique-se de que uma cópia de backup de dados nos conjuntos de armazenamentos esteja disponível em um site remoto.

### **Vantagens**

- Recuperação rápida e reconstrução do sistema de origem.

### **Desvantagens**

- Somente dados são protegidos; metadados não são protegidos.
- Para cada conjunto de armazenamentos, você deve definir a mídia de armazenamento.

Use diferentes técnicas para proteger contra a perda permanente de dados que são armazenados em conjuntos de armazenamentos de contêiner e em conjuntos de armazenamentos FILE e DISK.

### **Conjuntos de armazenamentos de contêiner de diretório**

Se você não precisar replicar todos os dados que estão contidos em um nó cliente, você usará os conjuntos de armazenamentos de cópia do contêiner para proteger alguns conjuntos de armazenamentos de contêiner de diretório. Ao proteger um conjunto de armazenamentos de contêiner de diretório, não use recursos que replicam dados e metadados existentes, o que melhora o desempenho do servidor.

O método preferencial é proteger o conjunto de armazenamentos de contêiner de diretório antes de replicar o nó cliente. Quando a replicação de nó for iniciada, as extensões de dados que já estão replicadas por meio da proteção do conjunto de armazenamentos serão ignoradas, o que reduz o tempo de processamento de replicação. Se os dados em um conjunto de armazenamentos de contêiner de diretório forem danificados, é possível repará-los de uma cópia em um conjunto de armazenamento de cópia do contêiner.

### **Conjuntos de armazenamentos de cópia do contêiner**

Você protege conjuntos de armazenamentos de contêiner de diretório copiando os dados no conjunto de armazenamentos de contêiner de diretório para conjuntos de armazenamentos de cópia do contêiner. Use conjuntos de armazenamentos de cópia do contêiner para criar até duas cópias de fita de um conjunto de armazenamentos de contêiner de diretório. O armazenamento das cópias de fita poder no local ou externo. Os dados danificados nos conjuntos de armazenamentos de contêiner de diretório podem ser reparados usando conjuntos de armazenamentos de cópia do contêiner. Os conjuntos de armazenamentos de cópia do contêiner

fornece uma alternativa para usar um servidor de replicação para proteger dados em um conjunto de armazenamentos de contêiner de diretório.

### **Conjuntos de armazenamentos que estão associados a classes de dispositivos FILE e DISK**

Para conjuntos de armazenamentos que estão associados a classes de dispositivos FILE e DISK, use a replicação de nó para manter uma cópia consistente de nó dos dados no servidor de destino. A cópia de dados pode ser restaurada diretamente do servidor de destino para os conjuntos de armazenamentos.

## **Backups de banco de dados**

Use backups de banco de dados para recuperar seu sistema após dano do banco de dados. Além disso, as operações de backup de banco de dados devem ser usadas para evitar que o Db2 seja executado sem espaço de log de archive. As operações de backup de banco de dados não fazem parte da replicação de nó. Um backup de banco de dados pode ser integral, incremental ou de captura instantânea. Para fornecer recuperação de desastre, uma cópia dos backups de banco de dados deve ser armazenada externamente. Para restaurar o banco de dados, deve-se ter os volumes de backup para o banco de dados. É possível restaurar o banco de dados a partir de volumes de backup por meio de uma operação de restauração de um momento ou de uma operação de restauração mais atual.

### **Restauração de um momento**

Use operações de restauração do momento para situações como recuperação de desastre ou para remover os efeitos de erros que podem causar inconsistências no banco de dados. Operações de restauração para o banco de dados que usa backups de captura instantânea são uma forma de operação de restauração do momento. A operação de restauração do momento inclui as ações a seguir:

- Remove e recria o diretório de log ativo e o diretório de log de archive especificados no arquivo `dsmserv.opt`.
- Restaura a imagem do banco de dados de volumes de backup para os diretórios do banco de dados que são registrados em um backup de banco de dados ou em novos diretórios.
- Restaura logs de archive de volumes de backup para o diretório de estouro.
- Usa informações de log do diretório de estouro até um momento especificado.

### **Restauração mais recente**

Se desejar recuperar o banco de dados para o momento em que ele foi perdido, recupere-o para o estado mais atual. A operação de restauração mais atual inclui as ações a seguir:

- Restaura uma imagem do banco de dados dos volumes de backup para os diretórios do banco de dados que são registrados em um backup de banco de dados ou em novos diretórios.
- Restaura logs de archive de volumes de backup para o diretório de estouro.
- Usa informações de log do diretório de estouro e logs de archive do diretório de log de archive.

A restauração mais atual não remove e recria o diretório de log ativo ou o diretório de log de archive.

## **Métodos alternativos para proteção de desastre**

Além da replicação, proteção do conjunto de armazenamentos e backups de banco de dados, também é possível usar os seguintes métodos para proteger dados e implementar a recuperação de desastre com o IBM Spectrum Protect:

### **Envio de fitas de backup para um site remoto**

Os dados são submetidos a backup em fita em horários planejados pelo servidor de origem. As fitas são enviadas para um site remoto. Se ocorrer um desastre, as fitas serão retornadas ao site do servidor de origem e os dados serão restaurados nos clientes de origem. As cópias de dados externas em fitas de backup também podem ajudar na recuperação de ataques de ransomware.

### **Replicação do dispositivo de vários sites para um servidor de espera**

Na configuração do dispositivo de vários sites, o dispositivo de origem é replicado para um servidor remoto em uma arquitetura de SAN. Nesta configuração, se o hardware do cliente no site original for danificado, o dispositivo de origem poderá ser replicado do servidor de espera no site remoto. Essa configuração fornece operações de backup e restauração baseadas em disco.

## **Comparação de estratégias de configuração de proteção**

Considere os cenários de perda de dados em potencial a seguir:

- Os dados do banco de dados são danificados: proteja-se contra a perda e dados no banco de dados usando o backup de banco de dados no local.
- Os dados do conjunto de armazenamentos são danificados: proteja-se contra a perda de dados em conjuntos de armazenamentos usando conjuntos de armazenamentos de cópia no local ou replicação de nó.
- Cenário de desastre em que o banco de dados e conjuntos de armazenamentos no local são perdidos: proteja-se contra um desastre total usando a replicação de nó e cópias de backup de banco de dados externas e de backup do conjunto de armazenamentos.

As configurações possíveis a seguir abordam os cenários de proteção de dados mais comuns:

### **Configurações apenas para proteção contra dano**

- Implemente operações de backup de banco de dados no local com um conjunto de armazenamento de cópia do contêiner opcional no local para proteger dados em conjuntos de armazenamentos de contêiner de diretório.
- Implemente operações de backup de banco de dados no local e replicação de nó no local.

### **Configurações para recuperação de desastre e proteção contra dano**

- Implemente operações de backup de banco de dados externas com conjuntos de armazenamento de cópia do contêiner externos para proteger dados em conjuntos de armazenamentos de contêiner de diretório.

- Implemente operações de backup de banco de dados no local e replicação de nó externa com um conjunto de armazenamento de cópia do contêiner opcional no local para recuperação mais rápida de dados danificados.

## Estratégias para recuperação de desastre com o IBM Spectrum Protect

O IBM Spectrum Protect fornece várias maneiras de recuperar o servidor se o banco de dados ou conjuntos de armazenamentos falharem.

### Failover automático para recuperação de desastre

*Failover automático* é uma operação que alterna para um sistema de espera se ocorrer uma interrupção de software, de hardware ou de rede. Failover automático é usado com replicação de nó para recuperar dados após uma falha do sistema. A Figura 14 mostra o processo de failover automático do IBM Spectrum Protect.

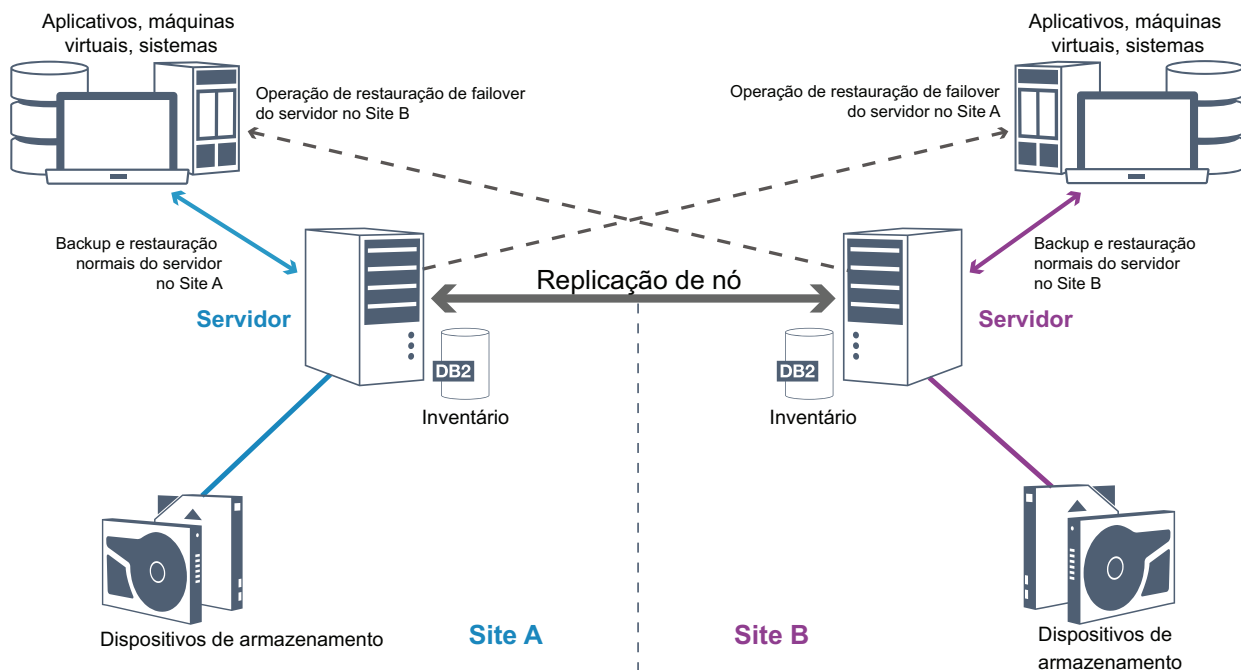


Figura 14. Processo de failover automático

O failover automático para recuperação de dados ocorrerá se o servidor de replicação de origem estiver indisponível devido a um desastre ou uma indisponibilidade do sistema. Durante operações normais, quando o cliente acessa um servidor de replicação de origem, o cliente recebe informações de conexão para o servidor de replicação de destino. O nó cliente armazena as informações de conexão de failover no arquivo de opções do cliente.

Durante operações de restauração do cliente, o servidor muda automaticamente os clientes do servidor de replicação de origem para o servidor de replicação de destino e vice-versa. Apenas um servidor por nó pode ser usado para proteção de failover a qualquer momento. Quando uma nova operação do cliente é iniciada, o cliente tenta conectar-se ao servidor de replicação de origem. O cliente continuará as operações no servidor de origem se o servidor de replicação de origem estiver disponível.



Para usar o failover automático para nós clientes replicados, o servidor de replicação de origem, o servidor de replicação de destino e o cliente devem estar no nível da V7.1 ou mais recente. Se algum dos servidores estiver em um nível anterior, o failover automático será desativado e deve-se contar com um processo de failover manual.

## **Recuperação de componentes do IBM Spectrum Protect**

O banco de dados do servidor, o log de recuperação e conjuntos de armazenamentos são críticos para a operação do IBM Spectrum Protect e devem ser protegidos. Se o banco de dados estiver inutilizável, todo o servidor estará indisponível e a recuperação de dados gerenciados pelo servidor poderá ser difícil ou impossível.

Mesmo sem o banco de dados, os fragmentos de dados ou arquivos completos podem ser lidos a partir de volumes do conjunto de armazenamentos que não estão criptografados e a segurança pode ser comprometida. Portanto, sempre deve-se fazer backup do banco de dados. Além disso, sempre criptografe os dados sensíveis usando o cliente ou o dispositivo de armazenamento, a menos que a mídia de armazenamento esteja fisicamente assegurada.

O IBM Spectrum Protect fornece vários métodos de proteção de dados, que incluem o backup de conjuntos de armazenamentos e do banco de dados. Por exemplo, é possível definir planejamentos para que ocorram as seguintes operações:

- Após o backup completo inicial de seus conjuntos de armazenamentos, os backups incrementais do conjunto de armazenamentos são executados todas as noites.
- Os backups de banco de dados incrementais são executados todas as noites.
- Os backups de banco de dados completos são executados uma vez por semana.

Para ambientes baseados em fita, é possível usar o gerenciador de recuperação de desastres (DRM) para ajudá-lo em muitas das tarefas que estão associadas com a proteção e a recuperação de dados. O DRM está disponível com o IBM Spectrum Protect Extended Edition.

## **Ações preventivas para recuperação**

A recuperação é baseada nas ações preventivas a seguir:

- Espelhamento, pelo qual o servidor mantém uma cópia do log ativo
- Fazendo backup do banco de dados
- Fazendo backup dos conjuntos de armazenamentos
- Auditoria de conjuntos de armazenamentos para arquivos danificados e recuperação de arquivos danificados quando necessário
- Backup dos arquivos de configuração do dispositivo e do histórico de volume
- Validação dos dados em conjuntos de armazenamentos usando a verificação cíclica de redundância
- Armazenamento do arquivo cert.kdb em um local seguro para garantir que o Secure Sockets Layer (SSL) esteja seguro

Se estiver usando fita para armazenamento, também é possível criar um plano de recuperação de desastres para orientá-lo no processo de recuperação usando o DRM. É possível usar o plano de recuperação de desastres para propósitos de

auditoria para certificar a recuperabilidade do servidor. Os métodos de recuperação de desastre do DRM são baseados na tomada das ações a seguir:

- Criação de um arquivo de plano de recuperação de desastres para o servidor
- Backup dos dados do servidor para a fita
- Envio dos dados de backup do servidor para um site remoto ou para outro servidor
- Armazenamento das informações do sistema do cliente
- Definição e rastreamento da mídia de armazenamento que é usada para armazenar e recuperar dados de cliente

---

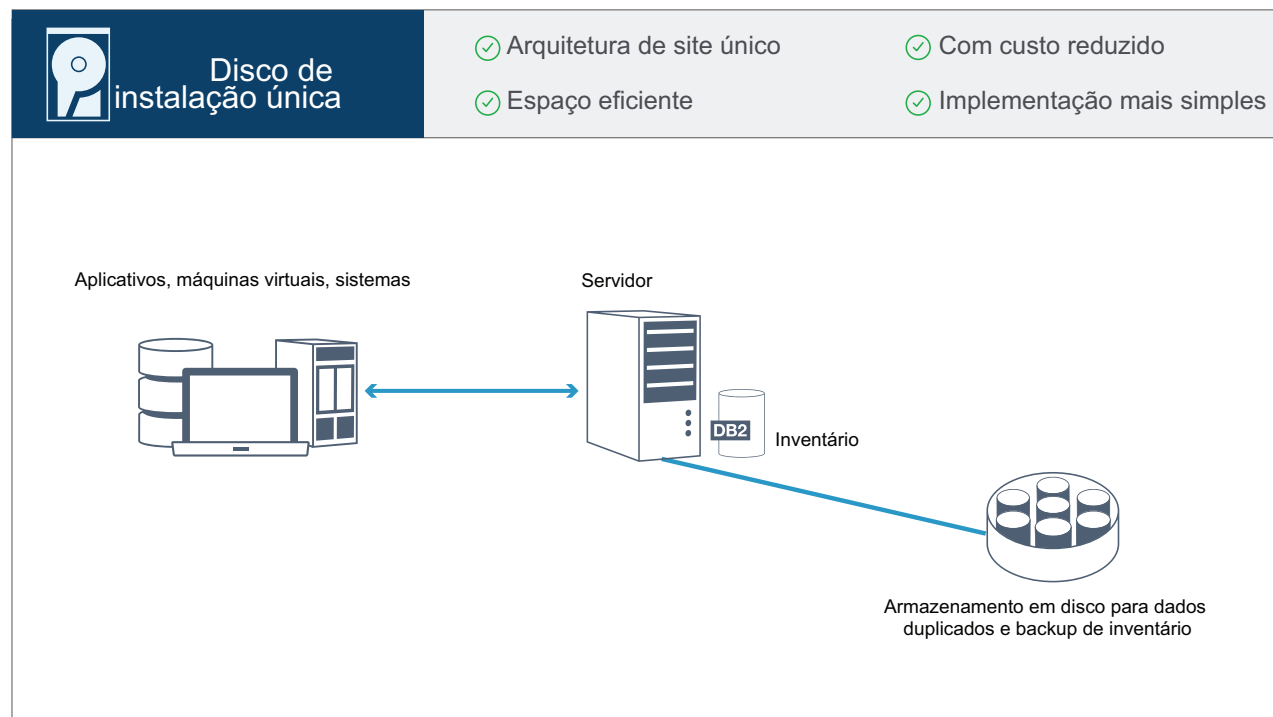
## **Parte 2. Soluções do IBM Spectrum Protect para proteção de dados**

Para ajudar a implementar um ambiente de proteção de dados, revise as informações sobre configurações do IBM Spectrum Protect e selecione a melhor solução para as suas necessidades de negócios.



## Capítulo 4. Implementação baseada em disco de uma solução de proteção de dados para um site único

Essa implementação baseada em disco de uma solução de proteção de dados com o IBM Spectrum Protect usa deduplicação de dados sequencial e fornece proteção para dados em um site único.



Essa solução de proteção de dados fornece os benefícios a seguir:

- Sistema do servidor e hardware de armazenamento em um site único
- Uso com custo reduzido de armazenamento através do recurso de deduplicação de dados
- Solução eficiente em espaço com configuração mínima de hardware
- Implementação mínima que requer instalação e configuração apenas para um servidor e hardware de armazenamento de apoio

Nessa solução, o cliente envia dados para o servidor IBM Spectrum Protect, em que os dados são deduplicados e armazenados em um conjunto de armazenamentos de contêineres de diretório que é implementado em armazenamento em disco. Dados a partir do inventário também têm backup feito para armazenamento em disco. Essa solução é adequada para ambientes de nível de entrada para os quais uma segunda cópia de dados não é necessária.

### Referências relacionadas:

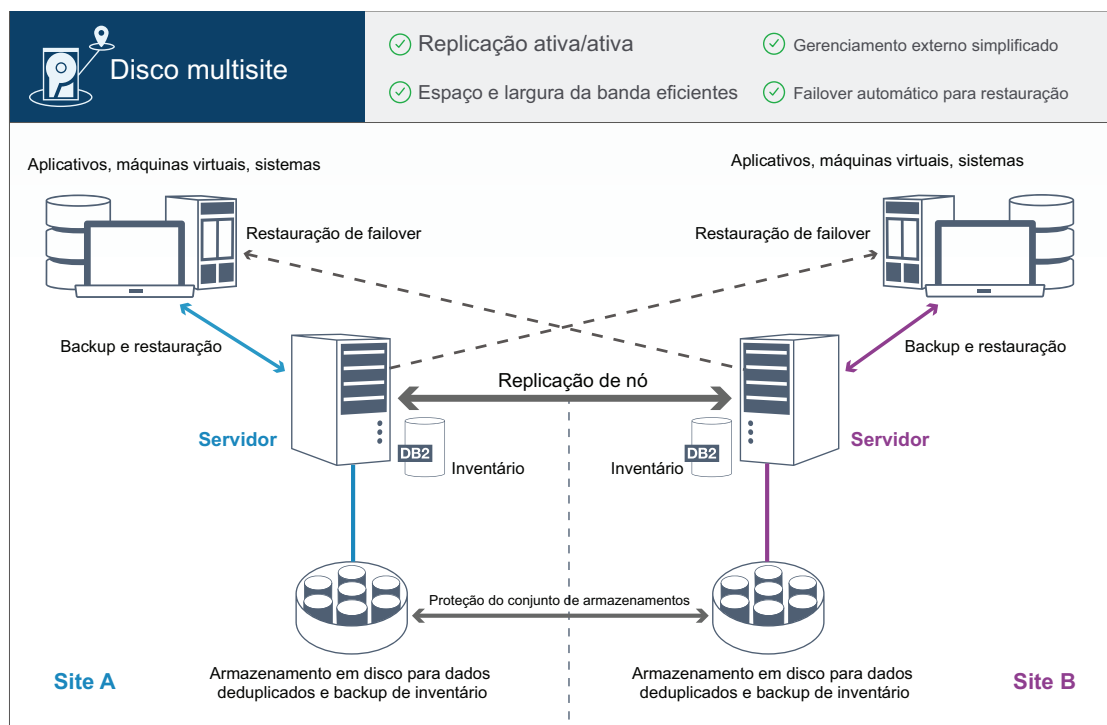
Capítulo 8, “Comparação de soluções de proteção de dados”, na página 53

Capítulo 9, “Roteiro para implementar uma solução de proteção de dados”, na página 55



## Capítulo 5. Implementação baseada em disco de uma solução de proteção de dados para vários sites

Essa implementação baseada em disco de uma solução de proteção de dados com o IBM Spectrum Protect usa deduplicação e replicação de dados sequenciais em dois sites.



Essa solução de proteção de dados fornece os benefícios a seguir:

- A replicação pode ser configurada em ambos os sites de forma que cada servidor proteja dados para o outro site
- O armazenamento de dados externo para cada local é simplificado
- A largura da banda é usada de forma eficiente porque apenas dados deduplicados são replicados entre os sites
- Os clientes podem falhar automaticamente para um servidor de replicação de destino, se o servidor de replicação de origem não estiver disponível

Nessa solução, os clientes enviam dados para o servidor de origem, em que os dados são deduplicados e armazenados em um conjunto de armazenamentos de contêiner de diretório que é implementado no armazenamento em disco. Os dados são replicados para o conjunto de armazenamentos no servidor de destino para cada site. Esta solução é apropriada para ambientes que requerem proteção contra desastres. Se a replicação mútua estiver configurada, os clientes em ambos os sites podem usar recuperação de failover para backups e recuperação de dados continuados a partir do servidor disponível no outro site.

### Referências relacionadas:

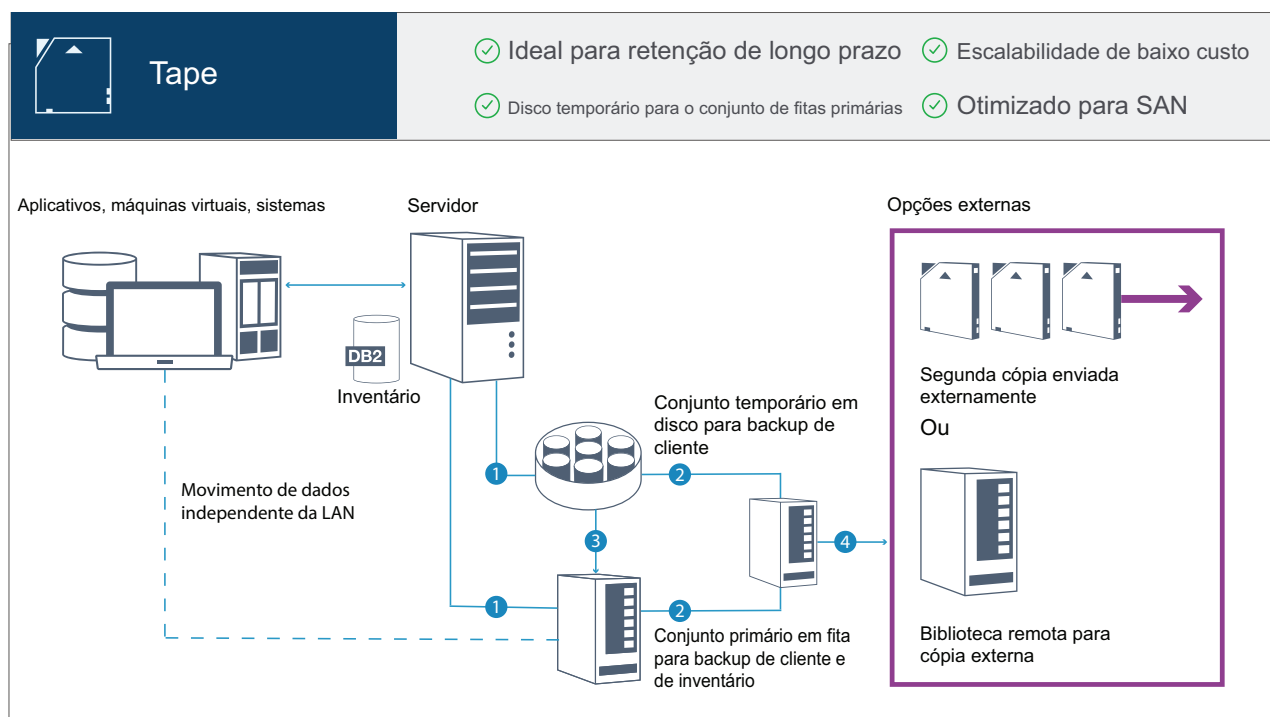
Capítulo 8, "Comparação de soluções de proteção de dados", na página 53

Capítulo 9, “Roteiro para implementar uma solução de proteção de dados”, na página 55



## Capítulo 6. Implementação baseada em fita de uma solução de proteção de dados

Essa implementação de uma solução de proteção de dados com o IBM Spectrum Protect usa um ou mais dispositivos de armazenamento em fita para fazer backup de dados. A fita de backup fornece escalabilidade de baixo custo que é otimizada para retenção a longo prazo.



Essa solução de proteção de dados fornece os benefícios a seguir:

- O desempenho é otimizado para operações de backup em redes de área de armazenamento (SAN) de alta velocidade diretamente na fita para tipos de dados grandes e para retenção de dados de longo prazo.
- A disponibilidade de dados é otimizada armazenando cópias de dados em locais externos para recuperação de desastre. Se você ativar a função de gerenciamento de recuperação de desastre (DRM) e um desastre ocorrer, o DRM ajudará a simplificar o processo de recuperação dos servidores.
- A segurança de dados é otimizada porque cópias de dados são armazenadas externamente em dispositivos de fita que *não* estão conectadas à Internet. Ataques de ransomware dependem de conexões de internet; portanto, o armazenamento externo pode ajudar a proteger contra tais ataques.
- Escalabilidade de baixo custo é obtida reduzindo a necessidade de hardware de disco adicional e diminuindo os custos de energia.

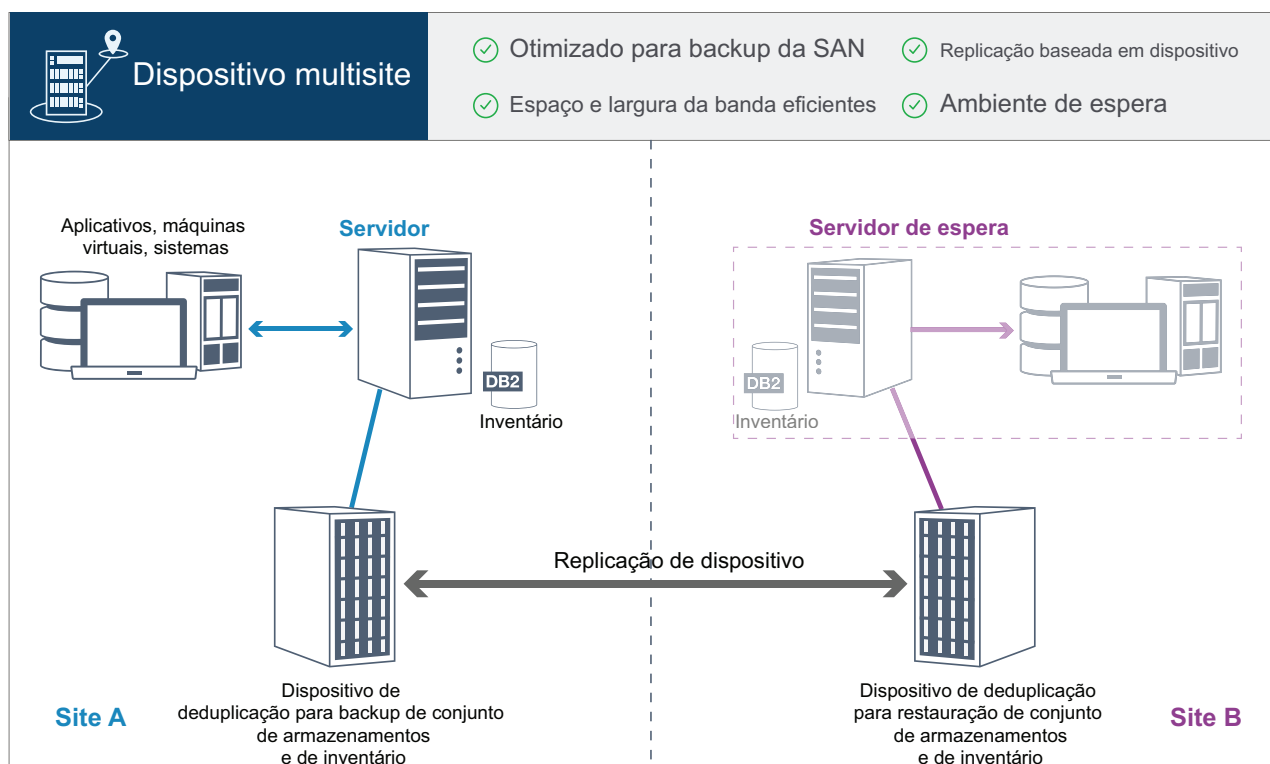
### Referências relacionadas:

Capítulo 8, "Comparação de soluções de proteção de dados", na página 53



## Capítulo 7. Implementação baseada em dispositivo de uma solução de proteção de dados para vários sites

Essa implementação de uma solução de proteção de dados multisite do IBM Spectrum Protect usa deduplicação e replicação de dados com base no dispositivo. Um servidor de espera será configurado em um segundo site para recuperar dados se o servidor principal estiver indisponível.



Essa solução de proteção de dados fornece os benefícios a seguir:

- O desempenho é otimizado para backups em redes de área de armazenamento de alta velocidade (SAN) e para uso com o IBM Spectrum Protect para SAN, quando clientes fazem backup diretamente para dispositivos de fita virtuais conectados à SAN.
- A replicação rápida baseada em dispositivo libera o servidor de ter que rastrear metadados de replicação no banco de dados do servidor.
- Espaços de largura da banda e de armazenamento são usados de forma eficiente, pois apenas dados deduplicados são replicados entre os sites.
- Um ambiente de espera fornece recuperação de desastre, mas não requer a quantidade de recursos necessários para um site totalmente ativo.

Nessa configuração de proteção de dados, o servidor usa dispositivos de hardware para deduplicar e replicar dados. O dispositivo no Site A deduplica dados e, em seguida, replica os dados para o dispositivo no Site B para proteção de desastre. Se ocorrer uma falha no Site A, ative o servidor de espera restaurando o backup de banco de dados mais recente e ativando a cópia de dados replicada.

Para obter informações adicionais sobre como configurar virtual tape libraries, consulte Configurando Virtual Tape Libraries.





**Referências relacionadas:**





Capítulo 8, “Comparação de soluções de proteção de dados”, na página 53

Capítulo 9, “Roteiro para implementar uma solução de proteção de dados”, na página 55

## Capítulo 8. Comparação de soluções de proteção de dados

Compare os recursos-chave de cada solução do IBM Spectrum Protect para determinar qual configuração melhor atende aos seus requisitos de proteção de dados. Em seguida, revise a documentação disponível para implementar a solução.

	Disco de instalação única	Disco multisite	Dispositivo multisite	Tape
				
<b>Destaques</b>				
Custo	\$	\$\$\$	\$\$\$\$	\$\$
Nível de proteção	Uma cópia de dados	Duas ou mais cópias de dados	Duas ou mais cópias de dados	Duas ou mais cópias de dados
Recuperação de desastre	Nenhuma	Servidor ativo	Servidor de espera	Cópias externas
<b>Principais benefícios</b>				
Redução de dados de borda dianteira	✓	✓	✓	✓
Operações de backup e restauração baseadas em disco rápidas e eficientes	✓	✓	✓	
Gerenciamento externo simplificado		✓		
Recurso de deduplicação de dados sem custo extra	✓	✓		
Processamento de replicação incluído sem nenhum encargo adicional		✓		
Deduplicação de dados nos servidores de origem e de destino		✓		
Escalabilidade de baixo custo e otimizada para retenção de longo prazo				✓
<b>Eficiência e custo</b>				
Otimizado para operações de backup de rede de área de armazenamento (SAN) de alta velocidade			✓	✓
Otimizado para rede local (LAN) de alta velocidade	✓	✓	✓	
Deduplicação de dados global em todos os tipos e origens de dados	✓	✓	✓	
Replicação eficiente de largura da banda		✓	✓	
Custos de energia mais baixos				✓
Opção para uma segunda cópia sem hardware de disco extra				✓
<b>Disponibilidade</b>				

	Disco de instalação única	Disco multisite	Dispositivo multisite	Tape
				
Recurso de cópia externa		✓	✓	✓
Replicação baseada em dispositivo			✓	
Recuperação do cliente a partir do servidor de alta disponibilidade		✓		
Destino de replicação na nuvem		✓		
Gerenciamento independente de políticas de retenção para dados de replicação; capacidade para manter mais ou menos dados no site de recuperação		✓		
Replicação em nível do aplicativo; capacidade para escolher quais sistemas e aplicativos serão replicados		✓		
<b>Escalabilidade</b>				
Deduplicação de dados globais em servidores			✓	
Backup otimizado para SAN diretamente na fita para tipos de dados grandes				✓
Escalabilidade de petabyte de instância única				✓

## O que fazer a seguir

Revise a documentação disponível para as soluções em Capítulo 9, “Roteiro para implementar uma solução de proteção de dados”, na página 55.

### Referências relacionadas:

Capítulo 4, “Implementação baseada em disco de uma solução de proteção de dados para um site único”, na página 45

Capítulo 5, “Implementação baseada em disco de uma solução de proteção de dados para vários sites”, na página 47

Capítulo 7, “Implementação baseada em dispositivo de uma solução de proteção de dados para vários sites”, na página 51

Capítulo 6, “Implementação baseada em fita de uma solução de proteção de dados”, na página 49

---

## Capítulo 9. Roteiro para implementar uma solução de proteção de dados

Planeje e implemente a solução de proteção de dados mais adequada para o seu ambiente de negócios com o IBM Spectrum Protect.

### Solução de disco de instalação única

Para obter as etapas que descrevem como planejar, implementar, monitorar e operar uma solução de disco de instalação única, consulte Solução de disco de único site.

### Solução de disco multisite

Para obter as etapas que descrevem como planejar, implementar, monitorar e operar uma solução de disco multisite, consulte Solução de disco multisite.

### Solução de fita

Para obter as etapas que descrevem como planejar, implementar, monitorar e operar uma solução de dispositivo de fita, consulte Solução de fita.

### Solução de dispositivo multisite

Para obter uma visão geral das tarefas que são necessárias para implementar uma solução de dispositivo de vários sites, revise as etapas a seguir:

1. Comece a planejar a solução revisando as informações nos seguintes links:
  - AIX: Planejamento de Capacidade
  - Linux: Planejamento de Capacidade
  - Windows: Planejamento de Capacidade
2. Instale o servidor e, opcionalmente, o Operations Center. Revise as informações nos seguintes links:
  - Instalando e Atualizando o Servidor
  - Instalando e fazendo upgrade do Operations Center
3. Configure o servidor para armazenamento em uma biblioteca de fitas virtual.
  - Gerenciando bibliotecas de fitas virtuais
  - Conectando dispositivos de fita para o servidor

Para obter orientação sobre como melhorar o desempenho do sistema, consulte Melhores Práticas de Configuração.
4. Configure políticas para proteger seus dados. Revise as informações em Customizando políticas.
5. Configure planejamentos de cliente. Revise as informações em Planejando backup e as operações de archive.
6. Instale e configure clientes. Para determinar o tipo de software cliente que é necessário, revise as informações em Incluindo clientes para obter detalhes.
7. Configure o monitoramento para seu sistema. Revise as informações em Monitorando soluções de armazenamento.

#### Referências relacionadas:

Capítulo 8, “Comparação de soluções de proteção de dados”, na página 53

Capítulo 4, “Implementação baseada em disco de uma solução de proteção de dados para um site único”, na página 45

Capítulo 5, “Implementação baseada em disco de uma solução de proteção de dados para vários sites”, na página 47

Capítulo 7, “Implementação baseada em dispositivo de uma solução de proteção de dados para vários sites”, na página 51

Capítulo 6, “Implementação baseada em fita de uma solução de proteção de dados”, na página 49



---

## Parte 3. Apêndices



---

## Apêndice. 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/](http://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](http://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/](http://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/releasesnotes.html?view=kc#accessibility](http://www.ibm.com/support/knowledgecenter/about/releasesnotes.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](http://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 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](http://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](http://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

## A

API

*Veja* interface de programação de aplicativos

aplicativos clientes 5

armazenamento

conceitos 3

conjuntos 3, 15, 20

dispositivos 3, 15

gerenciamento de 27

hierarquia 3, 27

objetos 15

redes 27

representações 15

suporte de dispositivo para 27

tipos 15

volumes 20

arquitetura de SAN 35, 40

## B

backup incremental progressivo 33

biblioteca 15

## C

camada

físico 15

lógico 15

caminho 15

classe de dispositivo 15

clientes

aplicativos 5

clientes do sistema 5

conceitos 3

máquinas virtuais 5

nós clientes 3

software cliente 3

tipos de 5

clientes do sistema 5

conceitos

armazenamento 3

banco de dados 3

clientes 3

inventário 3

log de recuperação 3

servidor 3

visão geral 3

conjuntos de armazenamentos

contêiner 20, 33

cópia 20

cópia de contêiner 20

dados do archive 20

nuvem 20

primário 20

representação 20

tipos de 20

conjuntos de armazenamentos de contêiner 33

conjuntos de armazenamentos de contêiner de diretório 20

conjuntos de armazenamentos de contêiner em nuvem 20

conjuntos de armazenamentos de cópia 20

conjuntos de armazenamentos de cópia de contêiner 20

conjuntos de armazenamentos de dados ativos 20

conjuntos de armazenamentos primários 20

conjuntos de dados ativos 27

## D

dados de cliente

consolidação de 27

criar um conjunto de backup para 27

gerenciamento de 27

migração de 27

movendo para o armazenamento 27

deduplicação de dados

lado do cliente 33

lado do servidor 33

sequencial 33

deduplicação de dados sequenciais 33

deficiência 59

disposição 27

dispositivos de fita

físico 15

virtual 15

## F

failover, automático 40

## G

gerenciamento da segurança

registro aberto 7, 27

registro fechado 7, 27

senhas 7, 27

SSL 7, 27

TLS 7, 27

GUI, para clientes 11

## I

IBM Knowledge Center v

instruções SQL, acessar o banco de dados do servidor 11

interface da linha de comandos 11

interface da web, para cliente de backup-archive 11

interface de programação de aplicativos 11

interfaces

API 11

cliente de backup-archive 11

GUI do cliente 11

instruções SQL 11

linha de comandos 11

operations center 11

inventário 7

## K

Knowledge Center v

## L

- log
  - espelho de log 7
  - log ativo 7
  - log de archive 7
  - log de failover de archive 7
  - log de recuperação 7
- log de recuperação 7

## M

- máquinas virtuais 5
- mídia
  - recuperação de 27
- mídia, removível 15
- movedor de dados 15

## O

- operations center
  - acesso a 11
  - funções 11

## P

- política
  - conjunto de políticas 7
  - domínio de política 7
  - gerenciamento de dados por 7
  - padrão 7
- proteção de dados
  - estratégias 33
- publicações v

## R

- recuperação
  - componentes do sistema 40
  - dados 40
- recuperação de desastre
  - DRM 40
  - failover automático 40
  - gerenciador 40
  - medidas preventivas 40
  - métodos 35
- recursos de acessibilidade 59
- rede, tipos de
  - Armazenamento conectado à rede 27
  - LAN 27
  - NAS 27
  - SAN 27
  - sem a LAN 27
- replicação
  - função na recuperação de desastre 35
  - nó 35
  - servidor de destino 35
  - servidor de origem 35
- replicação de dispositivo 35, 40
- replicação de nó 35, 40

## S

- server 15
- serviço de archive 5

- serviço de backup 5
- serviço de migração 5
- serviço de rechamada 5
- serviço de recuperação 5
- serviço de restauração 5
- serviços
  - arquivar e recuperar 5
  - backup e restauração 5
  - migrar e rechamar 5
- serviços de proteção de dados 5
- servidor
  - armazenamentos de dados 7
  - conceitos 3
  - inventário 7
  - log de recuperação 7
- sistemas operacionais 5
- Sobre esta publicação v
- soluções
  - solução multisite
    - baseada em dispositivo 51
  - soluções de proteção de dados
    - baseada em dispositivo 51
- Soluções do IBM Spectrum Protect
  - roteiro 55
  - solução de instalação única
    - baseado em disco 45
  - solução multisite
    - baseado em disco 47
  - soluções de proteção de dados 49
    - comparação 53
    - disco de instalação única 45
    - disco multisite 47

## T

- teclado 59
- transporte de fita 35, 40

## U

- unidade 15

## V

- volume 15
- volumes 20





Número do Programa: 5725-W98  
5725-W99  
5725-X15

Impresso no Brasil