# Documentação do software SANtricity 11,80

SANtricity 11.8

NetApp
December 16, 2024

# Índice

# Documentação do software SANtricity 11,80

# Notas de lançamento

## Novidades no SANtricity os 11,80

A tabela a seguir descreve os novos recursos no Gerenciador de sistema do SANtricity 11,8.

### Novos recursos na versão 11.80.1R1

| Novo recurso | Descrição |
| --- | --- |
| Aumento do tamanho da chave dos novos certificados de gerenciamento autoassinados e assinados pela CA. | O comprimento do tamanho da chave do certificado de gerenciamento para o SANtricity System Manager e o certificado autoassinado pelos aplicativos do Unified Manager foi modificado de 2048 para 3072 bits. A alteração se aplica a certificados autoassinados e assinados pela CA recém-gerados dos aplicativos SANtricity. O comprimento da chave é fixo e não é afetado pelas definições de tamanho de chave padrão na NVSRAM. |

### Novos recursos na versão 11.80.1

| Novo recurso | Descrição |
| --- | --- |
| `-identifyDevices` parâmetro | Um novo `-identifyDevices` parâmetro está agora disponível no SMcli. Esse novo parâmetro permite que você procure todos os dispositivos de bloco nativo SCSI associados aos storages de armazenamento. Para obter mais informações, "Parâmetros da linha de comando SMcli para download"consulte . |
| Estatísticas do Kernel Ethernet | Uma nova opção de Estatísticas do Kernel Ethernet está agora disponível na página Ver Pacotes de Estatísticas iSCSI no System Manager. Esta nova opção permite visualizar estatísticas para os controladores de kernel da plataforma do dispositivo iSCSI. Para obter mais informações, "Visualizar Pacotes de Estatísticas iSCSI"consulte . |
| Adicionada capacidade de bloquear endereços IP por meio do endpoint da API REST | Os usuários agora podem bloquear endereços IP específicos através do endpoint Configurações (`/devmgr/v2/settings`). Uma vez configurado através do endpoint Settings (Definições), apenas os endereços IP especificados através de uma lista branca podem comunicar com o dispositivo de armazenamento. Este novo recurso suporta listas de endereços IPv4 e IPv6. |
| Plug-in do vCenter Storage | O plug-in do vCenter Storage foi atualizado para compatibilidade com a versão e-Series 11.80.1. |
| Proxy de serviços Web | O Web Services Proxy foi atualizado para a versão 6,1 para compatibilidade com a versão e-Series 11.80.1. |

## Novos recursos na versão 11,80

| Novo recurso | Descrição |
| --- | --- |
| Análise de paridade de volume melhorada | A verificação de paridade de volume agora pode ser iniciada como um processo em segundo plano, seja através da API REST ou via CLI. A digitalização de paridade resultante será executada em segundo plano, desde que seja necessário para concluir a operação de digitalização. As operações de digitalização sobreviverão às reinicializações e operações de failover do controlador. |
| Suporte a SAML para Unified Manager | O Unified Manager agora é compatível com SAML (Security Assertion Markup Language). Depois que o SAML estiver habilitado para o Unified Manager, os usuários devem usar a autenticação multifator contra o provedor de identidade para interagir com a interface do usuário. Observe que uma vez que o SAML está habilitado no Unified Manager, a API REST não pode ser usada sem passar pelo IDP para autenticar solicitações. |
| Funcionalidade de configuração automática | Agora suporta a capacidade de definir o parâmetro tamanho do bloco de volume a ser usado com o recurso Configuração automática para configuração inicial do array. Este recurso está disponível na CLI apenas como um parâmetro "blocksize". |
| Assinatura criptográfica do firmware do controlador | O firmware da controladora é assinado criptograficamente. As assinaturas são verificadas durante o download inicial e em cada inicialização do controlador. Nenhum impactos esperado do usuário final. As assinaturas são apoiadas por um certificado de Validação estendida emitido pela CA. |
| Assinatura criptográfica do firmware da unidade | O firmware da unidade é assinado criptograficamente. As assinaturas são verificadas durante o download inicial e apoiadas por um certificado de Validação estendida emitido pela CA. O conteúdo do firmware da unidade agora é fornecido como um arquivo ZIP, que contém o firmware não assinado mais antigo, bem como o novo firmware assinado. O usuário deve escolher o arquivo apropriado com base na versão de lançamento do código que está sendo executado no sistema de destino. |

| Novo recurso | Descrição |
| --- | --- |
| Gerenciamento do servidor de chaves externo - tamanho da chave do certificado | O novo tamanho padrão da chave do certificado é de 3072 bits (de 2048). Tamanhos de chave até 4096 bits são suportados. Um bit NVSRAM deve ser alterado para suportar os tamanhos de chave não padrão.<br><br>Os valores de seleção do tamanho da chave são os seguintes:<br><br>• PADRÃO: 0<br>• COMPRIMENTO 2048: 1CM<br>• COMPRIMENTO 3072: 2CM<br>• COMPRIMENTO 4096: 3CM<br><br>Para alterar o tamanho da chave para 4096 através do SMcli:<br><br>`set controller[b] globalnvsrambyte[0xc0]=3;`<br>`set controller[a] globalnvsrambyte[0xc0]=3;`<br><br>Interrogar o tamanho da chave:<br><br>`show allcontrollers globalnvsrambyte[0xc0];` |
| Melhorias no pool de discos | Os pools de discos criados com controladores executando 11,80 ou acima serão *Version 1* pools em vez de *Version 0* pools. Uma operação de downgrade é restrita quando um pool de discos *Version 1* existe.<br><br>A versão de um pool de discos pode ser identificada no perfil do storage array. |
| O System Manager e o Unified Manager não serão iniciados a menos que os requisitos mínimos do navegador sejam atendidos | É necessária uma versão mínima do navegador antes de o System Manager ou o Unified Manager serem iniciados. A seguir estão as versões mínimas suportadas:<br><br>• Firefox versão mínima 80<br>• Chrome versão mínima 89<br>• Edge versão mínima 90<br>• Safari versão mínima 14 |
| Suporte para unidades SSD NVMe FIPS 140-3 | Agora, as unidades SSD NVMe FIPS 140-3 com certificação NetApp são compatíveis. Eles serão corretamente identificados como tal no perfil do storage array e no System Manager. |
| Suporte para cache de leitura SSD em EF300 e EF600 | O cache de leitura SSD agora é suportado em controladores EF300 e EF600 usando HDD com expansão SAS. |

| Novo recurso | Descrição |
| --- | --- |
| Suporte para espelhamento remoto assíncrono iSCSI e Fibre Channel em EF300 e EF600 | O espelhamento remoto assíncrono (ARVM) agora é compatível com controladoras EF300 e EF600 com volumes baseados em NVMe e SAS. |
| Suporte a EF300 TB e EF600 TB sem unidades na bandeja de base | As configurações de controladora EF300 e EF600 sem unidades NVMe na bandeja base agora são compatíveis. |
| Portas USB desativadas para todas as plataformas | As portas USB estão agora desativadas em todas as plataformas. |

# Notas de lançamento

Notas de versão estão disponíveis fora deste site. Você será solicitado a fazer login usando suas credenciais do site de suporte da NetApp.

- "11,80 Notas de lançamento"
- "11,70 Notas de lançamento"
- "11,60 Notas de lançamento"
- "11,50 Notas de lançamento"

# Comece agora

## Visão geral do software SANtricity

Os sistemas e-Series incluem o software SANtricity para provisionamento de storage e outras tarefas.

Este site descreve como usar as seguintes interfaces de gerenciamento do SANtricity:

- System Manager — uma interface baseada na Web usada para gerenciar um storage array individual em sua rede.
- Unified Manager — uma interface baseada na Web usada para visualizar e gerenciar todos os storages de armazenamento em sua rede.

Os storage arrays EF600 e EF300 não são compatíveis com espelhamento síncrono ou thin volumes.

### Gerente do sistema da SANtricity

O System Manager é um software de gerenciamento baseado na Web incorporado a cada controlador. Para acessar a interface do usuário, aponte um navegador para o endereço IP do controlador. Um assistente de configuração ajuda você a começar com a configuração do sistema.

O System Manager oferece uma variedade de recursos de gerenciamento, incluindo:

| |
|---|
|  **Desempenho** |
| Visualize até 30 dias de dados de performance, incluindo latência de e/S, IOPS, utilização de CPU e taxa de transferência. |
|  **Armazenamento** |
| Provisione storage usando pools ou grupos de volumes e crie workloads de aplicações. |
|  **Proteção de dados** |
| Realizar backup e recuperação de desastres usando snapshots, cópia de volume e espelhamento remoto. |

| |
|---|
|  **Hardware** |
| Verifique o status do componente e execute algumas funções relacionadas a esses componentes, como a atribuição de unidades hot spare. |
|  **Alertas** |
| Notifique os administradores sobre eventos importantes que ocorrem no storage array. Os alertas podem ser enviados por e-mail, traps SNMP e syslog. |
|  **Gerenciamento de Acesso** |
| Configure a autenticação de usuário que exige que os usuários façam login no sistema com credenciais atribuídas. |
|  **Configurações do sistema** |
| Configure outros recursos de desempenho do sistema, como cache SSD e balanceamento automático de toload. |
|  **Suporte** |
| Visualize dados de diagnóstico, gerencie atualizações e configure o AutoSupport, que monitora a integridade de um storage array e envia patches automáticos para o suporte técnico. |

## Gerenciador unificado do SANtricity

O Unified Manager é um software baseado na Web usado para gerenciar todo o seu domínio. Em uma visualização central, você vê o status de todos os arrays e-Series e EF-Series mais recentes, como E2800, EF280, EF300, E5700, EF570 e EF600. Você também pode executar operações em lote em matrizes de armazenamento selecionadas.

O Unified Manager é instalado em um servidor de gerenciamento juntamente com o Web Services Proxy. Para

acessar o Unified Manager, abra um navegador e insira o URL apontando para o servidor onde o Proxy de Serviços Web está instalado.

O Unified Manager oferece uma variedade de recursos de gerenciamento, incluindo:

| |
|---|
|  **Descubra matrizes de armazenamento** |
| Localize e adicione os storages de armazenamento que você deseja gerenciar na rede da sua organização. Em seguida, você pode exibir o status de todos os storages de armazenamento de uma única página. |
|  **Lançamento** |
| Abra uma instância do System Manager para executar operações de gerenciamento individuais em um array de storage específico. |
|  **Importar configurações** |
| Execute uma importação em lote de um storage array para vários arrays, incluindo configurações de alertas, AutoSupport e serviços de diretório. |
|  **Espelhamento** |
| Configurar pares espelhados assíncronos ou síncronos entre dois storage arrays. |
|  **Gerenciar grupos** |
| Organize matrizes de armazenamento em grupos para facilitar o gerenciamento. |

| |
|---|
|  **Centro de Atualização** |
| Atualizar o software SANtricity os em vários arrays de storage. |
|  **Certificados** |
| Crie solicitações de assinatura de certificado (CSRs), importe certificados e gerencie certificados existentes para vários storages de storage. |
|  **Gerenciamento de Acesso** |
| Configurar a autenticação de usuário que exige que os usuários façam login no Unified Manager com credenciais atribuídas. |

# Navegadores e sistemas operacionais suportados

O software SANtricity suporta vários tipos de navegadores e sistemas operacionais.

## Navegadores

Os seguintes navegadores e versões são suportados.

| Navegador | Versão mínima |
|---|---|
| Google Chrome | 89 |
| Mozilla Firefox | 80 |
| Safari | 14 |
| Microsoft Edge | 90 |

Para o Unified Manager, o Proxy de serviços da Web deve estar instalado e disponível para o navegador. Para obter mais informações, consulte "Visão geral do proxy dos serviços da Web da SANtricity"

## Sistemas operacionais

Os seguintes sistemas operacionais e versões são suportados.

| Sistema operacional | Versão/arquitetura mínima |
|---|---|
| Red Hat Enterprise Linux (RHEL) | 7.x, 8.x / 64 bits |
| SUSE Linux Enterprise Server (SLES) | 12.x, 15.x / 64 bits |
| Oracle Linux (OL) | 7.x, 8.x / 64 bits |
| Windows Server | 2016, 2019, 2022 / 64 bits |
| Ubuntu | 18,04, 20,04 / 64 bits |

# Configuração do System Manager

## Acesse o System Manager

Para acessar a interface do usuário do System Manager, você aponta um navegador para o endereço IP do controlador. Um assistente de configuração ajuda você a começar com a configuração do sistema.

**Antes de começar**

- Instale e configure o hardware, conforme descrito em um dos guias de configuração expressos:
  - "Configuração expressa do Linux"
  - "Configuração do VMware Express"
  - "Configuração expressa do Windows"
- Configure uma estação de gerenciamento que atenda aos seguintes requisitos:
  - Ligado a uma rede de 1 Gbps ou mais rápida.
  - Anexado à mesma sub-rede que as portas de gerenciamento de armazenamento.
  - Usado como uma estação separada, em vez de um host (e/S anexado) usado para gerenciamento de dados.
  - Configure o gerenciamento fora da banda, no qual uma estação de gerenciamento de storage envia comandos ao sistema de storage por meio das conexões Ethernet ao controlador.
  - Configurar com um navegador suportado. "Navegadores e sistemas operacionais suportados"Consulte .

**Passos**

1. No seu navegador, insira o seguinte URL: `https://<IPAddress>`

   `IPAddress` é o endereço de uma das controladoras de storage array.

   Na primeira vez que o System Manager é aberto em uma matriz que não foi configurada, o prompt Set Administrator Password (Definir senha do administrador) é exibido.

2. Introduza a palavra-passe do Gestor do sistema para a função de administrador nos campos Definir palavra-passe do administrador e confirmar palavra-passe e, em seguida, clique em **Definir palavra-passe**.

   O assistente de configuração é iniciado no início de sessão pela primeira vez.

3. Use o assistente de configuração para executar as seguintes tarefas:
   - **Verifique o hardware (controladores e unidades)** — Verifique o número de controladores e unidades no storage de armazenamento. Atribua um nome à matriz.
   - **Verifique hosts e sistemas operacionais** — Verifique os tipos de host e sistema operacional que o storage array pode acessar.
   - **Accept pools** — aceite a configuração de pool recomendada para o método de instalação expressa. Um pool é um grupo lógico de unidades.
   - **Configurar alertas** — permitir que o System Manager receba notificações automáticas quando ocorrer um problema com a matriz de armazenamento.
   - * Ativar AutoSupport* — monitore automaticamente a integridade do seu storage array e tenha despachos enviados para o suporte técnico.

Para obter mais informações sobre o Assistente de configuração, "Descrição geral do Assistente de configuração"consulte .

## Descrição geral do assistente de configuração

Use o assistente de configuração para configurar seu storage array, incluindo hardware, hosts, aplicativos, workloads, pools, alertas e AutoSupport.

### Configuração pela primeira vez

Quando abre o System Manager pela primeira vez, o assistente de configuração é iniciado. O assistente de configuração solicita que você execute tarefas básicas de configuração, como nomear sua matriz de armazenamento, configurar seus hosts, selecionar aplicativos e criar pools de armazenamento.

> Antes de continuar com a configuração inicial, vá para a Central de Atualização (**suporte › Centro de Atualização**) e certifique-se de que o software SANtricity os está atualizado. Se necessário, atualize para a versão mais recente e atualize o navegador para continuar a configuração. Para obter mais informações, "Visão geral do Centro de atualizações"consulte .

Se você cancelar o assistente, não será possível reiniciá-lo manualmente. O assistente reinicia automaticamente quando você abre o System Manager ou atualiza o navegador e *pelo menos uma* das seguintes condições é atendida:

- Não foram detetados pools e grupos de volume.
- Nenhuma carga de trabalho é detetada.
- Nenhuma notificação está configurada.

### Terminologia

O assistente de configuração usa os seguintes termos.

| Prazo | Descrição |
| --- | --- |
| Aplicação | Um aplicativo é um programa de software, como o Microsoft SQL Server ou o Microsoft Exchange. |
| Alerta | Os alertas notificam os administradores sobre eventos importantes que ocorrem nos storage arrays. Os alertas podem ser enviados por e-mail, traps SNMP ou syslog. |
| AutoSupport | O recurso AutoSupport monitora a integridade de um storage array e envia patches automáticos para o suporte técnico. |
| Hardware | O hardware do sistema de storage inclui storage arrays, controladores e unidades. |
| Host | Um host é um servidor que envia e/S para um volume em um storage array. |
| Objeto | Um objeto é qualquer componente de storage lógico ou físico. Os objetos lógicos incluem grupos de volumes, pools e volumes. Os objetos físicos incluem o storage array, controladores de array, hosts e unidades. |
| Piscina | Um pool é um conjunto de unidades que é agrupado logicamente. Você pode usar um pool para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um pool ou de um grupo de volumes.) |
| Volume | Um volume é um contêiner no qual aplicativos, bancos de dados e sistemas de arquivos armazenam dados. É o componente lógico criado para que o host acesse o storage no storage array.<br><br>Um volume é criado a partir da capacidade disponível em um pool ou em um grupo de volumes. Um volume tem uma capacidade definida. Embora um volume possa consistir em mais de uma unidade, um volume aparece como um componente lógico para o host. |
| Grupo de volume | Um grupo de volumes é um contentor para volumes com caraterísticas compartilhadas. Um grupo de volumes tem uma capacidade definida e um nível RAID. Você pode usar um grupo de volumes para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um grupo de volumes ou de um pool.) |
| Workload | Um workload é um objeto de storage compatível com uma aplicação. Você pode definir uma ou mais cargas de trabalho ou instâncias por aplicação. Para alguns aplicativos, o sistema configura a carga de trabalho para conter volumes com caraterísticas de volume subjacentes semelhantes. Essas características de volume são otimizadas com base no tipo de aplicação compatível com o workload. Por exemplo, se você criar uma carga de trabalho que suporte um aplicativo Microsoft SQL Server e, posteriormente, criar volumes para essa carga de trabalho, as caraterísticas de volume subjacentes serão otimizadas para oferecer suporte ao Microsoft SQL Server. |

## FAQs

**E se eu não vir todos os meus componentes de hardware?**

Se você não vir todos os componentes de hardware na caixa de diálogo verificar hardware, isso pode significar que um compartimento de unidade não está conetado corretamente ou que um compartimento incompatível está instalado no storage de armazenamento.

Verifique se todos os compartimentos de unidades estão conetados corretamente. Se você não tiver certeza sobre quais gavetas de unidade são compatíveis, entre em Contato com o suporte técnico.

**E se eu não ver todos os meus anfitriões?**

Se você não vir seus hosts conetados, a deteção automática falhou, os hosts estão conetados incorretamente ou nenhum host está conetado atualmente.

Você pode configurar os hosts mais tarde, uma vez que você terminar com a configuração. Você pode criar hosts manualmente da seguinte forma:

- Você pode criar manualmente hosts e associar os identificadores de porta de host apropriados acessando o **armazenamento › hosts**. Os hosts que foram criados manualmente também são exibidos no assistente **Initial Setup**.
- O destino e o host devem ser configurados para o tipo de porta do host (por exemplo, iSCSI ou NVMe sobre RoCE) e uma sessão para o storage estabelecida antes que a deteção automática funcione.

**Como a identificação de aplicativos me ajuda a gerenciar meu storage array?**

Quando você identifica aplicações, o System Manager recomenda automaticamente uma configuração de volume que otimiza o storage com base no tipo de aplicação.

Otimizar volumes por aplicação pode tornar as operações de storage de dados mais eficientes. Caraterísticas como tipo de e/S, tamanho do segmento, propriedade do controlador e cache de leitura e gravação estão incluídas na configuração do volume. Além disso, você pode visualizar os dados de performance por aplicação e workload para avaliar a latência, IOPS e MIB/s das aplicações e seus workloads associados.

**O que é uma carga de trabalho?**

Para alguns aplicativos em sua rede, como SQL Server ou Exchange, você pode definir uma carga de trabalho que otimiza o armazenamento para esse aplicativo.

Um workload é um objeto de storage compatível com uma aplicação. Você pode definir uma ou mais cargas de trabalho ou instâncias por aplicação. Para alguns aplicativos, o sistema configura a carga de trabalho para conter volumes com caraterísticas de volume subjacentes semelhantes. Essas características de volume são otimizadas com base no tipo de aplicação compatível com o workload. Por exemplo, se você criar uma carga de trabalho que suporte um aplicativo Microsoft SQL Server e, posteriormente, criar volumes para essa carga de trabalho, as caraterísticas de volume subjacentes serão otimizadas para oferecer suporte ao Microsoft SQL Server.

Durante a criação de volume, o sistema solicita que você responda a perguntas sobre o uso de uma carga de trabalho. Por exemplo, se você estiver criando volumes para o Microsoft Exchange, será perguntado quantas caixas de correio você precisa, quais são seus requisitos médios de capacidade de caixa de correio e quantas

cópias do banco de dados deseja. O sistema usa essas informações para criar uma configuração de volume ideal para você, que pode ser editada conforme necessário.

#### Como faço para configurar o método de entrega para o AutoSupport?

Para acessar as tarefas de configuração para os métodos de entrega do AutoSupport, vá para o **suporte › Centro de suporte** e clique na guia **AutoSupport**.

Os seguintes protocolos são suportados: HTTPS, HTTP e SMTP.

#### Como sei se devo aceitar a configuração recomendada do pool?

Se você aceitar a configuração de pool recomendada depende de alguns fatores.

Determine o tipo de armazenamento mais adequado aos seus requisitos respondendo às seguintes perguntas:

- Você prefere vários pools de capacidades menores, em vez dos maiores pools possíveis?
- Você prefere grupos de volume RAID em pools?
- Você prefere provisionar manualmente suas unidades, em vez de ter uma configuração recomendada para você?

Se você respondeu Sim a qualquer uma dessas perguntas, considere rejeitar a configuração recomendada do pool.

#### O System Manager não detetou nenhum host. O que faço?

Se você não vir seus hosts conetados, a deteção automática falhou, os hosts estão conetados incorretamente ou nenhum host está conetado atualmente.

Você pode configurar os hosts mais tarde, uma vez que você terminar com a configuração. Você pode criar hosts manualmente da seguinte forma:

- Você pode criar manualmente hosts e associar os identificadores de porta de host apropriados acessando o **armazenamento › hosts**. Os hosts que foram criados manualmente também são exibidos no assistente **Initial Setup**.
- O destino e o host devem ser configurados para o tipo de porta do host (por exemplo, iSCSI ou NVMe sobre RoCE) e uma sessão para o storage estabelecida antes que a deteção automática funcione.

# Configuração do Unified Manager

## Instale o Unified Manager

O Unified Manager está incluído no Proxy de serviços da Web, que é um servidor de API RESTful instalado separadamente em um sistema host para gerenciar os sistemas de storage NetApp e-Series.

Para instalar o Proxy de serviços da Web e o Gerenciador Unificado, consulte as instruções a seguir no centro de documentação e-Series e SANtricity:

1. "Reveja os requisitos de instalação e atualização"
2. "Baixe e instale o arquivo Proxy de serviços da Web"

## Acesse o Unified Manager

Depois de instalar o Web Services Proxy, você pode acessar o Unified Manager para gerenciar vários sistemas de armazenamento em uma interface baseada na Web.

Para navegadores compatíveis, "Navegadores e sistemas operacionais suportados"consulte .

**Passos**

1. Abra um navegador e insira o seguinte URL:

   `http[s]://<server>:<port>/um`

   Neste URL, `<server>` representa o endereço IP ou FQDN do servidor onde o Proxy de Serviços Web está instalado e `<port>` representa o número da porta de escuta (o padrão é 8080 para HTTP ou 8443 para HTTPS).

   A página de login do Unified Manager será aberta.

2. Para iniciar sessão pela primeira vez, introduza `admin` o nome de utilizador e, em seguida, defina e confirme uma palavra-passe para o utilizador admin.

   A senha pode incluir até 30 carateres.

Para obter mais informações sobre usuários e senhas, "Como o Gerenciamento de Acesso funciona"consulte .

# Gerenciamento de array único com System Manager 11,8

## Interface principal

### Visão geral da interface do System Manager

O System Manager é uma interface baseada na Web que permite gerenciar um storage array em uma única visualização.

#### Página inicial

A página inicial fornece uma visualização de painel para o gerenciamento diário de seu storage array. Ao iniciar sessão no System Manager, a página inicial é a primeira tela exibida.

A visualização do dashboard compreende quatro áreas de resumo que contêm informações importantes sobre o estado e a integridade do storage array. Pode encontrar mais informações na área de resumo.

| Área | Descrição |
| --- | --- |
| Notificações | A área notificações exibe notificações de problemas que indicam o status do storage array e seus componentes. Além disso, esse portlet exibe alertas automatizados que podem ajudar você a solucionar problemas antes que isso afete outras áreas do seu ambiente de storage. |
| Desempenho | A área desempenho permite comparar e contrastar o uso de recursos ao longo do tempo. É possível visualizar as métricas de desempenho de um storage array para tempo de resposta (IOPS), taxas de transferência (MIB/s) e a quantidade de capacidade de processamento usada (CPU). |
| Capacidade | A área capacidade exibe uma visualização de gráfico da capacidade alocada, da capacidade de armazenamento livre e da capacidade de armazenamento não atribuída no storage. |
| Hierarquia de armazenamento | A área hierarquia de armazenamento fornece uma visualização organizada dos vários componentes de hardware e objetos de armazenamento gerenciados pelo seu storage array. Clique na seta suspensa para executar uma determinada ação nesse componente de hardware ou objeto de armazenamento. |

#### Definições de interface

Pode alterar as preferências de apresentação e outras definições a partir da interface principal.

| Definição | Descrição |
| --- | --- |
| Preferências de visualização | Altere os valores de capacidade e o período de tempo na lista suspensa Preferências no canto superior direito da interface. |

| Definição | Descrição |
| --- | --- |
| Tempos limite da sessão | Configure tempos limite para que as sessões inativas dos usuários sejam desconetadas após um tempo especificado. |
| Ajuda | Acesse a documentação da Ajuda e outros recursos no menu suspenso no canto superior direito da interface. |

#### Logins de usuário e senhas

O usuário atual conetado ao sistema é mostrado no canto superior direito da interface.

Para obter mais informações sobre usuários e senhas, consulte:

- "Defina a proteção de senha de administrador"
- "Alterar senhas"

## Visualizar dados de desempenho

#### Visão geral do desempenho

A página desempenho fornece maneiras fáceis de monitorar a performance do storage array.

##### O que posso aprender com os dados de desempenho?

Os gráficos e tabelas de desempenho mostram dados de desempenho quase em tempo real, o que ajuda a determinar se um storage array está enfrentando problemas. Você também pode salvar dados de performance para criar uma visualização histórica de um storage array e identificar quando um problema foi iniciado ou o que causou um problema.

Saiba mais:

- "Gráficos de desempenho e diretrizes"
- "Termos de desempenho"

##### Como posso visualizar dados de desempenho?

Os dados de desempenho estão disponíveis na página inicial e na página armazenamento.

Saiba mais:

- "Visualizar dados gráficos de desempenho"
- "Visualizar e guardar dados de desempenho tabulares"
- "Interpretar dados de performance"

#### Gráficos de desempenho e diretrizes

A página desempenho fornece gráficos e tabelas de dados que permitem avaliar o desempenho da matriz de armazenamento em várias áreas-chave.

As funções de desempenho permitem realizar estas tarefas:

- Visualize dados de desempenho quase em tempo real para ajudá-lo a determinar se um storage array está enfrentando problemas.
- Exporte dados de performance para criar uma visualização histórica de um storage array e identificar quando um problema foi iniciado ou o que causou um problema.
- Selecione os objetos, as métricas de desempenho e o período de tempo que você deseja exibir.
- Comparar métricas.

Você pode visualizar dados de desempenho em três formatos:

- * Gráficos em tempo real* — traça dados de desempenho em um gráfico em tempo quase real.
- **Próximo tabular em tempo real** — lista os dados de desempenho em uma tabela em tempo quase real.
- * Arquivo CSV exportado * — permite salvar dados tabulares de desempenho em um arquivo de valores separados por vírgula para visualização e análise.

**Caraterísticas dos formatos de dados de desempenho**

| Tipo de monitoramento de desempenho | Intervalo de amostragem | Duração do tempo exibido | Número máximo de objetos exibidos | * Capacidade de salvar dados* |
|---|---|---|---|---|
| Gráfico em tempo real, ao vivo<br><br>Gráfico em tempo real, histórico | 10 seg. (ao vivo)<br><br>5 min (histórico)<br><br>Os pontos de dados mostrados dependem do período de tempo selecionado | O intervalo de tempo predefinido é de 1 hora.<br><br>Opções:<br>• 5 minutos<br>• 1 hora<br>• 8 horas<br>• 1 dia<br>• 7 dias<br>• 30 dias | 5 | Não |
| Tabela quase em tempo real (vista de tabela) | 10 seg. -1 h | Valor mais atual | Ilimitado | Sim |
| Arquivo de valores separados por vírgula (CSV) | Depende do período de tempo selecionado | Depende do período de tempo selecionado | Ilimitado | Sim |

**Diretrizes para visualização de dados de desempenho**

- A coleta de dados de desempenho está sempre ativa. Não há opção para desligá-lo.
- Cada vez que o intervalo de amostragem transcorrer, a matriz de armazenamento é consultada e os dados são atualizados.

- Para dados gráficos, o período de tempo de 5 minutos suporta a média de atualização de 10 segundos ao longo de 5 minutos. Todos os outros intervalos de tempo são atualizados a cada 5 minutos, com média do período de tempo selecionado.
- Os dados de desempenho nas visualizações gráficas são atualizados em tempo real. Os dados de desempenho na vista de tabela são atualizados quase em tempo real.
- Se um objeto monitorado mudar durante o tempo em que os dados são coletados, o objeto pode não ter um conjunto completo de pontos de dados abrangendo o período de tempo selecionado. Por exemplo, os conjuntos de volumes podem mudar à medida que os volumes são criados, excluídos, atribuídos ou não atribuídos; ou unidades podem ser adicionadas, removidas ou falhadas.

**Terminologia de desempenho**

Saiba como os termos de desempenho se aplicam ao storage array.

| Prazo | Descrição |
|---|---|
| Aplicação | Um aplicativo é um programa de software, como SQL ou Exchange. |
| CPU | CPU é curto para "unidade de processamento central". CPU indica a porcentagem da capacidade de processamento da matriz de armazenamento sendo usada. |
| Host | Um host é um servidor que envia e/S para um volume em um storage array. |
| IOPS | IOPS significa operações de entrada/saída por segundo. |
| Latência | Latência é o intervalo de tempo entre uma solicitação, como para um comando de leitura ou gravação, e a resposta do host ou do storage array. |
| LUN | Um número de unidade lógica (LUN) é o número atribuído ao espaço de endereço que um host usa para acessar um volume. O volume é apresentado ao host como capacidade na forma de um LUN.<br><br>Cada host tem seu próprio espaço de endereço LUN. Portanto, o mesmo LUN pode ser usado por diferentes hosts para acessar diferentes volumes. |
| MIB | MIB é uma abreviatura de mebibyte (mega byte binário). Um MIB é 220, ou 1.048.576 bytes. Compare com MB, que significa um valor base 10. Um MB equivale a 1.024 bytes. |
| Objeto | Um objeto é qualquer componente de storage lógico ou físico.<br><br>Os objetos lógicos incluem grupos de volumes, pools e volumes. Os objetos físicos incluem o storage array, controladores de array, hosts e unidades. |
| Piscina | Um pool é um conjunto de unidades que é agrupado logicamente. Você pode usar um pool para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um pool ou de um grupo de volumes.) |

| Prazo | Descrição |
| --- | --- |
| Leia | A leitura é abreviada para "operação de leitura", que ocorre quando o host solicita dados do storage array. |
| Volume | Um volume é um contêiner no qual aplicativos, bancos de dados e sistemas de arquivos armazenam dados. É o componente lógico criado para que o host acesse o storage no storage array.<br><br>Um volume é criado a partir da capacidade disponível em um pool ou em um grupo de volumes. Um volume tem uma capacidade definida. Embora um volume possa consistir em mais de uma unidade, um volume aparece como um componente lógico para o host. |
| Nome do volume | Um nome de volume é uma cadeia de carateres atribuída ao volume quando é criado. Você pode aceitar o nome padrão ou fornecer um nome mais descritivo indicando o tipo de dados armazenados no volume. |
| Grupo de volume | Um grupo de volumes é um contentor para volumes com caraterísticas compartilhadas. Um grupo de volumes tem uma capacidade definida e um nível RAID. Você pode usar um grupo de volumes para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um grupo de volumes ou de um pool.) |
| Workload | Um workload é um objeto de storage compatível com uma aplicação. Você pode definir uma ou mais cargas de trabalho ou instâncias por aplicação. Para alguns aplicativos, o sistema configura a carga de trabalho para conter volumes com caraterísticas de volume subjacentes semelhantes. Essas características de volume são otimizadas com base no tipo de aplicação compatível com o workload. Por exemplo, se você criar uma carga de trabalho que suporte um aplicativo Microsoft SQL Server e, posteriormente, criar volumes para essa carga de trabalho, as caraterísticas de volume subjacentes serão otimizadas para oferecer suporte ao Microsoft SQL Server. |
| Escreva | A gravação é curta para "operação de gravação", quando os dados são enviados do host para o array para armazenamento. |

### Visualizar dados gráficos de desempenho

É possível exibir dados de performance gráficos para objetos lógicos, objetos físicos, aplicações e workloads.

#### Sobre esta tarefa

Os gráficos de desempenho mostram dados históricos, bem como dados em tempo real que estão sendo capturados. Uma linha vertical no gráfico, rotulada Live Updating, distingue os dados históricos dos dados em tempo real.

- Visualização da página inicial*

A página inicial contém um gráfico que mostra o desempenho do nível da matriz de armazenamento. Você pode selecionar métricas limitadas nessa exibição ou clicar em **Exibir detalhes de desempenho** para

selecionar todas as métricas disponíveis.

**Vista detalhada**

Os gráficos disponíveis na vista de desempenho detalhada estão dispostos em três separadores:

- **Exibição lógica** — exibe dados de desempenho para objetos lógicos agrupados por grupos de volume e pools. Os objetos lógicos incluem grupos de volumes, pools e volumes.
- **Physical View** — exibe dados de desempenho para o controlador, canais host, canais de unidade e unidades.
- **Exibição de aplicativos e cargas de trabalho** — exibe uma lista de objetos lógicos (volumes) agrupados pelos tipos de aplicativos e cargas de trabalho que você definiu.

**Passos**

1. Selecione **Home**.
2. Para selecionar uma visualização em nível de matriz, clique no botão IOPS, MIB/s ou CPU.
3. Para ver mais detalhes, clique em **Exibir detalhes de desempenho**.
4. Selecione a guia **Exibição lógica**, a guia **Exibição física** ou a guia **Exibição de aplicativos e cargas de trabalho**.

   Dependendo do tipo de objeto, diferentes gráficos aparecem em cada guia.

| Ver separadores | Dados de desempenho exibidos para cada tipo de objeto |
|---|---|
| Vista lógica | • **Storage array**: IOPS, MIB/s.<br>• **Pools**: Latência, IOPS, MIB/s<br>• **Grupos de volume**: Latência, IOPS, MIB/s.<br>• **Volumes**: Latência, IOPS, MIB/s |
| Vista física | • **Controladores**: IOPS, MIB/s, CPU, espaço livre<br>• **Canais de host**: Latência, IOPS, MIB/s, espaço livre<br>• **Canais de unidade**: Latência, IOPS, MIB/s.<br>• **Unidades**: Latência, IOPS, MIB/s |
| Visualização de aplicações e workloads | • **Storage array**: IOPS, MIB/s.<br>• **Aplicações**: Latência, IOPS, MIB/s<br>• **Cargas de trabalho**: Latência, IOPS, MIB/s<br>• **Volumes**: Latência, IOPS, MIB/s |

5. Utilize as opções para visualizar os objetos e as informações de que necessita.

**Opções**

| Opções para visualização de objetos | Descrição |
| --- | --- |
| Expanda uma gaveta para ver a lista de objetos. | *Gavetas de navegação* contêm objetos de armazenamento, como pools, grupos de volume e unidades.<br><br>Clique na gaveta para ver a lista de objetos na gaveta. |
| Selecione objetos para visualizar. | Marque a caixa de seleção à esquerda de cada objeto para escolher os dados de desempenho que deseja exibir. |
| Use filtro para encontrar nomes de objetos ou nomes parciais. | Na caixa filtro, insira o nome ou um nome parcial de objetos para listar apenas esses objetos na gaveta. |
| Clique em **Atualizar gráficos** depois de selecionar objetos. | Depois de selecionar objetos nas gavetas, selecione **Atualizar gráficos** para ver os dados gráficos dos itens selecionados. |
| Ocultar ou mostrar gráfico | Selecione o título do gráfico para ocultar ou mostrar o gráfico. |

6. Conforme necessário, use as opções adicionais para visualizar dados de desempenho.

**Opções adicionais**

| Opção | Descrição |
|---|---|
| Período de tempo | Selecione a duração do tempo que pretende visualizar (5 minutos, 1 hora, 8 horas, 1 dia, 7 dias ou 30 dias). O padrão é 1 hora.<br><br>O carregamento de dados de desempenho para um período de 30 dias pode demorar vários minutos. Não navegue para fora da página da Web, atualize a página da Web ou feche o navegador enquanto os dados estão sendo carregados. |
| Detalhes do ponto de dados | Passe o cursor sobre o gráfico para ver as métricas de um determinado ponto de dados. |
| Barra de deslocamento | Use a barra de rolagem abaixo do gráfico para exibir um período de tempo anterior ou posterior. |
| Barra de zoom | Abaixo do gráfico, arraste as alças da barra de zoom para diminuir o zoom em um período de tempo. Quanto mais larga a barra de zoom, menos granulares os detalhes do gráfico.<br><br>Para repor o gráfico, selecione uma das opções de intervalo de tempo. |
| Arraste e solte | No gráfico, arraste o cursor de um ponto no tempo para outro para aumentar o zoom em um período de tempo.<br><br>Para repor o gráfico, selecione uma das opções de intervalo de tempo. |

### Visualizar e guardar dados de desempenho tabulares

Você pode visualizar e salvar dados de gráficos de desempenho em formato tabular. Isto permite-lhe filtrar os dados que pretende visualizar.

**Passos**

1. A partir de qualquer gráfico de dados de desempenho, clique em **Iniciar exibição de tabela**.

   É exibida uma tabela que lista todos os dados de desempenho dos objetos selecionados.

2. Utilize a opção de seleção de objetos e o filtro conforme necessário.
3. Clique no botão **Mostrar/Ocultar colunas** para selecionar as colunas que deseja incluir na tabela.

   Você pode clicar em cada caixa de seleção para selecionar ou desmarcar um item.

4. Selecione **Exportar** na parte inferior da tela para salvar a exibição tabular em um arquivo de valores separados por vírgula (CSV).

   A caixa de diálogo Exportar Tabela é exibida, indicando o número de linhas a serem exportadas e o formato de arquivo da exportação (valores separados por vírgula ou formato CSV).

5. Clique em **Exportar** para prosseguir com o download ou clique em **Cancelar**.

   Dependendo das configurações do navegador, o arquivo será salvo ou você será solicitado a escolher um nome e local para o arquivo.

   O formato padrão do nome do arquivo é `performanceStatistics-yyyy-mm-dd_hh-mm-ss.csv`, que inclui a data e a hora em que o arquivo foi exportado.

**Interpretar dados de performance**

## Os dados de desempenho podem orientá-lo no ajuste do desempenho do seu storage array.

Ao interpretar dados de desempenho, tenha em mente que vários fatores afetam o desempenho de seu storage array. A tabela a seguir descreve as principais áreas a serem consideradas.

| Dados de performance | Implicações para o ajuste de desempenho |
| --- | --- |
| Latência (milissegundos ou ms) | Monitorar a atividade de e/S de um objeto específico.<br><br>Identifique potencialmente objetos que são gargalos:<br><br>• Se um grupo de volumes for compartilhado entre vários volumes, os volumes individuais poderão precisar de seus próprios grupos de volumes para melhorar o desempenho sequencial das unidades e diminuir a latência.<br>• Com pools, latências maiores são introduzidas e workloads irregulares podem existir entre unidades, o que torna os valores de latência menos significativos e, em geral, maiores.<br>• O tipo de unidade e a velocidade influenciam a latência. Com e/S aleatória, as unidades giratórias mais rápidas gastam menos tempo movendo-se de e para diferentes locais no disco.<br>• Poucas unidades resultam em mais comandos enfileirados e um período de tempo maior para a unidade processar o comando, aumentando a latência geral do sistema.<br>• I/os maiores têm maior latência devido ao tempo adicional envolvido na transferência de dados.<br>• Maior latência pode indicar que o padrão de e/S é aleatório por natureza. As unidades com e/S aleatórias terão maior latência do que aquelas com fluxos sequenciais.<br>• Uma disparidade na latência entre unidades ou volumes de um grupo de volumes comum pode indicar uma unidade lenta. |

| Dados de performance | Implicações para o ajuste de desempenho |
| --- | --- |
| IOPS | Os fatores que afetam as operações de entrada/saída por segundo (IOPS ou iOS/seg) incluem estes itens:<br>• Padrão de acesso (aleatório ou sequencial)<br>• Tamanho de e/S.<br>• Nível RAID<br>• Tamanho do bloco de cache<br>• Se o armazenamento em cache de leitura está ativado<br>• Se o armazenamento em cache de gravação está ativado<br>• Pré-busca de leitura de cache dinâmico<br>• Tamanho do segmento<br>• O número de unidades nos grupos de volumes ou no storage de armazenamento<br>Quanto maior a taxa de acerto do cache, maiores serão as taxas de e/S. Taxas de e/S de gravação mais altas são experimentadas com o armazenamento em cache de gravação ativado em comparação com desativado. Ao decidir se deseja ativar o armazenamento em cache de gravação para um volume individual, observe o IOPS atual e o IOPS máximo. Você deve ver taxas mais altas para padrões de e/S sequenciais do que para padrões de e/S aleatórios. Independentemente do seu padrão de e/S, ative o armazenamento em cache de gravação para maximizar a taxa de e/S e reduzir o tempo de resposta do aplicativo.<br>Você pode ver melhorias de desempenho causadas pela alteração do tamanho do segmento nas estatísticas de IOPS de um volume. Experimente para determinar o tamanho ideal do segmento ou use o tamanho do sistema de arquivos ou o tamanho do bloco do banco de dados. |
| MIB/s. | As taxas de transferência ou taxa de transferência são determinadas pelo tamanho de e/S do aplicativo e pela taxa de e/S. Geralmente, solicitações de e/S de aplicativos pequenos resultam em uma taxa de transferência mais baixa, mas fornecem uma taxa de e/S mais rápida e um tempo de resposta menor. Com solicitações de e/S de aplicações maiores, taxas de transferência mais altas são possíveis.<br>Compreender os padrões típicos de e/S de aplicativos pode ajudá-lo a determinar as taxas máximas de transferência de e/S para um storage array específico. |

| Dados de performance | Implicações para o ajuste de desempenho |
| --- | --- |
| CPU | Este valor é uma percentagem da capacidade de processamento que está a ser utilizada.<br><br>Você pode notar uma disparidade no uso da CPU dos mesmos tipos de objetos. Por exemplo, o uso da CPU de um controlador é pesado ou está aumentando ao longo do tempo, enquanto o do outro controlador é mais leve ou mais estável. Nesse caso, você pode querer alterar a propriedade do controlador de um ou mais volumes para o controlador com a porcentagem de CPU mais baixa.<br><br>Você pode querer monitorar a CPU em toda a matriz de armazenamento. Se a CPU continuar a aumentar com o tempo enquanto o desempenho do aplicativo diminui, talvez seja necessário adicionar storage arrays. Ao adicionar storage arrays à sua empresa, você pode continuar atendendo às necessidades dos aplicativos em um nível de desempenho aceitável. |
| Espaço livre | Espaço livre refere-se à capacidade de desempenho restante dos controladores, dos canais de host do controlador e dos canais de unidade do controlador. Esse valor é expresso como uma porcentagem e representa a lacuna entre o desempenho máximo possível que esses objetos podem fornecer e os níveis de desempenho atuais.<br><br>• Para as controladoras, o espaço livre representa uma porcentagem do máximo de IOPS possível.<br>• Para os canais, o espaço livre é uma porcentagem do rendimento máximo, ou MIB/s. Taxa de transferência de leitura, taxa de transferência de gravação e taxa de transferência bidirecional estão incluídos no cálculo. |

## Exibir hierarquia de armazenamento

A hierarquia de armazenamento na interface principal fornece uma visualização organizada dos vários componentes de hardware e objetos de armazenamento gerenciados pelo seu storage array.

Para exibir a hierarquia de armazenamento, vá para a página inicial e clique na seta suspensa em um componente de storage ou objeto de armazenamento. Um storage array consiste em uma coleção de componentes físicos e componentes lógicos.

### Componentes físicos

Os componentes físicos de um storage array são descritos nesta tabela.

| Componente | Descrição |
| --- | --- |
| Controlador | Um controlador consiste em uma placa, firmware e software. Controla as unidades e implementa as funções do System Manager. |

| Componente | Descrição |
| --- | --- |
| Gaveta | Uma prateleira é um gabinete instalado em um gabinete ou rack. Ele contém os componentes de hardware para o storage array. Há dois tipos de compartimentos: Um compartimento de controladora e um compartimento de unidade. Um compartimento de controladora inclui controladores e unidades. Um compartimento de unidades inclui módulos de entrada/saída (IOMs) e unidades.<br><br>Se o storage array contiver diferentes tipos de Mídia ou diferentes tipos de interface, um compartimento de unidade para cada tipo de unidade será exibido. |
| Condução | Uma unidade é um dispositivo mecânico eletromagnético ou um dispositivo de memória de estado sólido que fornece os meios de armazenamento físico para os dados. |
| Host | Um host é um servidor que envia e/S para um volume em um storage array. |
| Adaptador de barramento do host (HBA) | Um adaptador de barramento de host (HBA) é uma placa que reside em um host e contém uma ou mais portas de host. |
| Porta de host | Uma porta de host é uma porta em um adaptador de barramento de host (HBA) que fornece a conexão física a um controlador e é usada para operações de e/S. |
| Cliente de gestão | Um cliente de gerenciamento é o computador em que um navegador está instalado para acessar o System Manager. |

### Componentes lógicos

As unidades no storage array fornecem a capacidade de armazenamento físico para os dados. Use o System Manager para configurar a capacidade física em componentes lógicos, como pools, grupos de volumes e volumes. Esses componentes são as ferramentas que você usa para configurar, armazenar, manter e preservar dados no storage array. Os componentes lógicos de um storage array são descritos nesta tabela.

| Componente | Descrição |
| --- | --- |
| Piscina | Um pool é um conjunto de unidades que é agrupado logicamente. Você pode usar um pool para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um pool ou de um grupo de volumes.) |
| Grupo de volume | Um grupo de volumes é um contentor para volumes com caraterísticas compartilhadas. Um grupo de volumes tem uma capacidade definida e um nível RAID. Você pode usar um grupo de volumes para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um grupo de volumes ou de um pool.) |
| Volume | Um volume é um contêiner no qual aplicativos, bancos de dados e sistemas de arquivos armazenam dados. É o componente lógico criado para que o host acesse o storage no storage array. |

| Componente | Descrição |
| --- | --- |
| Número de unidade lógica (LUN) | Um número de unidade lógica (LUN) é o número atribuído ao espaço de endereço que um host usa para acessar um volume. O volume é apresentado ao host como capacidade na forma de um LUN.<br><br>Cada host tem seu próprio espaço de endereço LUN. Portanto, o mesmo LUN pode ser usado por diferentes hosts para acessar diferentes volumes. |

## Gerir as definições da interface

### Gerenciar a proteção por senha

Você deve configurar o storage array com senhas para protegê-lo contra acesso não autorizado.

#### Definir e alterar senhas

Ao iniciar o System Manager pela primeira vez, você será solicitado a definir uma senha de administrador. Qualquer usuário que tenha a senha de administrador pode fazer alterações de configuração na matriz de armazenamento, como adicionar, alterar ou remover objetos ou configurações. Para definir a senha de administrador durante a inicialização inicial, "Acesse o System Manager"consulte .

Por razões de segurança, você pode tentar inserir uma senha apenas cinco vezes antes que o storage de armazenamento entre em um estado de "bloqueio". Nesse estado, o storage array rejeitará tentativas subsequentes de senha. Você deve esperar 10 minutos para que a matriz de armazenamento seja redefinida para um estado "normal" antes de tentar digitar uma senha novamente.

Além da senha de administrador, o storage array inclui perfis de usuário predefinidos com uma ou mais funções mapeadas para eles. Para obter mais informações, "Permissões para funções mapeadas"consulte . Os perfis de usuário e mapeamentos não podem ser alterados. Apenas as senhas podem ser modificadas. Se pretender alterar a palavra-passe de administrador ou outras palavras-passe de utilizador, "Alterar senhas"consulte .

#### Volte a introduzir palavras-passe após os tempos limite da sessão

O sistema solicita a senha apenas uma vez durante uma única sessão de gerenciamento. No entanto, uma sessão expira após 30 minutos de inatividade, altura em que deve introduzir novamente a palavra-passe. Se outro usuário que gerencia o mesmo storage array de outro cliente de gerenciamento alterar a senha enquanto sua sessão estiver em andamento, você será solicitado a digitar uma senha da próxima vez que tentar uma operação de configuração ou uma operação de exibição.

Você pode ajustar o tempo limite da sessão ou desativar completamente os tempos limite da sessão. "Gerenciar tempos limite de sessão"Consulte .

#### Remova as unidades ou a proteção por senha

Se você remover unidades protegidas por senha ou quiser desativar a proteção por senha, tenha em atenção o seguinte:

- **Se você remover unidades com proteção por senha** — a senha é armazenada em uma área reservada de cada unidade no storage de armazenamento. Se você remover todas as unidades de um storage array, sua senha não funcionará mais. Para corrigir essa condição, reinstale uma das unidades originais no

storage de armazenamento.

- **Se você quiser remover a proteção por senha** — se você não quiser mais ter comandos protegidos por senha, digite a senha atual do administrador e deixe as caixas de texto da nova senha em branco.

> Executar comandos de configuração em um storage array pode causar sérios danos, incluindo perda de dados. Por esse motivo, você sempre deve definir uma senha de administrador para o storage array. Use uma senha de administrador longa com pelo menos 15 carateres alfanuméricos para aumentar a segurança.

#### Definir unidades padrão para valores de capacidade

O System Manager pode exibir os valores de capacidade em gibibibytes (GiB) ou tebibytes (TIB).

As preferências são armazenadas no armazenamento local do navegador para que todos os usuários possam ter suas próprias configurações.

**Passos**

1. Selecione **Preferências › Definir preferências**.
2. Clique no botão de opção para **Gibibytes** ou **Tebibytes** e confirme que deseja executar a operação.

   Consulte a tabela a seguir para obter abreviaturas e valores.

| Abreviatura | Valor |
|---|---|
| Gib | 1.024 3 bytes |
| TIB | 1.024 4 bytes |

#### Definir o período de tempo predefinido para gráficos de desempenho

Pode alterar o período de tempo predefinido apresentado pelos gráficos de desempenho.

**Sobre esta tarefa**

Os gráficos de desempenho apresentados na página inicial e na página desempenho mostram inicialmente um período de tempo de 1 hora. As preferências são armazenadas no armazenamento local do navegador para que todos os usuários possam ter suas próprias configurações.

**Passos**

1. Selecione **Preferências › Definir preferências**.
2. Na lista suspensa, selecione **5 minutes**, **1 hour**, **8 hours**, **1 day** ou **7 Days** e confirme que deseja executar a operação.

#### Configurar o banner de login

Você pode criar um banner de login que é apresentado aos usuários antes que eles estabeleçam sessões no System Manager. O banner pode incluir um aviso de aviso e uma mensagem de consentimento.

**Sobre esta tarefa**

Quando você cria um banner, ele aparece antes da tela de login em uma caixa de diálogo.

**Passos**

1. Selecione **Definições › sistema**.
2. Na seção Geral, selecione **Configure Login Banner**.

   A caixa de diálogo Configurar banner de login será aberta.

3. Introduza o texto que pretende aparecer no banner de início de sessão.

   Não use HTML ou outras tags de marcação para formatação.

4. Clique em **Salvar**.

**Resultados**

Na próxima vez que os usuários fizerem login no System Manager, o texto será aberto em uma caixa de diálogo. Os usuários devem clicar em **OK** para continuar para a tela de login.

### Gerenciar tempos limite de sessão

É possível configurar tempos limite no System Manager para que as sessões inativas dos usuários sejam desconetadas após um tempo especificado.

**Sobre esta tarefa**

Por padrão, o tempo limite da sessão para o System Manager é de 30 minutos. Você pode ajustar esse tempo ou pode desativar os tempos limite da sessão por completo.

Se o Gerenciamento de Acesso for configurado usando os recursos SAML (Security Assertion Markup Language) incorporados no array, um tempo limite de sessão pode ocorrer quando a sessão SSO do usuário atingir seu limite máximo. Isso pode ocorrer antes do tempo limite da sessão do System Manager.

**Passos**

1. Selecione **Definições › sistema**.
2. Na seção Geral, selecione **Ativar/Desativar tempo limite da sessão**.

   A caixa de diálogo Ativar/Desativar tempo limite da sessão é aberta.

3. Utilize os controlos giratórios para aumentar ou diminuir o tempo em minutos.

   O tempo limite mínimo que você pode definir para o System Manager é de 15 minutos.

   Para desativar os tempos limite da sessão, desmarque a caixa de seleção **Definir o período de tempo…**.

4. Clique em **Salvar**.

# Gerenciar notificações

## Descrição geral das notificações de problemas

O System Manager usa ícones e vários outros métodos para notificá-lo de que existem problemas com a matriz de armazenamento.

### Ícones

O System Manager usa esses ícones para indicar o status do storage array e seus componentes.

| Ícone | Descrição |
| --- | --- |
|  | Ideal |
|  | Não-ideal ou falhou |
|  | Precisa de atenção ou fixação |
|  | Cuidado |

O System Manager exibe esses ícones em vários locais.

- A área notificações na página inicial exibe o ícone com falha e uma mensagem.
- O ícone da página inicial na área de navegação exibe o ícone com falha.
- Na página componentes, os gráficos para unidades e controladores exibem o ícone com falha.

### Alertas e LEDs

Além disso, o System Manager notifica você sobre problemas de outras maneiras.

- O System Manager envia notificações SNMP ou mensagens de erro de e-mail.
- Os LEDs da Ação de Serviço necessária no hardware acendem-se.

Quando você receber notificação de um problema, use o Recovery Guru para ajudá-lo a corrigir o problema. Quando necessário, use a documentação de hardware com as etapas de recuperação para substituir componentes com falha.

## Visualizar e agir sobre as operações em andamento

Para ver e agir em operações de longa duração, use a página operações em andamento.

### Sobre esta tarefa

Para cada operação listada na página operações em andamento, uma porcentagem de conclusão e o tempo estimado restante para concluir a operação são mostrados. Em alguns casos, você pode parar uma operação ou colocá-la em uma prioridade maior ou menor. Também pode limpar uma operação de cópia de volume concluída da lista.

### Passos

1. Na página inicial, selecione **Mostrar operações em andamento**.

A página operações em andamento é exibida.

2. Se desejar, use os links na coluna ações para parar ou alterar a prioridade de uma operação.

   Leia todo o texto de advertência fornecido nas caixas de diálogo, particularmente ao parar uma operação.

   Pode parar uma operação de cópia de volume ou alterar a sua prioridade.

3. Quando uma operação de cópia de volume estiver concluída, você poderá selecionar **Clear** para removê-la da lista.

   Na parte superior da página inicial, uma mensagem informativa e um ícone de chave amarela aparecem quando uma operação estiver concluída. Esta mensagem inclui um link que permite limpar a operação da página operações em andamento.

As operações que aparecem na página operações em andamento incluem o seguinte:

| Operação | Possível estado da operação | Ações que você pode tomar |
|---|---|---|
| Cópia de volume | Concluído | Limpar |
| Cópia de volume | Em curso | • Alterar prioridade<br>• Parar |
| Cópia de volume | Pendente | Limpar |
| Cópia de volume | Falha | • Limpar<br>• Volte a copiar |
| Cópia de volume | Parado | • Limpar<br>• Volte a copiar |
| Criar volume (volumes de pool espessos maiores que 64TiB somente) | Em curso | *none* |
| Eliminação de volume (volumes de pool espessos maiores que 64TiB somente) | Em curso | *none* |
| Sincronização inicial do grupo de espelhos assíncrono | Em curso | Suspender |
| Sincronização inicial do grupo de espelhos assíncrono | Suspenso | Retomar |
| Espelhamento síncrono | Em curso | Suspender |

| Operação | Possível estado da operação | Ações que você pode tomar |
| --- | --- | --- |
| Espelhamento síncrono | Suspenso | Retomar |
| Reversão de imagem instantânea | Em curso | Cancelar |
| Reversão de imagem instantânea | Pendente | Cancelar |
| Reversão de imagem instantânea | Em pausa | • Cancelar<br>• Retomar |
| Conduza a evacuação | Em curso | Cancelar (depende do tipo de evacuação da unidade) |
| Adicionar capacidade ao pool ou ao grupo de volumes | Em curso | *none* |
| Alterar um nível RAID para um volume | Em curso | *none* |
| Reduzir a capacidade de um pool | Em curso | *none* |
| Exigência de volume fino | Em curso | *none* |
| Verifique o tempo restante em uma operação de formato de disponibilidade instantânea (IAF) para volumes de pool | Em curso | *none* |
| Verifique a redundância de dados de um grupo de volumes | Em curso | *none* |
| Desfragmentar um grupo de volume | Em curso | *none* |
| Inicialize um volume | Em curso | *none* |
| Aumentar a capacidade de um volume | Em curso | *none* |
| Altere o tamanho do segmento para um volume | Em curso | *none* |
| Cópia da unidade | Em curso | *none* |
| Reconstrução de dados | Em curso | *none* |

| Operação | Possível estado da operação | Ações que você pode tomar |
| --- | --- | --- |
| Copyback | Em curso | *none* |
| Eliminação da transmissão | Em curso | *none* |
| Importação de armazenamento remoto | Em curso | • Alterar prioridade<br>• Parar |
| Importação de armazenamento remoto | Parado | • Retomar<br>• Desligar |
| Importação de armazenamento remoto | Falha | • Retomar<br>• Desligar |
| Importação de armazenamento remoto | Concluído | Desligar |

**Recuperar de problemas usando Recovery Guru**

O Recovery Guru é um componente do System Manager que diagnostica problemas de storage array e recomenda procedimentos de recuperação para corrigir os problemas.

**Passos**

1. Selecione **Home**.
2. Clique no link **Recover from *n* problems** no centro da janela.

   A caixa de diálogo Recovery Guru (Guru de recuperação) é exibida.

3. Selecione o primeiro problema mostrado na lista de resumo e siga as instruções no procedimento de recuperação para corrigir o problema. Sempre que necessário, utilize as instruções de substituição para substituir os componentes avariados. Repita esta etapa para cada problema listado.

   Vários problemas em um storage array podem ser relacionados. Neste caso, a ordem em que os problemas são corrigidos pode afetar o resultado. Selecione e corrija os problemas na ordem em que eles estão listados na lista de resumo.

   Várias falhas para um recipiente de fonte de alimentação são agrupadas e listadas como um problema na lista de resumo. Várias falhas para um recipiente do ventilador também são listadas como um problema.

4. Para se certificar de que o procedimento de recuperação foi bem-sucedido, clique em **verificar novamente**.

   Se você selecionou um problema para um grupo de espelhos assíncronos ou um membro de um grupo de espelhos assíncronos, clique em **Clear** primeiro para apagar a falha do controlador e clique em **Reverifique** para remover o evento do Recovery Guru.

   Se todos os problemas tiverem sido corrigidos, o ícone do storage array eventualmente transita de precisa de atenção para o ideal. Para alguns problemas, aparece um ícone de fixação enquanto uma operação,

como a reconstrução, está em andamento.

5. **Opcional:** para salvar as informações do Recovery Guru em um arquivo, clique no ícone **Salvar**.

   O arquivo é salvo na pasta Downloads do navegador com o nome `recovery-guru-failure-yyyy-mm-dd-hh-mm-ss-mmm.html`.

6. Para imprimir as informações do Recovery Guru, clique no ícone **Print**.

## FAQs

### Quais são os navegadores suportados?

O System Manager suporta essas versões do navegador.

| Navegador | Versão mínima |
|---|---|
| Google Chrome | 89 |
| Mozilla Firefox | 80 |
| Safari | 14 |
| Microsoft Edge | 90 |

### Quais são os atalhos de teclado?

Você pode navegar pelo System Manager usando apenas o teclado.

#### Navegação geral

| Ação | Atalho de teclado |
|---|---|
| Mover para o item seguinte. | Separador |
| Mover para o item anterior. | Shift e Tab |
| Selecione um item. | Introduza |
| Lista suspensa - mova para o item seguinte ou anterior. | Seta para baixo ou seta para cima |
| Caixa de seleção—Selecione um item. | Barra de espaço |
| Botões de rádio - alternar entre itens. | Seta para baixo ou seta para cima |
| Texto expansível—expandir ou contrato item. | Introduza |

**Navegação da mesa**

| Ação | Atalho de teclado |
|---|---|
| Selecione uma linha. | Para selecionar uma linha e, em seguida, prima Enter |
| Role para cima ou para baixo. | Seta para baixo/seta para cima ou Página para baixo/Página para cima |
| Altere a ordem de classificação de uma coluna. | Para selecionar um título de coluna e, em seguida, prima Enter |

**Navegação no calendário**

| Ação | Atalho de teclado |
|---|---|
| Passar para o mês anterior. | Página para cima |
| Passar para o próximo mês. | Página para baixo |
| Mudar para o ano anterior. | Página para cima |
| Mude para o próximo ano. | Página para baixo |
| Abra o seletor de data se estiver fechado. | Controle e Home |
| Mover para o mês atual. | Controle / comando e Home |
| Passar para o dia anterior. | Controle / comando à esquerda |
| Passar para o dia seguinte. | Controle / comando à direita |
| Passar para a semana anterior. | Controle / comando para cima |
| Passar para a próxima semana. | Controle / comando para baixo |
| Selecione a data focada. | Introduza |
| Feche o seletor de data e apague a data. | Controle / comando e fim |
| Feche o seletor de data sem seleção. | Escape |

**Como as estatísticas de desempenho para volumes individuais se relacionam com o total?**

As estatísticas de pools e grupos de volumes são calculadas agregando todos os volumes, incluindo volumes de capacidade reservada.

A capacidade reservada é usada internamente pelo sistema de storage para dar suporte a thin volumes, snapshots e espelhamento assíncrono, e não é visível para hosts de e/S. Como resultado, as estatísticas do pool, do controlador e do storage array podem não ser a soma dos volumes visíveis.

No entanto, para estatísticas de aplicações e cargas de trabalho, apenas os volumes visíveis são agregados.

**Por que os dados são exibidos como zero nos gráficos e na tabela?**

Quando um zero é exibido para um ponto de dados nos gráficos e tabela, significa que não há atividade de e/S para o objeto para esse ponto no tempo. Essa situação pode ocorrer porque o host não está iniciando e/S para esse objeto, ou pode ser um problema com o próprio objeto.

Os dados históricos do objeto ainda estão disponíveis para visualização. Os gráficos e a tabela mostrarão dados não-zero assim que a atividade de e/S começar a ocorrer para o objeto.

A tabela a seguir lista as razões mais comuns pelas quais um valor de ponto de dados pode ser zero para qualquer objeto.

| Tipo de objeto no nível do array | Os dados de motivo são exibidos como zero |
|---|---|
| Volume | • O volume não tinha atribuição de host. |
| Grupo de volume | • O grupo de volume está a ser importado.<br>• O grupo de volumes não contém um volume atribuído a um host, o grupo de volumes ***e*** não contém nenhuma capacidade reservada. |
| Condução | • A unidade falhou.<br>• A unidade foi removida.<br>• A unidade está num estado desconhecido. |
| Controlador | • O controlador está offline.<br>• O controlador falhou.<br>• O controlador foi removido.<br>• O controlador está num estado desconhecido. |
| Storage array | • Storage array não contém volumes. |

**O que o gráfico de latência mostra?**

O gráfico de latência fornece estatísticas de latência, em milissegundos (ms), para volumes, grupos de volumes, pools, aplicações e workloads. Este gráfico é apresentado nos separadores Vista lógica, Vista física e Vista aplicações e cargas de trabalho.

Latência refere-se a qualquer atraso que ocorre à medida que os dados são lidos ou gravados. Passe o cursor sobre um ponto no gráfico para ver os seguintes valores, em milissegundos (ms), para esse ponto no tempo:

- Tempo de leitura.
- Tempo de gravação.
- Tamanho médio de e/S.

**O que o gráfico IOPS mostra?**

O gráfico IOPS exibe estatísticas para operações de entrada/saída por segundo. Na página inicial, este gráfico exibe estatísticas para a matriz de armazenamento. Nas guias Exibição lógica, Exibição física e visualização de aplicativos e cargas de trabalho do bloco desempenho, esse gráfico exibe estatísticas do storage array, volumes, grupos de volumes, pools, aplicativos e cargas de trabalho.

IOPS é uma abreviatura para *IOPS/IOPS (e/S) operações por segundo*. Passe o cursor sobre um ponto no gráfico para ver os seguintes valores para esse ponto no tempo:

- Número de operações de leitura.
- Número de operações de gravação.
- Total de operações de leitura e gravação combinadas.

**O que o gráfico MIB/s mostra?**

O gráfico MIB/s exibe estatísticas de velocidade de transferência em mebibytes por segundo. Na página inicial, este gráfico exibe estatísticas para a matriz de armazenamento. Nas guias Exibição lógica, Exibição física e visualização de aplicativos e cargas de trabalho do bloco desempenho, esse gráfico exibe estatísticas do storage array, volumes, grupos de volumes, pools, aplicativos e cargas de trabalho.

MIB/s é uma abreviatura de *mebibytes por segundo*, ou 1.048.576 bytes por segundo. Passe o cursor sobre um ponto no gráfico para ver os seguintes valores para esse ponto no tempo:

- A quantidade de dados lidos.
- A quantidade de dados escritos.
- A quantidade total combinada de dados lidos e escritos.

**O que o gráfico da CPU mostra?**

O gráfico da CPU exibe estatísticas de capacidade de processamento para cada controlador (controlador A e controlador B). CPU é uma abreviatura para *central processing unit*. Na página inicial, este gráfico exibe estatísticas para a matriz de armazenamento. Na guia Exibição física do bloco desempenho, esse gráfico exibe estatísticas para o storage de armazenamento e unidades.

O gráfico da CPU mostra a porcentagem da capacidade de processamento da CPU que está sendo usada em relação às operações no array. Mesmo quando nenhuma e/S externa está ocorrendo, a porcentagem de utilização da CPU pode não ser zero porque o sistema operacional de armazenamento pode estar fazendo operações e monitoramento em segundo plano. Passe o cursor sobre um ponto no gráfico para ver uma percentagem da capacidade de processamento que está a ser utilizada nesse momento.

#### O que o gráfico da cabeceira mostra?

O gráfico de espaço livre está relacionado à capacidade de desempenho restante para os controladores do storage array. Este gráfico é visível na página inicial e na guia Exibição física do bloco desempenho.

O gráfico de altura mostra a capacidade de desempenho restante dos objetos físicos no sistema de armazenamento. Passe o cursor sobre um ponto no gráfico para ver as porcentagens de capacidade de IOPS e MIB/s restantes para o controlador A e para o controlador B.

#### Onde posso encontrar mais informações sobre as preferências de visualização?

Para encontrar informações sobre as opções de visualização disponíveis:

- Para ler mais sobre as unidades padrão para exibir valores de capacidade, "Definir unidades padrão para valores de capacidade"consulte .
- Para ler mais sobre o período de tempo predefinido para apresentar gráficos de desempenho, "Definir o período de tempo predefinido para gráficos de desempenho"consulte .

# Piscinas e grupos de volume

## Visão geral de pools e grupos de volume

É possível criar capacidade de armazenamento lógica a partir de um subconjunto de unidades não atribuídas no storage array. Essa capacidade lógica pode assumir a forma de um pool ou de um grupo de volumes, dependendo das necessidades do seu ambiente.

#### O que são pools e grupos de volume?

Um *pool* é um conjunto de unidades agrupadas logicamente. Um *volume group* é um contentor para volumes com caraterísticas compartilhadas. Você pode usar um pool ou um grupo de volumes para criar volumes acessíveis a um host.

Saiba mais:

- "Como os pools e os grupos de volume funcionam"
- "Terminologia de capacidade"
- "Decida se deseja usar um pool ou um grupo de volume"

#### Como você cria piscinas?

Você pode permitir que o System Manager crie pools automaticamente quando detetar capacidade não atribuída em um storage array. Alternativamente, quando a criação automática não pode determinar a melhor configuração, você pode criar pools manualmente a partir do **armazenamento › pools & grupos de volume**.

Saiba mais:

- "Criação automática versus manual de pool"
- "Criar pool automaticamente"

- "Criar pool manualmente"
- "Adicionar capacidade a um pool ou grupo de volumes"

#### Como criar grupos de volume?

Pode criar grupos de volume a partir do **armazenamento › pools & grupos de volume**.

Saiba mais:

- "Crie um grupo de volumes"
- "Adicionar capacidade a um pool ou grupo de volumes"

#### Informações relacionadas

Saiba mais sobre conceitos relacionados a pools e grupos de volumes:

- "Como funciona a capacidade reservada"
- "Como o cache SSD funciona"

## Conceitos

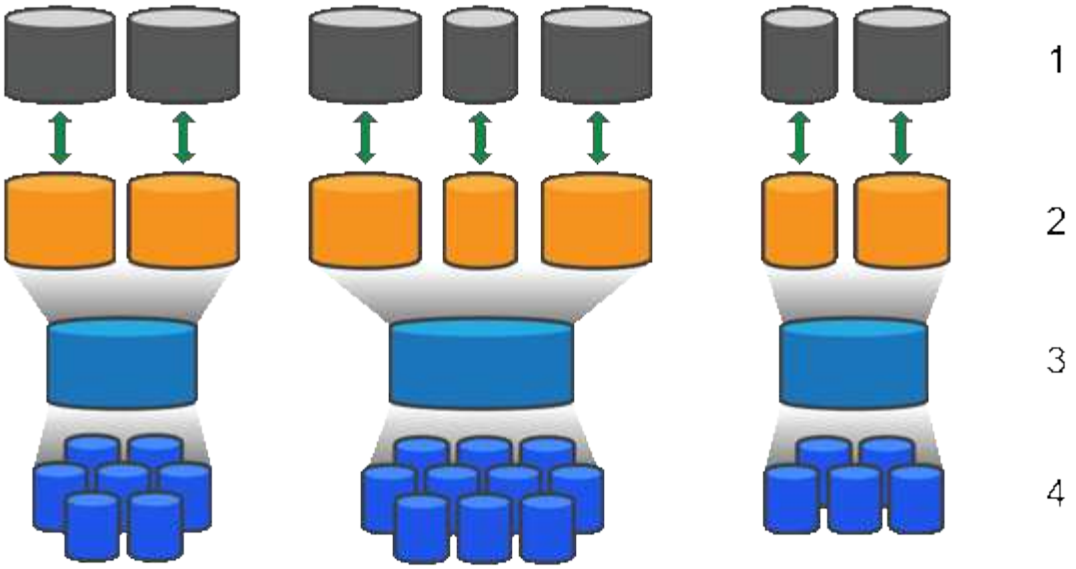
#### Como os pools e os grupos de volume funcionam

Para provisionar o armazenamento, você cria um pool ou um grupo de volumes que conterá as unidades de disco rígido (HDD) ou de disco de estado sólido (SSD) que você deseja usar em seu storage array.

O hardware físico é provisionado em componentes lógicos para que os dados possam ser organizados e facilmente recuperados. Há dois tipos de agrupamentos suportados:

- Piscinas
- Grupos de volume RAID

Os pools e grupos de volumes são as unidades de armazenamento de nível superior em um storage array: Dividem a capacidade das unidades em divisões gerenciáveis. Dentro dessas divisões lógicas estão os volumes individuais ou LUNs onde os dados são armazenados. A figura a seguir ilustra esse conceito.




1 unidades de disco rígido ou SSD; 2 unidades de disco rígido ou SSD; 4 unidades de disco rígido ou SSD. 3 unidades de disco rígido ou SSD

Quando um sistema de storage é implantado, a primeira etapa é apresentar a capacidade de unidade disponível para os vários hosts:

- Criação de pools ou grupos de volumes com capacidade suficiente
- Adicionar o número de unidades necessárias para atender aos requisitos de desempenho ao pool ou ao grupo de volumes
- Selecionar o nível desejado de proteção RAID (se estiver usando grupos de volume) para atender a requisitos empresariais específicos

Você pode ter pools ou grupos de volume no mesmo sistema de armazenamento, mas uma unidade não pode fazer parte de mais de um pool ou grupo de volumes. Os volumes que são apresentados aos hosts para e/S são então criados, usando o espaço no pool ou grupo de volumes.

#### Piscinas

Os pools foram projetados para agregar unidades de disco rígido físicas em um grande espaço de armazenamento e oferecer proteção RAID aprimorada para ele. Um pool cria muitos conjuntos de RAID virtuais a partir do número total de unidades atribuídas ao pool e distribui os dados uniformemente entre todas as unidades participantes. Se uma unidade for perdida ou adicionada, o System Manager reequilibra dinamicamente os dados em todas as unidades ativas.

Os pools funcionam como outro nível RAID, virtualizando a arquitetura RAID subjacente para otimizar o desempenho e a flexibilidade ao executar tarefas como reconstrução, expansão da unidade e manipulação da perda da unidade. O System Manager define automaticamente o nível RAID em 6 em uma 2 configuração de mais de 8 GB (oito discos de dados mais dois discos de paridade).

### Correspondência de condução

Você pode escolher entre HDD ou SSDs para uso em pools. No entanto, assim como nos grupos de volumes, todas as unidades do pool precisam usar a mesma tecnologia. Os controladores selecionam automaticamente quais unidades incluir, portanto, você deve ter certeza de que tem um número suficiente de unidades para a tecnologia escolhida.

### Gerenciamento de unidades com falha

Os pools têm uma capacidade mínima de 11 unidades; no entanto, uma unidade de capacidade é reservada para capacidade extra em caso de falha da unidade. Esta capacidade sobressalente é chamada de "capacidade de preservação".

Quando os pools são criados, uma certa quantidade de capacidade é preservada para uso de emergência. Essa capacidade é expressa em termos de várias unidades no System Manager, mas a implementação real está espalhada por todo o pool de unidades. A quantidade padrão de capacidade preservada é baseada no número de unidades no pool.

Depois que o pool é criado, você pode alterar o valor da capacidade de preservação para mais ou menos capacidade, ou até mesmo configurá-lo para nenhuma capacidade de preservação (valor de 0 unidade). A quantidade máxima de capacidade que pode ser preservada (expressa como um número de unidades) é de 10 TB, mas a capacidade disponível pode ser menor, com base no número total de unidades no pool.

#### Grupos de volume

Os grupos de volume definem como a capacidade é alocada no sistema de storage para volumes. As unidades de disco são organizadas em grupos RAID e os volumes residem nas unidades de um grupo RAID. Portanto, as configurações do grupo de volume identificam quais unidades fazem parte do grupo e qual nível RAID é usado.

Quando você cria um grupo de volumes, os controladores selecionam automaticamente as unidades a serem incluídas no grupo. Você deve escolher manualmente o nível RAID para o grupo. A capacidade do grupo de volumes é o total do número de unidades selecionadas, multiplicado pela sua capacidade.

### Correspondência de condução

Você deve corresponder as unidades no grupo de volumes para tamanho e desempenho. Se houver unidades menores e maiores no grupo de volumes, todas as unidades serão reconhecidas como o menor tamanho de capacidade. Se houver unidades mais lentas e mais rápidas no grupo de volumes, todas as unidades são reconhecidas na velocidade mais lenta. Esses fatores afetam o desempenho e a capacidade geral do sistema de storage.

Não é possível misturar diferentes tecnologias de unidade (unidades HDD e SSD). RAID 3, 5 e 6 estão limitados a um máximo de 30 unidades. RAID 1 e RAID 10 usam espelhamento, portanto, esses grupos de volume devem ter um número par de discos.

### Gerenciamento de unidades com falha

Os grupos de volume usam unidades hot spare como modo de espera no caso de uma unidade falhar nos volumes RAID 1/10, RAID 3, RAID 5 ou RAID 6 contidos em um grupo de volumes. Uma unidade hot spare não contém dados e adiciona outro nível de redundância à sua matriz de armazenamento.

Se uma unidade falhar no storage de armazenamento, a unidade hot spare será automaticamente substituída pela unidade com falha sem exigir uma troca física. Se a unidade hot spare estiver disponível quando uma unidade falhar, a controladora usará dados de redundância para reconstruir os dados da unidade com falha para a unidade hot spare.

### Terminologia de capacidade

Saiba como os termos de capacidade se aplicam ao storage array.

#### Objetos de storage

A terminologia a seguir descreve os diferentes tipos de objetos de armazenamento que podem interagir com seu storage array.

| Objeto de storage | Descrição |
| --- | --- |
| Host | Um host é um servidor que envia e/S para um volume em um storage array. |
| LUN | Um número de unidade lógica (LUN) é o número atribuído ao espaço de endereço que um host usa para acessar um volume. O volume é apresentado ao host como capacidade na forma de um LUN.<br><br>Cada host tem seu próprio espaço de endereço LUN. Portanto, o mesmo LUN pode ser usado por diferentes hosts para acessar diferentes volumes. |
| Grupo de consistência do espelho | Um grupo de consistência de espelho é um recipiente para um ou mais pares espelhados. Para operações de espelhamento assíncrono, você precisa criar um grupo de consistência de espelhamento. |
| Par de volume espelhado | Um par espelhado é composto por dois volumes, um volume primário e um volume secundário. |
| Piscina | Um pool é um conjunto de unidades que é agrupado logicamente. Você pode usar um pool para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um pool ou de um grupo de volumes.) |
| Grupo de consistência do Snapshot | Um grupo de consistência de snapshot é uma coleção de volumes que são tratados como uma única entidade quando uma imagem instantânea é criada. Cada um desses volumes tem sua própria imagem instantânea, mas todas as imagens são criadas no mesmo momento. |
| Grupo de instantâneos | Um grupo de instantâneos é uma coleção de imagens instantâneas a partir de um único volume base. |
| Volume do Snapshot | Um volume instantâneo permite que o host acesse dados na imagem instantânea. O volume instantâneo contém a sua própria capacidade reservada, que guarda quaisquer modificações no volume base sem afetar a imagem instantânea original. |
| Volume | Um volume é um contêiner no qual aplicativos, bancos de dados e sistemas de arquivos armazenam dados. É o componente lógico criado para que o host acesse o storage no storage array. |
| Grupo de volume | Um grupo de volumes é um contentor para volumes com caraterísticas compartilhadas. Um grupo de volumes tem uma capacidade definida e um nível RAID. Você pode usar um grupo de volumes para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um grupo de volumes ou de um pool.) |

#### Capacidade de storage

A terminologia a seguir descreve os diferentes tipos de capacidade usados em seu storage array.

| Tipo de capacidade | Descrição |
|---|---|
| Capacidade alocada | Capacidade alocada é a capacidade física alocada das unidades em um pool ou grupo de volumes.<br><br>Você usa a capacidade alocada para criar volumes e operações de serviços de cópia. |
| Capacidade livre | A capacidade livre é a capacidade disponível em um pool ou grupo de volumes que ainda não foi alocada para operações de criação de volume ou serviços de cópia e objetos de armazenamento. |
| Capacidade de pool ou grupo de volumes | A capacidade de pool, volume ou grupo de volumes é a capacidade de um storage array que foi atribuída a um pool ou grupo de volumes. Essa capacidade é usada para criar volumes e atender às várias necessidades de capacidade de operações de serviços de cópia e objetos de storage. |
| Pool capacidade inutilizável | Pool capacidade inutilizável é o espaço em um pool que não pode ser usado devido a tamanhos de unidade incompatíveis. |
| Capacidade de preservação | Capacidade de preservação é a quantidade de capacidade (número de unidades) reservada em um pool para dar suporte a possíveis falhas de unidade. |
| Capacidade comunicada | Capacidade reportada é a capacidade que é relatada ao host e pode ser acessada pelo host. |
| Capacidade reservada | A capacidade reservada é a capacidade alocada física usada para qualquer operação de serviço de cópia e objeto de storage. Não é diretamente legível pelo host. |
| Cache SSD | Cache SSD é um conjunto de unidades de disco de estado sólido (SSD) que você agrupa logicamente em sua matriz de armazenamento. O recurso cache SSD armazena em cache os dados acessados com mais frequência ("dados ativos") em unidades SSD de baixa latência para acelerar dinamicamente os workloads de aplicações. |
| Capacidade não atribuída | A capacidade não atribuída é o espaço em um storage array que **não** foi atribuído a um pool ou grupo de volumes. |
| Capacidade escrita | Capacidade escrita é a quantidade de capacidade que foi escrita a partir da capacidade reservada alocada para volumes finos. |

#### Decida se deseja usar um pool ou um grupo de volume

Você pode criar volumes usando um pool ou um grupo de volumes. A melhor seleção depende principalmente dos principais requisitos de storage, como o workload de e/S

esperado, os requisitos de performance e os requisitos de proteção de dados.

#### Razões para escolher um pool ou grupo de volume

### Escolha uma piscina

- Se você precisar de reconstruções de unidades mais rápidas e administração simplificada de storage, exija thin volumes e/ou tenha um workload altamente aleatório.
- Se você quiser distribuir os dados para cada volume aleatoriamente em um conjunto de unidades que compõem o pool.

  Não é possível definir ou alterar o nível RAID de pools ou volumes nos pools. Os pools usam RAID nível 6.

### Escolha um grupo de volume

- Se você precisar de largura de banda máxima do sistema, a capacidade de ajustar as configurações de storage e um workload altamente sequencial.
- Se você quiser distribuir os dados entre as unidades com base em um nível RAID. Você pode especificar o nível RAID ao criar o grupo de volumes.
- Se você quiser gravar os dados para cada volume sequencialmente no conjunto de unidades que compõem o grupo de volumes.

Como os pools podem coexistir com grupos de volume, um storage array pode conter pools e grupos de volume.

#### Diferenças de recursos entre pools e grupos de volume

A tabela a seguir fornece uma comparação de recursos entre grupos de volume e pools.

| Utilização | Piscina | Grupo de volume |
|---|---|---|
| Carga de trabalho aleatória | Melhor | Bom |
| Workload sequencial | Bom | Melhor |
| Tempo de recriação da unidade | Mais rápido | Mais lento |
| Desempenho (modo ideal) | Bom: Melhor para bloco pequeno, carga de trabalho aleatória. | Bom: Melhor para cargas de trabalho sequenciais e em blocos grandes |
| Desempenho (modo de recriação da unidade) | Melhor: Geralmente melhor que RAID 6 | Degradada: Queda de até 40% no desempenho |
| Várias falhas de unidade | Maior proteção de dados: Reconstruções com maior rapidez e prioridade | Menos proteção de dados: Reconstruções lentas, maior risco de perda de dados |

| Utilização | Piscina | Grupo de volume |
| --- | --- | --- |
| Adicionar unidades | Mais rápido: Adicionar à piscina em tempo real | Mais lento: Requer operação de expansão de capacidade dinâmica |
| Suporte a volumes finos | Sim | Não |
| Suporte a disco de estado sólido (SSD) | Sim | Sim |
| Administração simplificada | Sim: Não hot spares ou configurações RAID para configurar | Não: Deve alocar hot spares, configurar RAID |
| Desempenho ajustável | Não | Sim |

#### Comparação funcional de piscinas e grupos de volume

A função e o propósito de um pool e um grupo de volume são os mesmos. Ambos os objetos são um conjunto de unidades agrupadas logicamente em um storage array e são usados para criar volumes que um host pode acessar.

A tabela a seguir ajuda você a decidir se um pool ou um grupo de volumes se adapta melhor às suas necessidades de armazenamento.

| Função | Piscina | Grupo de volume |
| --- | --- | --- |
| Nível RAID diferente suportado | Não. Sempre RAID 6 no System Manager. | Sim. RAID 0, 1, 10, 5 e 6 disponíveis. |
| Thin volumes suportados | Sim | Não |
| Suporte a criptografia completa de disco (FDE) | Sim | Sim |
| Garantia de dados (DA) suportada | Sim | Sim |
| Proteção contra perda de prateleira suportada | Sim | Sim |
| Proteção contra perda de gaveta suportada | Sim | Sim |
| Velocidades de transmissão mistas suportadas | Recomendado para ser o mesmo, mas não necessário. A unidade mais lenta determina a velocidade para todas as unidades. | Recomendado para ser o mesmo, mas não necessário. A unidade mais lenta determina a velocidade para todas as unidades. |

| Função | Piscina | Grupo de volume |
| --- | --- | --- |
| Capacidade de unidade mista com suporte | Recomendado para ser o mesmo, mas não necessário. A menor unidade determina a capacidade de todas as unidades. | Recomendado para ser o mesmo, mas não necessário. A menor unidade determina a capacidade de todas as unidades. |
| Número mínimo de unidades | 11 | Depende do nível RAID. RAID 0 precisa de 1. RAID 1 ou 10 precisa de 2 (requer um número par). RAID 5 mínimo é 3. RAID 6 mínimo é 5. |
| Número máximo de unidades | Até o limite máximo para a matriz de armazenamento | RAID 1 e 10 - até o limite máximo das unidades RAID 5, 6—30 da matriz de armazenamento |
| Pode escolher unidades individuais ao criar um volume | Não | Sim |
| Pode especificar o tamanho do segmento ao criar um volume | Sim. 128K suportado. | Sim |
| Pode especificar as caraterísticas de e/S ao criar um volume | Não | Sim. Sistema de arquivos, banco de dados, Multimídia e personalizado suportados. |
| Proteção contra falha da unidade | Usa capacidade de preservação em cada unidade na piscina, tornando a reconstrução mais rápida. | Utiliza uma unidade hot spare. A reconstrução é limitada pelos IOPs da unidade. |
| Aviso ao atingir o limite de capacidade | Sim. Pode definir um alerta quando a capacidade utilizada atinge uma percentagem da capacidade máxima. | Não |
| Suporte à migração para um storage array diferente | Não. Requer que você migre para um grupo de volumes primeiro. | Sim |
| Tamanho dinâmico do segmento (DSS) | Não | Sim |
| Pode alterar o nível RAID | Não | Sim |
| Expansão de volume (aumentar a capacidade) | Sim | Sim |
| Expansão de capacidade (adicionar capacidade) | Sim | Sim |

| Função | Piscina | Grupo de volume |
| --- | --- | --- |
| Redução de capacidade | Sim | Não |

Os tipos de unidades mistas (HDD, SSD) não são compatíveis com pools ou grupos de volumes.

### Criação automática versus manual de pool

Você cria pools automaticamente ou manualmente para permitir que o storage físico seja agrupado e alocado dinamicamente conforme necessário. Quando um pool é criado, você pode adicionar unidades físicas.

#### Criação automática

A criação automática de pool é iniciada quando o System Manager deteta capacidade não atribuída em um storage array. Quando a capacidade não atribuída é detetada, o System Manager solicita automaticamente que você crie um ou mais pools ou adicione a capacidade não atribuída a um pool existente ou a ambos.

A criação automática de pool ocorre quando uma destas condições é verdadeira:

- Os pools não existem no storage array e há unidades similares suficientes para criar um novo pool.
- Novas unidades são adicionadas a um storage array que tenha pelo menos um pool.

Cada unidade em um pool deve ser do mesmo tipo de unidade (HDD ou SSD) e ter capacidade semelhante. O System Manager solicitará que você conclua as seguintes tarefas:

- Crie um único pool se houver um número suficiente de unidades desses tipos.
- Crie vários pools se a capacidade não atribuída consistir em diferentes tipos de unidade.
- Adicione as unidades ao pool existente se um pool já estiver definido no storage de armazenamento e adicione novas unidades do mesmo tipo de unidade ao pool.
- Adicione as unidades do mesmo tipo de unidade ao pool existente e use os outros tipos de unidade para criar pools diferentes se as novas unidades forem de tipos de unidade diferentes.

#### Criação manual

Você pode querer criar um pool manualmente quando a criação automática não puder determinar a melhor configuração. Esta situação pode ocorrer por uma das seguintes razões:

- As novas unidades podem ser potencialmente adicionadas a mais de um pool.
- Um ou mais dos novos candidatos à piscina podem usar proteção contra perda de prateleira ou proteção contra perda de gaveta.
- Um ou mais dos candidatos atuais ao pool não podem manter seu status de proteção contra perda de prateleira ou proteção contra perda de gaveta.

Você também pode querer criar um pool manualmente se tiver vários aplicativos em seu storage array e não quiser que eles concorram pelos mesmos recursos de unidade. Nesse caso, você pode considerar a criação manual de um pool menor para um ou mais aplicativos. Você pode atribuir apenas um ou dois volumes em vez de atribuir a carga de trabalho a um pool grande que tenha muitos volumes para distribuir os dados. A criação manual de um pool separado dedicado ao workload de uma aplicação específica pode permitir que as

operações de storage array tenham performance mais rápida, com menos contenção.

## Configurar o armazenamento

### Criar pool automaticamente

A criação de pool é iniciada automaticamente quando o System Manager deteta unidades não atribuídas no storage array. Você pode usar a criação automática de pool para configurar facilmente todas as unidades não atribuídas no storage em um pool e adicionar unidades a pools existentes.

#### Antes de começar

Você pode iniciar a caixa de diálogo Pool Auto-Configuration (Configuração automática do pool) quando uma destas condições for verdadeira:

- Pelo menos uma unidade não atribuída foi detetada que pode ser adicionada a um pool existente com tipos de unidade semelhantes.
- Onze (11) ou mais unidades não atribuídas foram detetadas que podem ser usadas para criar um novo pool (se elas não puderem ser adicionadas a um pool existente devido a tipos de unidades diferentes).

#### Sobre esta tarefa

Tenha em mente o seguinte:

- Quando você adiciona unidades a um storage array, o System Manager deteta automaticamente as unidades e solicita que você crie um único pool ou vários pools com base no tipo de unidade e na configuração atual.
- Se os pools foram definidos anteriormente, o System Manager solicitará automaticamente a opção de adicionar as unidades compatíveis a um pool existente. Quando novas unidades são adicionadas a um pool existente, o System Manager redistribui automaticamente os dados pela nova capacidade, que agora inclui as novas unidades adicionadas.
- Ao configurar um storage de armazenamento EF600 ou EF300, verifique se cada controlador tem acesso a um número igual de unidades nos primeiros 12 slots e a um número igual de unidades nos últimos 12 slots. Essa configuração ajuda os controladores a usar os dois barramentos PCIe do lado da unidade de forma mais eficaz.

Você pode iniciar a caixa de diálogo Configuração automática do pool usando qualquer um dos seguintes métodos:

- Quando a capacidade não atribuída é detetada, a recomendação Pool Auto-Configuration (Configuração automática do conjunto) é apresentada na página inicial na área Notification (notificação). Clique em **View Pool Auto-Configuration** para iniciar a caixa de diálogo.
- Você também pode iniciar a caixa de diálogo Pool Auto-Configuration (Configuração automática do pool) na página pools e grupos de volume, conforme descrito na tarefa a seguir.

#### Passos

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione **mais › Launch pool auto-Configuration** (Iniciar configuração automática do pool).

   A tabela de resultados lista novos pools, pools existentes com unidades adicionadas ou ambos. Um novo pool é nomeado com um número sequencial por padrão.

O System Manager executa as seguintes tarefas:

- Cria um único pool se houver um número suficiente de unidades com o mesmo tipo de unidade (HDD ou SSD) e tiverem capacidade semelhante.
- Cria vários pools se a capacidade não atribuída consistir em diferentes tipos de unidade.
- Adiciona as unidades a um pool existente se um pool já estiver definido no storage de armazenamento e você adicionar novas unidades do mesmo tipo de unidade ao pool.
- Adiciona as unidades do mesmo tipo de unidade ao pool existente e usa os outros tipos de unidade para criar pools diferentes se as novas unidades forem de tipos de unidade diferentes.

3. Para alterar o nome de um novo pool, clique no ícone **Editar** (o lápis).
4. Para ver caraterísticas adicionais do pool, posicione o cursor sobre ou toque no ícone **Detalhes** (a página).

   São exibidas informações sobre o tipo de unidade, a capacidade de segurança, a capacidade de garantia de dados (DA), a proteção contra perda de gaveta e a proteção contra perda de gaveta.

   Para storages EF600 e EF300, as configurações também são exibidas para provisionamento de recursos e tamanhos de blocos de volume.

5. Clique em **aceitar**.

### Criar pool manualmente

## Você pode criar um pool manualmente (a partir de um conjunto de candidatos) se o recurso Configuração automática do pool não fornecer um pool que atenda às suas necessidades.

Um pool fornece a capacidade de storage lógica necessária a partir da qual você pode criar volumes individuais que podem ser usados para hospedar seus aplicativos.

#### Antes de começar

- Você deve ter um mínimo de 11 unidades com o mesmo tipo de unidade (HDD ou SSD).
- A proteção contra perda de gaveta exige que as unidades que compõem o pool estejam localizadas em pelo menos seis compartimentos de unidades diferentes e não haja mais do que duas unidades em um único compartimento de unidades.
- A proteção contra perda de gaveta exige que as unidades que compõem o pool estejam localizadas em pelo menos cinco gavetas diferentes e o pool inclua um número igual de prateleiras de unidades de cada gaveta.
- Ao configurar um storage de armazenamento EF600 ou EF300, verifique se cada controlador tem acesso a um número igual de unidades nos primeiros 12 slots e a um número igual de unidades nos últimos 12 slots. Essa configuração ajuda os controladores a usar os dois barramentos PCIe do lado da unidade de forma mais eficaz. Atualmente o System Manager permite a seleção de unidades no recurso Avançado ao criar um grupo de volumes. Para a criação de pool, recomenda-se usar todas as unidades no storage de armazenamento.

#### Passos

1. Selecione **armazenamento › pools & grupos de volume**.
2. Clique em **criar › Pool**.

A caixa de diálogo criar pool é exibida.

3. Digite um nome para o pool.
4. **Opcional:** se você tiver mais de um tipo de unidade em sua matriz de armazenamento, selecione o tipo de unidade que você deseja usar.

   A tabela de resultados lista todos os pools possíveis que você pode criar.

5. Selecione o candidato ao pool que você deseja usar com base nas seguintes caraterísticas e clique em **criar**.

| Característica | Utilização |
| --- | --- |
| Capacidade livre | Mostra a capacidade livre do candidato à pool em GiB. Selecione um candidato a pool com a capacidade para as necessidades de armazenamento do seu aplicativo.<br><br>A capacidade de preservação (sobressalente) também é distribuída em toda a piscina e não faz parte do valor da capacidade livre. |
| Total de unidades | Mostra o número de unidades disponíveis no candidato ao pool.<br><br>O System Manager reserva automaticamente o máximo de unidades possível para a capacidade de preservação (para cada seis unidades em um pool, o System Manager reserva uma unidade para a capacidade de preservação).<br><br>Quando ocorre uma falha de unidade, a capacidade de preservação é utilizada para manter os dados reconstruídos. |
| Tamanho do bloco de acionamento (somente EF300 e EF600) | Mostra o tamanho do bloco (tamanho do setor) que as unidades no pool podem gravar. Os valores podem incluir:<br><br>• 512 — tamanho do setor de 512 bytes.<br>• 4K — tamanho do setor de 4.096 bytes. |
| Com capacidade segura | Indica se esse candidato a pool é composto inteiramente de unidades com capacidade de segurança, que podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).<br><br>• Você pode proteger seu pool com o Drive Security, mas todas as unidades devem ser seguras para usar esse recurso.<br>• Se você quiser criar um pool apenas FDE, procure **Sim - FDE** na coluna compatível com segurança. Se você quiser criar um pool somente FIPS, procure **Sim - FIPS** ou **Sim - FIPS (Misto)**. "Mixed" (Misto) indica uma mistura de unidades de nível 140-2 e 140-3. Se você usar uma mistura desses níveis, esteja ciente de que o pool funcionará no nível mais baixo de segurança (140-2).<br>• Você pode criar um pool composto de unidades que podem ou não ser seguras ou que são uma combinação de níveis de segurança. Se as unidades no pool incluírem unidades que não são seguras, você não poderá tornar o pool seguro. |

| Característica | Utilização |
| --- | --- |
| Ativar segurança? | Fornece a opção para ativar o recurso de Segurança da Unidade com unidades com capacidade segura. Se o pool for seguro e você tiver criado uma chave de segurança, poderá ativar a segurança selecionando a caixa de seleção.<br><br>A única maneira de remover o Drive Security depois de ativado é excluir o pool e apagar as unidades. |
| DA capaz | Indica se a Garantia de dados (DA) está disponível para este candidato a pool. O DA verifica e corrige erros que podem ocorrer à medida que os dados são transferidos através dos controladores para as unidades.<br><br>A DA é ativada se todas as unidades forem capazes de DA. A DA pode ser desativada após a criação do volume selecionando **armazenamento › volumes › Ver/Editar Definições › Avançadas › Desativar permanentemente a garantia de dados**. Se A DA estiver desativada num volume, não poderá ser reativada. |
| Compatível com provisionamento de recursos (somente EF300 e EF600) | Mostra se o provisionamento de recursos está disponível para este candidato a pool. O provisionamento de recursos é um recurso disponível nas matrizes de armazenamento EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente sem processo de inicialização em segundo plano. |
| Proteção contra perda de prateleira | Mostra se a proteção contra perda de prateleira está disponível.<br><br>A proteção contra perda de gaveta garante a acessibilidade aos dados nos volumes em um pool se houver perda total de comunicação com um único compartimento de unidade. |
| Proteção contra perda de gaveta | Mostra se a proteção contra perda de gaveta está disponível, que é fornecida somente se você estiver usando uma prateleira de unidade que contém gavetas.<br><br>A proteção contra perda de gaveta garante a acessibilidade aos dados nos volumes em um pool se ocorrer uma perda total de comunicação com uma única gaveta em um compartimento de unidades. |
| Tamanhos de bloco de volume suportados (apenas EF300 e EF600) | Mostra os tamanhos de bloco que podem ser criados para os volumes no pool:<br><br>• 512n — 512 bytes nativos.<br>• 512e — 512 bytes emulados.<br>• 4K — 4.096 bytes. |

### Crie um grupo de volumes

Você usa um grupo de volumes para criar um ou mais volumes acessíveis ao host. Um grupo de volumes é um contêiner para volumes com características compartilhadas, como nível e capacidade de RAID.

Com unidades de capacidade maior e a capacidade de distribuir volumes entre controladores, criar mais de um volume por grupo de volumes é uma boa maneira de usar sua capacidade de storage e proteger seus dados.

#### Antes de começar

Reveja estas diretrizes antes de criar um grupo de volumes:

- Você precisa de pelo menos uma unidade não atribuída.
- Existem limites no número de unidades que você pode ter em um único grupo de volume. Esses limites variam de acordo com o nível RAID.
- Para ativar a proteção contra perda de gaveta/gaveta, você deve criar um grupo de volumes que use unidades localizadas em pelo menos três gavetas ou gavetas, a menos que esteja usando RAID 1, em que duas gavetas sejam mínimas.
- Se você tiver um storage array EF600 ou EF300 e planeja criar um grupo de volumes manualmente, verifique se cada controlador tem acesso a um número igual de unidades nos primeiros 12 slots e um número igual de unidades nos últimos 12 slots. Essa configuração ajuda os controladores a usar os dois barramentos PCIe do lado da unidade de forma mais eficaz. Atualmente o System Manager permite a seleção de unidades no recurso Avançado ao criar um grupo de volumes.
- Analise como sua escolha de nível RAID afeta a capacidade resultante do grupo de volumes:
  - Se selecionar RAID 1, tem de adicionar duas unidades de cada vez para se certificar de que está selecionado um par espelhado. O espelhamento e o striping (conhecido como RAID 10 ou RAID 1-0) são alcançados quando quatro ou mais unidades são selecionadas.
  - Se selecionar RAID 5, tem de adicionar um mínimo de três unidades para criar o grupo de volumes.
  - Se selecionar RAID 6, tem de adicionar um mínimo de cinco unidades para criar o grupo de volumes.

#### Passos

1. Selecione **armazenamento › pools & grupos de volume**.
2. Clique em **criar › Grupo de volume**.

   A caixa de diálogo criar grupo de volume é exibida.

3. Digite um nome para o grupo de volumes.
4. Selecione o nível RAID que melhor atende aos seus requisitos de armazenamento e proteção de dados.

   A tabela de candidatos ao grupo de volume é exibida e exibe apenas os candidatos que suportam o nível RAID selecionado.

5. **Opcional:** se você tiver mais de um tipo de unidade em sua matriz de armazenamento, selecione o tipo de unidade que você deseja usar.

   A tabela de candidatos ao grupo de volume é exibida e exibe apenas os candidatos que suportam o tipo de unidade selecionada e o nível RAID.

6. **Opcional:** você pode selecionar o método automático ou o método manual para definir quais unidades usar no grupo de volumes. O método Automático é a seleção padrão.

   Para selecionar as unidades manualmente, clique no link **manualmente Select Drives (Advanced)**. Quando clicado, ele muda para **automaticamente selecionar unidades (avançadas)**.

   O método Manual permite selecionar quais unidades específicas compõem o grupo de volumes. Você pode selecionar unidades específicas não atribuídas para obter a capacidade que você precisa. Se o storage de armazenamento contiver unidades com diferentes tipos de Mídia ou diferentes tipos de interface, você poderá escolher apenas a capacidade não configurada para um único tipo de unidade para criar o novo grupo de volumes.

   > Somente especialistas que entendem a redundância de unidades e as configurações ideais de unidades devem usar o método Manual.

7. Com base nas caraterísticas da unidade exibidas, selecione as unidades que deseja usar no grupo de volumes e clique em **criar**.

   As caraterísticas de condução apresentadas dependem da seleção do método automático ou do método manual.

**Caraterísticas automáticas do acionamento do método**

| Característica | Utilização |
| --- | --- |
| Capacidade livre | Mostra a capacidade disponível em GiB. Selecione um candidato a grupo de volume com a capacidade para as necessidades de armazenamento do seu aplicativo. |
| Total de unidades | Mostra o número de unidades disponíveis para este grupo de volumes. Selecione um candidato a grupo de volume com o número de unidades desejadas. |
| Tamanho do bloco de acionamento (somente EF300 e EF600) | Mostra o tamanho do bloco (tamanho do setor) que as unidades no grupo podem gravar. Os valores podem incluir:<br>• 512 — tamanho do setor de 512 bytes.<br>• 4K — tamanho do setor de 4.096 bytes. |
| Com capacidade segura | Indica se esse candidato a grupo de volumes é composto inteiramente de unidades com capacidade de segurança, que podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).<br>• Você pode proteger seu grupo de volumes com o Drive Security, mas todas as unidades devem ser seguras para usar esse recurso.<br>• Se você quiser criar um grupo de volumes apenas FDE, procure **Sim - FDE** na coluna compatível com segurança. Se você quiser criar um grupo de volumes somente FIPS, procure **Sim - FIPS** ou **Sim - FIPS (Misto)**. "Mixed" (Misto) indica uma mistura de unidades de nível 140-2 e 140-3. Se você usar uma mistura desses níveis, esteja ciente de que o grupo de volume funcionará no nível mais baixo de segurança (140-2).<br>• Você pode criar um grupo de volumes composto por unidades que podem ou não ser seguras ou que são uma combinação de níveis de segurança. Se as unidades do grupo de volumes incluírem unidades que não são seguras, não será possível tornar o grupo de volumes seguro. |
| Ativar segurança? | Fornece a opção para ativar o recurso de Segurança da Unidade com unidades com capacidade segura. Se o grupo de volumes for seguro e tiver configurado uma chave de segurança, pode ativar a Segurança da unidade selecionando a caixa de verificação.<br>A única maneira de remover o Drive Security depois de ativado é excluir o grupo de volumes e apagar as unidades. |

| Característica | Utilização |
| --- | --- |
| DA capaz | Indica se a Garantia de dados (DA) está disponível para este grupo. O Data Assurance (DA) verifica e corrige erros que podem ocorrer à medida que os dados são transferidos através dos controladores para as unidades.<br><br>Se pretender utilizar DA, selecione um grupo de volumes capaz de DA. (Para unidades compatíveis com DA, A DA é ativada automaticamente em volumes criados no pool.)<br><br>Um grupo de volumes pode conter unidades que são capazes de DA ou não, mas todas as unidades devem ser capazes de DA para você usar esse recurso. |
| Compatível com provisionamento de recursos (somente EF300 e EF600) | Mostra se o provisionamento de recursos está disponível para este grupo. O provisionamento de recursos é um recurso disponível nas matrizes de armazenamento EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente sem processo de inicialização em segundo plano. |
| Proteção contra perda de prateleira | Mostra se a proteção contra perda de prateleira está disponível. A proteção contra perda de prateleira garante a acessibilidade aos dados nos volumes de um grupo de volumes se ocorrer uma perda total de comunicação com uma prateleira. |
| Proteção contra perda de gaveta | Mostra se a proteção contra perda de gaveta está disponível, que é fornecida somente se você estiver usando uma prateleira de unidade que contém gavetas. A proteção contra perda de gaveta garante a acessibilidade aos dados nos volumes em um grupo de volumes se ocorrer uma perda total de comunicação com uma única gaveta em um compartimento de unidades. |
| Tamanhos de bloco de volume suportados (apenas EF300 e EF600) | Mostra os tamanhos de bloco que podem ser criados para os volumes no grupo:<br><br>• 512n — 512 bytes nativos.<br>• 512e — 512 bytes emulados.<br>• 4K — 4.096 bytes. |

**Caraterísticas de acionamento do método manual**

| Característica | Utilização |
| --- | --- |
| Tipo de material | Indica o tipo de material. São suportados os seguintes tipos de material:<br>• Disco rígido<br>• Disco de estado sólido (SSD)<br>Todas as unidades de um grupo de volumes devem ser do mesmo tipo de Mídia (todos os SSDs ou todos os discos rígidos). Os grupos de volume não podem ter uma mistura de tipos de Mídia ou tipos de interface. |
| Tamanho do bloco de acionamento (somente EF300 e EF600) | Mostra o tamanho do bloco (tamanho do setor) que as unidades no grupo podem gravar. Os valores podem incluir:<br>• 512 — tamanho do setor de 512 bytes.<br>• 4K — tamanho do setor de 4.096 bytes. |
| Capacidade da unidade | Indica a capacidade da unidade.<br>• Sempre que possível, selecione unidades que tenham uma capacidade igual às capacidades das unidades atuais no grupo de volumes.<br>• Se você precisar adicionar unidades não atribuídas com uma capacidade menor, lembre-se de que a capacidade utilizável de cada unidade atualmente no grupo de volumes será reduzida. Portanto, a capacidade da unidade é a mesma em todo o grupo de volume.<br>• Se você precisar adicionar unidades não atribuídas com uma capacidade maior, lembre-se de que a capacidade utilizável das unidades não atribuídas adicionadas será reduzida para que elas correspondam às capacidades atuais das unidades no grupo de volumes. |
| Tabuleiro | Indica a localização da bandeja da unidade. |
| Ranhura | Indica a localização da ranhura da unidade. |
| Velocidade (rpm) | Indica a velocidade da unidade. |
| Tamanho do setor lógico | Indica o tamanho e o formato do setor. |

| Característica | Utilização |
| --- | --- |
| Com capacidade segura | Indica se esse candidato a grupo de volumes é composto inteiramente de unidades com capacidade de segurança, que podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).<br><br>• Você pode proteger seu grupo de volumes com o Drive Security, mas todas as unidades devem ser seguras para usar esse recurso.<br>• Se você quiser criar um grupo de volumes apenas FDE, procure **Sim - FDE** na coluna compatível com segurança. Se você quiser criar um grupo de volumes somente FIPS, procure **Sim - FIPS** ou **Sim - FIPS (Misto)**. "Mixed" (Misto) indica uma mistura de unidades de nível 140-2 e 140-3. Se você usar uma mistura desses níveis, esteja ciente de que o grupo de volume funcionará no nível mais baixo de segurança (140-2).<br>• Você pode criar um grupo de volumes composto por unidades que podem ou não ser seguras ou que são uma combinação de níveis de segurança. Se as unidades do grupo de volumes incluírem unidades que não são seguras, não será possível tornar o grupo de volumes seguro. |
| DA capaz | Indica se a Garantia de dados (DA) está disponível para este grupo. O Data Assurance (DA) verifica e corrige erros que podem ocorrer à medida que os dados são comunicados através dos controladores para as unidades.<br><br>Se pretender utilizar DA, selecione um grupo de volumes capaz de DA. (Para unidades compatíveis com DA, A DA é ativada automaticamente em volumes criados no pool.)<br><br>Um grupo de volumes pode conter unidades que são capazes de DA ou não, mas todas as unidades devem ser capazes de DA para você usar esse recurso. |
| Tamanhos de bloco de volume suportados (apenas EF300 e EF600) | Mostra os tamanhos de bloco que podem ser criados para os volumes no grupo:<br><br>• 512n — 512 bytes nativos.<br>• 512e — 512 bytes emulados.<br>• 4K — 4.096 bytes. |
| Compatível com provisionamento de recursos (somente EF300 e EF600) | Mostra se o provisionamento de recursos está disponível para este grupo. O provisionamento de recursos é um recurso disponível nas matrizes de armazenamento EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente sem processo de inicialização em segundo plano. |

### Adicionar capacidade a um pool ou grupo de volumes

Você pode adicionar unidades para expandir a capacidade livre em um pool ou grupo de volumes existente.

A expansão faz com que a capacidade livre adicional seja incluída no pool ou no grupo de volumes. Você pode usar essa capacidade gratuita para criar volumes adicionais. Os dados nos volumes permanecem acessíveis durante esta operação.

#### Antes de começar

- As unidades devem estar em um status ideal.
- As unidades devem ter o mesmo tipo de unidade (HDD ou SSD).
- O pool ou grupo de volume deve estar em um status ideal.
- O número máximo de volumes permitido num grupo de volumes é 256.
- O número máximo de volumes permitidos em um pool depende do modelo do sistema de armazenamento:
  - 2.048 volumes (séries EF600 e E5700)
  - 1.024 volumes (EF300)
  - 512 volumes (série E2800)
- Se o pool ou grupo de volumes contiver todas as unidades com capacidade segura, adicione apenas unidades com capacidade segura para continuar a usar as habilidades de criptografia das unidades com capacidade segura.

  As unidades com capacidade segura podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).

#### Sobre esta tarefa

Para pools, você pode adicionar um máximo de 60 unidades de cada vez. Para grupos de volumes, você pode adicionar um máximo de duas unidades de cada vez. Se for necessário adicionar mais do que o número máximo de unidades, repita o procedimento. (Um pool não pode conter mais unidades do que o limite máximo para um sistema de armazenamento.)

> Com a adição de unidades, sua capacidade de preservação pode precisar ser aumentada. Você deve considerar aumentar a capacidade reservada após uma operação de expansão.

> Evite usar unidades que são capazes de garantia de dados (DA) para adicionar capacidade a um pool ou grupo de volume que não é capaz de DA. O pool ou o grupo de volumes não podem aproveitar as capacidades da unidade capaz de DA. Considere usar unidades que não são capazes de DA nesta situação.

#### Passos

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione o pool ou grupo de volumes ao qual deseja adicionar unidades e clique em **Adicionar capacidade**.

   A caixa de diálogo Adicionar capacidade é exibida. Somente as unidades não atribuídas compatíveis com o pool ou grupo de volumes são exibidas.

3. Em **Selecione unidades para adicionar capacidade…**, selecione uma ou mais unidades que você deseja adicionar ao pool ou grupo de volumes existente.

   O firmware do controlador organiza as unidades não atribuídas com as melhores opções listadas na parte superior. A capacidade total gratuita adicionada ao pool ou grupo de volumes aparece abaixo da lista em **capacidade total selecionada**.

**Detalhes do campo**

| Campo | Descrição |
| --- | --- |
| Gaveta | Indica a localização do compartimento da unidade. |
| Baía | Indica a localização do compartimento da unidade. |
| Capacidade (GiB) | Indica a capacidade da unidade.<br>• Sempre que possível, selecione unidades que tenham uma capacidade igual às capacidades das unidades atuais no pool ou grupo de volumes.<br>• Se você precisar adicionar unidades não atribuídas com uma capacidade menor, lembre-se de que a capacidade utilizável de cada unidade atualmente no pool ou grupo de volumes será reduzida. Portanto, a capacidade da unidade é a mesma em todo o pool ou grupo de volumes.<br>• Se você precisar adicionar unidades não atribuídas com uma capacidade maior, lembre-se de que a capacidade utilizável das unidades não atribuídas adicionadas será reduzida para que elas correspondam às capacidades atuais das unidades no pool ou grupo de volumes. |
| Com capacidade segura | Indica se a unidade é segura.<br>• Para proteger seu pool ou grupo de volumes com o recurso Segurança da unidade, todas as unidades devem ser seguras.<br>• É possível criar um pool ou grupo de volumes com uma combinação de unidades seguras e não seguras, mas o recurso Segurança da Unidade não pode ser ativado.<br>• Um pool ou grupo de volumes com todas as unidades com capacidade de segurança não pode aceitar uma unidade com capacidade de segurança para poupar ou expandir, mesmo que a capacidade de criptografia não esteja em uso.<br>• As unidades relatadas como seguras podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).<br>• Uma unidade FIPS pode ser nível 140-2 ou 140-3, com nível 140-3 como o nível mais alto de segurança. Se você selecionar uma combinação de unidades de nível 140-2 e 140-3, o pool ou grupo de volumes funcionará no nível mais baixo de segurança (140-2). |

| Campo | Descrição |
| --- | --- |
| DA capaz | Indica se a unidade é capaz de Garantia de dados (DA).<br>• O uso de unidades que não são capazes de garantia de dados (DA) para adicionar capacidade a um pool ou grupo de volume compatível com DA não é recomendado. O pool ou grupo de volumes não tem mais recursos DA e você não tem mais a opção de ativar DA em volumes recém-criados dentro do pool ou grupo de volumes.<br>• O uso de unidades que são capazes de garantia de dados (DA) para adicionar capacidade a um pool ou grupo de volume que não é capaz de DA não é recomendado, porque esse pool ou grupo de volume não pode tirar proveito dos recursos da unidade capaz de DA (os atributos da unidade não correspondem). Considere usar unidades que não são capazes DE DA nesta situação. |
| DULBE capaz | Indica se a unidade tem a opção de erro de bloco lógico desalocado ou não escrito (DULBE). O DULBE é uma opção nas unidades NVMe que permite que o storage array EF300 ou EF600 ofereça suporte a volumes provisionados por recursos. |

4. Clique em **Add**.

   Se você estiver adicionando unidades a um pool ou grupo de volumes, uma caixa de diálogo de confirmação será exibida se você selecionar uma unidade que faça com que o pool ou grupo de volumes não tenha mais um ou mais dos seguintes atributos:

   ◦ Proteção contra perda de prateleira*
   ◦ Proteção contra perda de gaveta
   ◦ Capacidade de encriptação total do disco
   ◦ Capacidade de garantia de dados
   ◦ Capacidade DULBE

   Atualmente, a caixa de diálogo de confirmação não é exibida ao adicionar unidades a um pool com proteção contra perda de prateleira ou proteção contra perda de gaveta.

1. Para continuar, clique em **Yes**; caso contrário, clique em **Cancel**.

**Resultados**

Depois de adicionar as unidades não atribuídas a um pool ou grupo de volumes, os dados em cada volume do pool ou grupo de volumes são redistribuídos para incluir as unidades adicionais.

## Gerenciar o storage

### Verifique a redundância de volume

Sob a orientação do suporte técnico ou conforme instruído pelo Recovery Guru, você pode verificar a redundância em um volume em um pool ou grupo de volumes para

determinar se os dados nesse volume são consistentes.

Os dados de redundância são usados para reconstruir rapidamente informações em uma unidade de substituição se uma das unidades no pool ou grupo de volumes falhar.

**Antes de começar**

- O status do pool ou grupo de volume deve ser ideal.
- O pool ou grupo de volume não deve ter operações de modificação de volume em andamento.
- Você pode verificar a redundância em qualquer nível RAID, exceto no RAID 0, porque o RAID 0 não tem redundância de dados.

> Verifique a redundância de volume somente quando instruído a fazê-lo pelo Recovery Guru e sob a orientação do suporte técnico.

**Sobre esta tarefa**

Você pode executar essa verificação somente em um pool ou grupo de volume de cada vez. Uma verificação de redundância de volume executa as seguintes ações:

- Verifica os blocos de dados em um volume RAID 3, um volume RAID 5 ou um volume RAID 6 e verifica as informações de redundância para cada bloco. (O RAID 3 só pode ser atribuído a grupos de volume usando a interface de linha de comando.)
- Compara os blocos de dados em unidades espelhadas RAID 1.
- Retorna erros de redundância se o firmware do controlador determinar que os dados são inconsistentes.

> Executar imediatamente uma verificação de redundância no mesmo pool ou grupo de volumes pode causar um erro. Para evitar esse problema, aguarde um a dois minutos antes de executar outra verificação de redundância no mesmo pool ou grupo de volume.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione **tarefas incomuns › verificar redundância de volume**.

   A caixa de diálogo verificar redundância é exibida.

3. Selecione os volumes que pretende verificar e, em seguida, escreva `check` para confirmar que pretende efetuar esta operação.
4. Clique em **verificar**.

   A operação de verificação de redundância de volume é iniciada. Os volumes no pool ou grupo de volumes são verificados sequencialmente, começando no topo da tabela na caixa de diálogo. Estas ações ocorrem à medida que cada volume é digitalizado:

   - O volume é selecionado na tabela de volumes.
   - O status da verificação de redundância é mostrado na coluna **Status**.
   - A verificação pára em qualquer Mídia ou erro de paridade encontrado e, em seguida, relata o erro.

**Mais sobre o status da verificação de redundância**

| Estado | Descrição |
|---|---|
| Pendente | Este é o primeiro volume a ser verificado e você não clicou em Iniciar para iniciar a verificação de redundância.<br><br>ou<br><br>A operação de verificação de redundância está sendo executada em outros volumes no pool ou grupo de volumes. |
| Verificação | O volume está passando pela verificação de redundância. |
| Aprovado | O volume passou na verificação de redundância. Não foram detetadas inconsistências nas informações de redundância. |
| Falha | O volume falhou na verificação de redundância. Inconsistências foram detetadas nas informações de redundância. |
| Erro de material | O suporte de dados da unidade está com defeito e é ilegível. Siga as instruções apresentadas no Recovery Guru. |
| Erro de paridade | A paridade não é o que deve ser para uma determinada parte dos dados. Um erro de paridade é potencialmente grave e pode causar uma perda permanente de dados. |

5. Clique em **Concluído** após o último volume no pool ou grupo de volumes ter sido verificado.

### Excluir pool ou grupo de volume

É possível excluir um pool ou grupo de volumes para criar mais capacidade não atribuída, que pode ser reconfigurada para atender às necessidades de armazenamento de aplicativos.

**Antes de começar**

- Você deve ter feito backup dos dados em todos os volumes no pool ou grupo de volumes.
- Você deve ter parado todas as entradas/saídas (e/S).
- Você deve desmontar qualquer sistema de arquivos nos volumes.
- Você deve ter excluído quaisquer relações de espelhamento no pool ou grupo de volumes.
- Você deve ter parado qualquer operação de cópia de volume em andamento para o pool ou grupo de volumes.
- O pool ou grupo de volume não deve estar participando de uma operação de espelhamento assíncrono.
- As unidades no grupo de volumes não devem ter uma reserva persistente.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione um pool ou grupo de volume na lista.

   Você pode selecionar apenas um pool ou grupo de volume de cada vez. Role a lista para baixo para ver pools ou grupos de volume adicionais.

3. Selecione **tarefas incomuns › Excluir** e confirme.

**Resultados**

O System Manager executa as seguintes ações:

- Exclui todos os dados no pool ou grupo de volumes.
- Exclui todas as unidades associadas ao pool ou grupo de volumes.
- Desatribui as unidades associadas, o que permite reutilizá-las em pools ou grupos de volumes novos ou existentes.

### Consolide a capacidade livre para um grupo de volumes

Use a opção consolidar capacidade livre para consolidar extensões livres existentes em um grupo de volumes selecionado. Ao executar esta ação, você pode criar volumes adicionais a partir da quantidade máxima de capacidade livre em um grupo de volumes.

**Antes de começar**

- O grupo de volume deve conter pelo menos uma área de capacidade livre.
- Todos os volumes no grupo de volumes devem estar online e em ótimo estado.
- As operações de modificação de volume não devem estar em andamento, como alterar o tamanho do segmento de um volume.

**Sobre esta tarefa**

Não é possível cancelar a operação depois de iniciada. Seus dados permanecem acessíveis durante a operação de consolidação.

Você pode iniciar a caixa de diálogo consolidar capacidade livre usando qualquer um dos seguintes métodos:

- Quando é detetada pelo menos uma área de capacidade livre para um grupo de volumes, a recomendação "consolidar capacidade livre" aparece na página inicial na área de notificação. Clique no link **consolidar capacidade livre** para iniciar a caixa de diálogo.
- Também é possível iniciar a caixa de diálogo consolidar capacidade livre a partir da página pools e grupos de volume, conforme descrito na tarefa a seguir.

### Mais sobre áreas de capacidade livre

Uma área de capacidade livre é a capacidade livre que pode resultar da exclusão de um volume ou da não utilização de toda a capacidade livre disponível durante a criação do volume. Quando você cria um volume em um grupo de volumes que tenha uma ou mais áreas de capacidade livre, a capacidade do volume é limitada à maior área de capacidade livre nesse grupo de volumes. Por exemplo, se um grupo de volume tiver um total de 15 GiB de capacidade livre, e a maior área de capacidade livre for de 10 GiB, o maior volume que você pode criar é de 10 GiB.

Você consolida a capacidade livre em um grupo de volumes para melhorar o desempenho de gravação. A capacidade livre do seu grupo de volumes ficará fragmentada ao longo do tempo à medida que o host grava, modifica e exclui arquivos. Eventualmente, a capacidade disponível não será localizada em um único bloco contíguo, mas será espalhada em pequenos fragmentos pelo grupo de volumes. Isso causa mais fragmentação de arquivos, já que o host deve gravar novos arquivos como fragmentos para encaixá-los nos intervalos disponíveis de clusters livres.

Ao consolidar a capacidade gratuita em um grupo de volumes selecionado, você notará o desempenho aprimorado do sistema de arquivos sempre que o host gravar novos arquivos. O processo de consolidação também ajudará a evitar que novos arquivos sejam fragmentados no futuro.

### Passos

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione o grupo de volumes com capacidade livre que deseja consolidar e, em seguida, selecione **tarefas incomuns › consolidar volume group free capacity**.

   A caixa de diálogo consolidar capacidade livre é exibida.

3. Digite `consolidate` para confirmar que deseja executar esta operação.
4. Clique em **consolidar**.

   O System Manager começa a consolidar (desfragmentar) as áreas de capacidade livre do grupo de volumes em um valor contíguo para tarefas de configuração de armazenamento subsequentes.

### Depois de terminar

Selecione **Home › View Operations in Progress** (Ver operações em curso) para ver o progresso da operação consolidar capacidade livre. Esta operação pode ser demorada e pode afetar o desempenho do sistema.

### Exportar/importar grupos de volume

A migração do grupo de volumes permite exportar um grupo de volumes para que você possa importar o grupo de volumes para um storage array diferente.

A função Exportar/Importar não é suportada na interface do utilizador do Gestor de sistema do SANtricity. Você deve usar a interface de linha de comando (CLI) para exportar/importar um grupo de volumes para um storage array diferente.

### Ligue as luzes de localização em um pool, grupo de volumes ou cache SSD

Você pode localizar unidades para identificar fisicamente todas as unidades que compõem um pool selecionado, grupo de volumes ou cache SSD. Um indicador LED

acende-se em cada unidade no pool selecionado, grupo de volume ou cache SSD.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione o pool, grupo de volume ou cache SSD que você deseja localizar e clique em **mais › Ativar luzes de localização**.

   É exibida uma caixa de diálogo que indica que as luzes nas unidades que compõem o pool selecionado, o grupo de volume ou o cache SSD estão ativados.

3. Depois de localizar as unidades com êxito, clique em **Desligar**.

### Remova a capacidade de um pool ou cache SSD

Você pode remover unidades para diminuir a capacidade de um pool existente ou cache SSD.

Depois de remover unidades, os dados em cada volume do pool ou cache SSD são redistribuídos para as unidades restantes. As unidades removidas tornam-se não atribuídas e sua capacidade se torna parte da capacidade livre total do storage array.

**Sobre esta tarefa**

Siga estas diretrizes ao remover a capacidade:

- Você não pode remover a última unidade em um cache SSD sem primeiro excluir o cache SSD.
- Não é possível reduzir o número de unidades em um pool para ser inferior a 11 unidades.
- Você pode remover um máximo de 12 unidades de cada vez. Se precisar remover mais de 12 unidades, repita o procedimento.
- Não é possível remover unidades se não houver capacidade livre suficiente no pool ou cache SSD para conter os dados, quando esses dados são redistribuídos para as unidades restantes no pool ou cache SSD.

**Leia sobre possíveis impactos no desempenho**

- Remover unidades de um pool ou cache SSD pode resultar em desempenho de volume reduzido.
- A capacidade de preservação não é consumida quando você remove a capacidade de um pool ou cache SSD. No entanto, a capacidade de preservação pode diminuir com base no número de unidades restantes no pool ou cache SSD.

**Leia sobre impactos em unidades com capacidade de segurança**

- Se você remover a última unidade que não é segura, o pool será deixado com todas as unidades seguras. Nesta situação, você tem a opção de ativar a segurança para o pool.
- Se você remover a última unidade que não é capaz de Data Assurance (DA), o pool é deixado com todas as unidades compatíveis com DA.

> Quaisquer novos volumes que você criar no pool serão capazes de DA. Se você quiser que os volumes existentes sejam capazes de DA, você precisa excluir e recriar o volume.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione o pool ou cache SSD e clique em **mais › Remover capacidade**.

   A caixa de diálogo Remover capacidade é exibida.

3. Selecione uma ou mais unidades na lista.

   À medida que você seleciona ou desseleciona unidades na lista, o campo **capacidade total selecionada** é atualizado. Este campo mostra a capacidade total do pool ou cache SSD resultante depois de remover as unidades selecionadas.

4. Clique em **Remover** e confirme que deseja remover as unidades.

   A capacidade recém-reduzida do pool ou cache SSD é refletida na visualização pools e grupos de volume.

## Modifique as configurações do pool e do grupo

### Altere as configurações de um pool

Você pode editar as configurações de um pool, incluindo seu nome, configurações de alertas de capacidade, prioridades de modificação e capacidade de preservação.

**Sobre esta tarefa**

Esta tarefa descreve como alterar as configurações de um pool.

> Não é possível alterar o nível RAID de um pool usando a interface do System Manager. O System Manager configura automaticamente pools como RAID 6.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione o pool que você deseja editar e clique em **Exibir/Editar configurações**.

   A caixa de diálogo Pool Setting (Definição do pool) é exibida.

3. Selecione a guia **Configurações** e edite as configurações do pool conforme apropriado.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| Nome | Você pode alterar o nome fornecido pelo usuário do pool. Especificar um nome para um pool é necessário. |
| Alertas de capacidade | Você pode enviar notificações de alerta quando a capacidade livre em um pool atingir ou exceder um limite especificado. Quando os dados armazenados no pool excedem o limite especificado, o System Manager envia uma mensagem, permitindo que você adicione mais espaço de armazenamento ou exclua objetos desnecessários.<br><br>Os alertas são exibidos na área notificações no Painel de instrumentos e podem ser enviados do servidor para administradores por e-mail e mensagens de intercetação SNMP.<br><br>Você pode definir os seguintes alertas de capacidade:<br><br>• **Alerta crítico** — este alerta crítico notifica-o quando a capacidade livre no pool atinge ou excede o limite especificado. Utilize os controlos giratórios para ajustar a percentagem de limiar. Selecione a caixa de verificação para desativar esta notificação.<br>• **Alerta antecipado** — este alerta antecipado notifica você quando a capacidade livre em um pool está atingindo um limite especificado. Utilize os controlos giratórios para ajustar a percentagem de limiar. Selecione a caixa de verificação para desativar esta notificação. |

| Definição | Descrição |
| --- | --- |
| Prioridades de modificação | Você pode especificar os níveis de prioridade para operações de modificação em um pool em relação ao desempenho do sistema. Uma prioridade mais alta para operações de modificação em um pool faz com que uma operação seja concluída mais rápido, mas pode diminuir o desempenho de e/S do host. Uma prioridade menor faz com que as operações demorem mais tempo, mas a performance de e/S do host é menos afetada.<br><br>Você pode escolher entre cinco níveis de prioridade: Mais baixo, baixo, médio, alto e mais alto. Quanto maior for o nível de prioridade, maior será o impacto na e/S do host e no desempenho do sistema.<br><br>• **Prioridade de reconstrução crítica** — esta barra deslizante determina a prioridade de uma operação de reconstrução de dados quando várias falhas de unidade resultam em uma condição em que alguns dados não têm redundância e uma falha de unidade adicional pode resultar em perda de dados.<br>• **Prioridade de reconstrução degradada** — esta barra deslizante determina a prioridade da operação de reconstrução de dados quando ocorreu uma falha na unidade, mas os dados ainda têm redundância e uma falha adicional na unidade não resulta na perda de dados.<br>• **Prioridade de operação em segundo plano** — esta barra deslizante determina a prioridade das operações de fundo do pool que ocorrem enquanto o pool está em um estado ideal. Essas operações incluem expansão dinâmica de volume (DVE), formato de disponibilidade instantânea (IAF) e migração de dados para uma unidade substituída ou adicionada. |

| Definição | Descrição |
| --- | --- |
| Capacidade de preservação ("capacidade de otimização" para o EF600 ou EF300) | **Capacidade de preservação** — você pode definir o número de unidades para determinar a capacidade reservada no pool para dar suporte a possíveis falhas de unidade. Quando ocorre uma falha de unidade, a capacidade de preservação é utilizada para manter os dados reconstruídos. Os pools usam capacidade de preservação durante o processo de reconstrução de dados em vez de unidades hot spare, que são usadas em grupos de volume.<br><br>Utilize os controlos giratórios para ajustar o número de unidades. Com base no número de unidades, a capacidade de preservação no pool aparece ao lado da caixa giratória.<br><br>Tenha em mente as seguintes informações sobre a capacidade de preservação.<br><br>• Como a capacidade de preservação é subtraída da capacidade livre total de um pool, a quantidade de capacidade que você reserva afeta a quantidade de capacidade livre disponível para criar volumes. Se você especificar 0 para a capacidade de preservação, toda a capacidade livre no pool será usada para a criação de volume.<br>• Se você diminuir a capacidade de preservação, aumentará a capacidade que pode ser usada para volumes de pool.<br><br>**Capacidade de otimização adicional** (somente arrays EF600 e EF300) — quando um pool é criado, uma capacidade de otimização recomendada é gerada que fornece um equilíbrio entre capacidade disponível versus desempenho e vida útil do desgaste. Você pode ajustar esse equilíbrio movendo o controle deslizante para a direita para melhor desempenho e vida útil do desgaste à custa do aumento da capacidade disponível, ou movendo-o para a esquerda para maior capacidade disponível à custa de um melhor desempenho e vida útil do desgaste.<br><br>As unidades SSD terão vida útil mais longa e melhor desempenho máximo de gravação quando uma parte de sua capacidade não for alocada. Para unidades associadas a um pool, a capacidade não alocada é composta pela capacidade de preservação de um pool, pela capacidade livre (capacidade não usada por volumes) e por uma parte da capacidade utilizável reservada como capacidade de otimização adicional. A capacidade de otimização adicional garante um nível mínimo de capacidade de otimização, reduzindo a capacidade utilizável, e, como tal, não está disponível para criação de volume. |

4. Clique em **Salvar**.

### Alterar as definições de configuração para um grupo de volumes

Você pode editar as configurações de um grupo de volumes, incluindo seu nome e nível RAID.

#### Antes de começar

Se você estiver alterando o nível RAID para acomodar as necessidades de desempenho dos aplicativos que estão acessando o grupo de volumes, certifique-se de atender aos seguintes pré-requisitos:

- O grupo de volume tem de estar no estado ideal.
- Você precisa ter capacidade suficiente no grupo de volumes para converter para o novo nível RAID.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione o grupo de volume que deseja editar e clique em **Exibir/Editar configurações**.

   A caixa de diálogo Configurações do grupo de volume é exibida.

3. Selecione a guia **Configurações** e edite as configurações do grupo de volume conforme apropriado.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| Nome | Pode alterar o nome fornecido pelo utilizador do grupo de volumes. É necessário especificar um nome para um grupo de volumes. |
| Nível RAID | Selecione o novo nível RAID no menu suspenso.<br><br>• **RAID 0 striping** — oferece alto desempenho, mas não fornece redundância de dados. Se uma única unidade falhar no grupo de volumes, todos os volumes associados falharão e todos os dados serão perdidos. Um grupo RAID de distribuição combina duas ou mais unidades em uma unidade lógica grande.<br>• **Espelhamento RAID 1** - oferece alto desempenho e a melhor disponibilidade de dados, e é adequado para armazenar dados confidenciais em um nível corporativo ou pessoal. Protege seus dados espelhando automaticamente o conteúdo de uma unidade para a segunda unidade no par espelhado. Ele fornece proteção em caso de falha única de unidade.<br>• **RAID 10 striping/mirroring** — fornece uma combinação de RAID 0 (striping) e RAID 1 (espelhamento), e é obtida quando quatro ou mais unidades são selecionadas. O RAID 10 é adequado para aplicações de transações de alto volume, como um banco de dados, que exigem alto desempenho e tolerância a falhas.<br>• **RAID 5** — ideal para ambientes multiusuário (como armazenamento de banco de dados ou sistema de arquivos) onde o tamanho típico de e/S é pequeno e há uma alta proporção de atividade de leitura.<br>• **RAID 6** — ideal para ambientes que exigem proteção de redundância além do RAID 5, mas que não exigem alto desempenho de gravação.<br><br>O RAID 3 só pode ser atribuído a grupos de volume usando a interface de linha de comando (CLI).<br><br>Quando você altera o nível RAID, você não pode cancelar essa operação depois que ela for iniciada. Durante a alteração, seus dados permanecem disponíveis. |

| Definição | Descrição |
| --- | --- |
| Capacidade de otimização (somente arrays EF600) | Quando um grupo de volumes é criado, é gerada uma capacidade de otimização recomendada que fornece um equilíbrio entre capacidade disponível e desempenho e vida útil do desgaste. Você pode ajustar esse equilíbrio movendo o controle deslizante para a direita para melhor desempenho e vida útil do desgaste à custa do aumento da capacidade disponível, ou movendo-o para a esquerda para maior capacidade disponível à custa de um melhor desempenho e vida útil do desgaste.<br><br>As unidades SSD terão vida útil mais longa e melhor desempenho máximo de gravação quando uma parte de sua capacidade não for alocada. Para unidades associadas a um grupo de volumes, a capacidade não alocada é composta pela capacidade livre de um grupo (capacidade não usada por volumes) e uma parte da capacidade utilizável reservada como capacidade de otimização adicional. A capacidade de otimização adicional garante um nível mínimo de capacidade de otimização, reduzindo a capacidade utilizável, e, como tal, não está disponível para criação de volume. |

4. Clique em **Salvar**.

   Uma caixa de diálogo de confirmação será exibida se a capacidade for reduzida, a redundância de volume for perdida ou a proteção contra perda de gaveta/gaveta for perdida como resultado da alteração do nível RAID. Selecione **Sim** para continuar; caso contrário, clique em **não**.

**Resultados**

Se você alterar o nível RAID para um grupo de volumes, o System Manager alterará os níveis RAID de cada volume que compreende o grupo de volumes. O desempenho pode ser ligeiramente afetado durante a operação.

### Ative ou desative o provisionamento de recursos em grupos de volumes e pools existentes

Para quaisquer unidades compatíveis com DULBE, você pode ativar ou desativar o provisionamento de recursos em volumes existentes em um pool ou grupo de volumes.

O provisionamento de recursos é um recurso disponível nas matrizes de armazenamento EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente sem processo de inicialização em segundo plano. Todos os blocos de unidade atribuídos ao volume são deslocalizados (não mapeados), o que pode melhorar a vida útil do SSD e aumentar o desempenho máximo de gravação.

Por padrão, o provisionamento de recursos é ativado em sistemas onde as unidades suportam DULBE. Não há necessidade de ativar o provisionamento de recursos, a menos que você o tenha desativado anteriormente.

**Antes de começar**

- Você precisa ter um storage array EF300 ou EF600.
- Você precisa ter grupos ou pools de volume SSD, em que todas as unidades sejam compatíveis com a funcionalidade de recuperação de erro de ativação de erro de bloco lógico (DULBE) desalocada ou não escrita do NVMe. Caso contrário, a opção de provisionamento de recursos não está disponível.

**Sobre esta tarefa**

Quando você ativa o provisionamento de recursos para grupos de volumes e pools existentes, todos os volumes no grupo ou pool de volumes selecionado são alterados para permitir que os blocos sejam deslocalizados. Esse processo pode envolver uma operação em segundo plano para garantir uma alocação consistente na granularidade unmap. Esta operação não desmapeia nenhum espaço. Uma vez concluída a operação em segundo plano, o sistema operacional precisa desmapear quaisquer blocos não utilizados para criar espaço livre.

Quando você desativa o provisionamento de recursos para grupos ou pools de volumes existentes, uma operação em segundo plano reescreve todos os blocos lógicos em cada volume. Os dados existentes permanecem intactos. As gravações mapearão ou provisionarão os blocos nas unidades associadas ao grupo de volumes ou pool.

> Para novos grupos de volumes e pools, você pode ativar ou desativar o provisionamento de recursos do **Configurações › sistema › Configurações adicionais › Ativar/Desativar volumes provisionados por recursos**.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione um pool ou grupo de volume na lista.

   Você pode selecionar apenas um pool ou grupo de volume de cada vez. Role a lista para baixo para ver pools ou grupos de volume adicionais.

3. Selecione **Uncommon Tasks** e, em seguida, **Enable resource Provisioning** (Ativar provisionamento de recursos) ou **Disable resource Provisioning** (Desativar provisionamento de recursos).
4. Na caixa de diálogo, confirme a operação.

> **Se você reativou o DULBE** — após a conclusão da operação em segundo plano, talvez seja necessário reiniciar o host para que ele detete as alterações de configuração do DULBE e remonte todos os sistemas de arquivos.

**Ative ou desative o provisionamento de recursos para novos grupos de volumes ou pools**

Se você desativou anteriormente o recurso padrão para o provisionamento de recursos, poderá reativá-lo para quaisquer novos grupos de volume SSD ou pools criados. Também pode desativar novamente a definição.

O provisionamento de recursos é um recurso disponível nas matrizes de armazenamento EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente sem processo de inicialização em segundo plano. Todos os blocos de unidade atribuídos ao volume são deslocalizados (não mapeados), o que pode melhorar a vida útil do SSD e aumentar o desempenho máximo de gravação.

> Por padrão, o provisionamento de recursos é ativado em sistemas onde as unidades suportam DULBE.

**Antes de começar**

- Você precisa ter um storage array EF300 ou EF600.
- Você precisa ter grupos ou pools de volume SSD, em que todas as unidades sejam compatíveis com a funcionalidade de recuperação de erro de ativação de erro de bloco lógico (DULBE) desalocada ou não

escrita do NVMe.

**Sobre esta tarefa**

Quando você rehabilita o provisionamento de recursos para novos grupos de volumes ou pools, apenas os grupos de volumes e pools recém-criados são afetados. Todos os grupos de volumes e pools existentes com provisionamento de recursos habilitado permanecerão inalterados.

**Passos**

1. Selecione **Definições › sistema**.
2. Role para baixo até **Configurações adicionais** e clique em **Ativar/Desativar volumes provisionados por recursos**.

   A descrição da configuração indica se o provisionamento de recursos está ativado ou desativado no momento.

3. Na caixa de diálogo, confirme a operação.

**Resultados**

A ativação ou desativação do provisionamento de recursos afeta apenas novos pools de SSD ou grupos de volume criados por você. Os pools ou grupos de volumes existentes permanecem inalterados.

### Ative a segurança para um pool ou grupo de volumes

Você pode ativar o Drive Security para um pool ou grupo de volumes para impedir o acesso não autorizado aos dados nas unidades contidas no pool ou grupo de volumes. O acesso de leitura e gravação para as unidades só está disponível através de um controlador configurado com uma chave de segurança.

**Antes de começar**

- O recurso Segurança da unidade deve estar ativado.
- Uma chave de segurança deve ser criada.
- O pool ou grupo de volume deve estar em um estado ideal.
- Todas as unidades no pool ou grupo de volumes devem ser unidades com capacidade de segurança.

**Sobre esta tarefa**

Se você quiser usar o Drive Security, selecione um pool ou grupo de volume que seja seguro. Um pool ou grupo de volumes pode conter unidades com capacidade de segurança e não seguras, mas todas as unidades devem ser seguras para usar seus recursos de criptografia.

Depois de ativar a segurança, você só pode removê-la excluindo o pool ou grupo de volumes e apagando as unidades.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione o pool ou grupo de volume no qual deseja ativar a segurança e clique em **mais › Ativar segurança**.

   A caixa de diálogo confirmar ativação da segurança é exibida.

3. Confirme se deseja ativar a segurança para o pool ou grupo de volumes selecionado e clique em **Ativar**.

# Gerenciar cache SSD

## Como o cache SSD funciona

O recurso cache SSD é uma solução baseada em controlador que armazena em cache os dados acessados com mais frequência ("dados ativos") em unidades de estado sólido (SSDs) de baixa latência para acelerar dinamicamente o desempenho do sistema. O cache SSD é usado exclusivamente para leituras de host.

### Cache SSD versus cache primário

Cache SSD é um cache secundário para uso com o cache primário na memória dinâmica de acesso aleatório (DRAM) da controladora.

O cache SSD opera de forma diferente do cache primário:

- Para o cache primário, cada operação de e/S deve encenar dados através do cache para executar a operação.

  No cache primário, os dados são armazenados na DRAM após uma leitura do host.

- Cache SSD é usado apenas se for benéfico colocar os dados no cache para melhorar o desempenho geral do sistema.

  No cache SSD, os dados são copiados de volumes e armazenados em dois volumes RAID internos (um por controlador) que são criados automaticamente quando você cria um cache SSD.

Os volumes RAID internos são usados para fins de processamento de cache interno. Esses volumes não são acessíveis ou exibidos na interface do usuário. No entanto, esses dois volumes contam com o número total de volumes permitidos no storage array.

### Como o cache SSD é usado

O armazenamento em cache inteligente coloca os dados em uma unidade de latência inferior. Assim, as respostas a futuras solicitações desses dados podem ocorrer muito mais rapidamente. Se um programa solicitar dados que estão no cache (chamado de "hit de cache"), a unidade de baixa latência pode atender essa transação. Caso contrário, ocorre uma "falta de cache" e os dados devem ser acessados a partir da unidade original, mais lenta. À medida que mais acessos ao cache ocorrem, o desempenho geral melhora.

Quando um programa host acessa as unidades do storage array, os dados são armazenados no cache SSD. Quando os mesmos dados são acessados pelo programa host novamente, eles são lidos a partir do cache SSD em vez dos discos rígidos. Os dados comumente acessados são armazenados no cache SSD. Os discos rígidos só são acessados quando os dados não podem ser lidos a partir do cache SSD.

O cache SSD é usado apenas quando é benéfico colocar os dados no cache para melhorar o desempenho geral do sistema.

Quando a CPU precisa processar dados de leitura, segue as etapas abaixo:

1. Verifique o cache DRAM.
2. Se não for encontrado no cache DRAM, verifique cache SSD.
3. Se não for encontrado no cache SSD, então obtenha do disco rígido. Se os dados forem considerados valiosos para armazenar em cache, copie para o cache SSD.

#### Melhor desempenho

Copiar os dados mais acessados (hot spot) para cache SSD permite uma operação mais eficiente do disco rígido, latência reduzida e velocidades de leitura e gravação aceleradas. O uso de SSDs de alto desempenho para armazenar dados em cache de volumes de HDD melhora o desempenho de e/S e os tempos de resposta.

Mecanismos simples de e/S de volume são usados para mover dados de e para o cache SSD. Depois que os dados são armazenados em cache e armazenados nos SSDs, as leituras subsequentes desses dados são executadas no cache SSD, eliminando assim a necessidade de acessar o volume do HDD.

#### Cache SSD e o recurso Segurança da unidade

Para usar cache SSD em um volume que também esteja usando a Segurança da unidade (ativada para segurança), os recursos de segurança da unidade do volume e o cache SSD devem corresponder. Se não corresponderem, o volume não será ativado com segurança.

#### Implementar cache SSD

Para implementar o cache SSD, faça o seguinte:

1. Crie o cache SSD.
2. Associe o cache SSD aos volumes para os quais você deseja implementar o armazenamento em cache de leitura SSD.

> Qualquer volume atribuído para usar o cache SSD de um controlador não é elegível para uma transferência automática de balanceamento de carga.

### Restrições de cache SSD

Saiba mais sobre as restrições ao usar cache SSD em seu storage array.

#### Restrições

- Qualquer volume atribuído para usar o cache SSD de um controlador não é elegível para uma transferência automática de balanceamento de carga.
- Atualmente, apenas um cache SSD é suportado por storage array.
- A capacidade máxima de cache SSD utilizável em um storage array é de 10 TB.
- O cache SSD não é suportado em imagens instantâneas.
- Se você importar ou exportar volumes que estejam habilitados ou desativados em cache SSD, os dados em cache não serão importados ou exportados.
- Você não pode remover a última unidade em um cache SSD sem primeiro excluir o cache SSD.

#### Restrições com Segurança da Unidade

- Você pode ativar a segurança no cache SSD somente quando você criar o cache SSD. Não é possível ativar a segurança mais tarde como pode num volume.
- Se você misturar unidades que são seguras com unidades que não são seguras no cache SSD, não será possível ativar a segurança da unidade para essas unidades.
- Os volumes habilitados para segurança devem ter um cache SSD seguro habilitado.

### Criar cache SSD

Para acelerar dinamicamente a performance do sistema, você pode usar o recurso cache SSD para armazenar em cache os dados acessados com mais frequência ("dados ativos") em unidades de estado sólido (SSDs) de baixa latência. O cache SSD é usado exclusivamente para leituras de host.

#### Antes de começar

Seu storage array deve conter algumas unidades SSD.

#### Sobre esta tarefa

Ao criar um novo cache SSD, você pode usar uma única unidade ou várias unidades. Como o cache de leitura está no storage array, o armazenamento em cache é compartilhado em todos os aplicativos que usam o storage array. Você seleciona os volumes que deseja armazenar em cache e, em seguida, o armazenamento em cache é automático e dinâmico.

Siga estas diretrizes ao criar um novo cache SSD.

- Você pode ativar a segurança no cache SSD somente quando você estiver criando, e não mais tarde.
- Apenas um cache SSD é suportado por storage array.
- Se apenas um volume tiver o cache SSD ativado, todo o cache SSD será atribuído à controladora que possui esse volume.
- A capacidade máxima de cache SSD utilizável em um storage array depende da capacidade de cache principal da controladora.
- O cache SSD não é suportado em imagens instantâneas.
- Se você importar ou exportar volumes que estejam habilitados ou desativados em cache SSD, os dados em cache não serão importados ou exportados.
- Qualquer volume atribuído para usar o cache SSD de um controlador não é elegível para uma transferência automática de balanceamento de carga.
- Se os volumes associados estiverem habilitados para segurança, crie um cache SSD habilitado para segurança.

#### Passos

1. Selecione **armazenamento › pools & grupos de volume**.
2. Clique em **criar › cache SSD**.

   A caixa de diálogo criar cache SSD é exibida.

3. Digite um nome para o cache SSD.
4. Selecione o candidato cache SSD que você deseja usar com base nas seguintes caraterísticas.

| Característica | Utilização |
| --- | --- |
| Capacidade | Mostra a capacidade disponível em GiB. Selecione a capacidade para as necessidades de armazenamento da sua aplicação.<br><br>A capacidade máxima para cache SSD depende da capacidade de cache principal da controladora. Se você alocar mais do que o valor máximo para cache SSD, qualquer capacidade extra será inutilizável.<br><br>A capacidade do cache SSD conta para sua capacidade alocada geral. |
| Total de unidades | Mostra o número de unidades disponíveis para este cache SSD. Selecione o candidato SSD com o número de unidades desejadas. |
| Com capacidade segura | Indica se o candidato à cache SSD é composto inteiramente de unidades com capacidade de segurança, que podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).<br><br>Se você quiser criar um cache SSD habilitado para segurança, procure **Sim - FDE** ou **Sim - FIPS** na coluna compatível com segurança. |
| Ativar a segurança? | Fornece a opção para ativar o recurso de Segurança da Unidade com unidades com capacidade segura. Se você quiser criar um cache SSD habilitado para segurança, marque a caixa de seleção Habilitar segurança .<br><br>Uma vez ativada, a segurança não pode ser desativada. Você pode ativar a segurança no cache SSD somente quando você estiver criando, e não mais tarde. |
| DA capaz | Indica se o Data Assurance (DA) está disponível para este candidato de cache SSD. O Data Assurance (DA) verifica e corrige erros que podem ocorrer à medida que os dados são transferidos através dos controladores para as unidades.<br><br>Se você quiser usar DA, selecione um candidato de cache SSD capaz de DA. Esta opção só está disponível quando a funcionalidade DA tiver sido ativada.<br><br>O cache SSD pode conter unidades com CAPACIDADE DA e não DA, mas todas as unidades devem ser capazes de DA para você usar DA. |

5. Associe o cache SSD aos volumes para os quais você deseja implementar o armazenamento em cache de leitura SSD. Para ativar o cache SSD em volumes compatíveis imediatamente, marque a caixa de seleção **Ativar cache SSD em volumes compatíveis existentes mapeados para hosts** .

   Os volumes são compatíveis se compartilharem os mesmos recursos de Segurança de Unidade e DA.

6. Clique em **criar**.

#### Altere as configurações de cache SSD

Você pode editar o nome do cache SSD e exibir seu status, capacidade máxima e atual,

segurança da unidade e status de garantia de dados e seus volumes e unidades associados.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione o cache SSD que você deseja editar e clique em **Exibir/Editar configurações**.

   A caixa de diálogo Configurações de cache SSD é exibida.

3. Revise ou edite as configurações do cache SSD conforme apropriado.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| Nome | Exibe o nome do cache SSD, que você pode alterar. É necessário um nome para o cache SSD. |
| Caraterísticas | Mostra o status do cache SSD. Os Estados possíveis incluem:<br>• Ideal<br>• Desconhecido<br>• Degradada<br>• Falha (Um estado com falha resulta em um evento de mel crítico.)<br>• Suspenso |
| Capacidades | Mostra a capacidade atual e a capacidade máxima permitida para o cache SSD.<br>A capacidade máxima permitida para o cache SSD depende do tamanho de cache principal da controladora:<br>• Até 1 GiB<br>• 1 GiB a 2 GiB<br>• 2 GiB a 4 GiB<br>• Mais de 4 GiB |
| Segurança e DA | Mostra o status de Segurança da unidade e garantia de dados para o cache SSD.<br>• **Secure-Capable** — indica se o cache SSD é composto inteiramente de unidades seguras. Uma unidade com capacidade segura é uma unidade com autocriptografia que protege os dados contra acesso não autorizado.<br>• **Secure-enabled** — indica se a segurança está ativada no cache SSD.<br>• **DA Capable** — indica se o cache SSD é composto inteiramente de unidades compatíveis com DA. Uma unidade capaz de DA pode verificar e corrigir erros que possam ocorrer à medida que os dados são comunicados entre o host e o storage array. |
| Objetos associados | Mostra os volumes e unidades associados ao cache SSD. |

4. Clique em **Salvar**.

**Exibir estatísticas de cache SSD**

É possível exibir estatísticas do cache SSD, como leituras, gravações, acertos de cache,

porcentagem de alocação de cache e porcentagem de utilização de cache.

As estatísticas nominais, que são um subconjunto das estatísticas detalhadas, são mostradas na caixa de diálogo View SSD Cache Statistics (Exibir estatísticas de cache SSD). Você pode exibir estatísticas detalhadas para o cache SSD somente quando exportar todas as estatísticas SSD para um `.csv` arquivo.

Ao rever e interpretar as estatísticas, tenha em mente que algumas interpretações são derivadas olhando para uma combinação de estatísticas.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione o cache SSD para o qual você deseja exibir estatísticas e clique em **mais › View SSD Cache statistics**.

   A caixa de diálogo View SSD Cache Statistics (Visualizar estatísticas de cache SSD) é exibida e exibe as estatísticas nominais para o cache SSD selecionado.

   **Detalhes do campo**

| Definições | Descrição |
| --- | --- |
| Lê | Mostra o número total de leituras de host dos volumes habilitados para cache SSD. Quanto maior a proporção de leituras para gravações, melhor é a operação do cache. |
| Gravações | O número total de gravações de host nos volumes habilitados para cache SSD. Quanto maior a proporção de leituras para gravações, melhor é a operação do cache. |
| Cache hits | Mostra o número de acessos de cache. |
| Cache atinge % | Mostra a porcentagem de acertos de cache. Este número é derivado de hits de cache / (leituras e gravações). A porcentagem de acerto do cache deve ser superior a 50 por cento para operação efetiva do cache SSD. |
| Alocação de cache % | Mostra a porcentagem de armazenamento em cache SSD que é alocado, expressa como uma porcentagem do armazenamento em cache SSD disponível para este controlador e é derivado de bytes alocados / bytes disponíveis. |
| % De utilização de cache | Mostra a porcentagem de armazenamento em cache SSD que contém dados de volumes ativados, expressos como uma porcentagem de armazenamento em cache SSD alocado. Esse valor representa a utilização ou a densidade do cache SSD. Derivado de bytes alocados / bytes disponíveis. |
| Exportar tudo | Exporta todas as estatísticas de cache SSD para um formato CSV. O arquivo exportado contém todas as estatísticas disponíveis para o cache SSD (nominal e detalhada). |

3. Clique em **Cancelar** para fechar a caixa de diálogo.

## Gerenciar a capacidade reservada

### Como funciona a capacidade reservada

A capacidade reservada é criada automaticamente quando operações de serviço de cópia, como snapshots ou operações de espelhamento assíncrono, são fornecidas para seus volumes.

O objetivo da capacidade reservada é armazenar alterações de dados nesses volumes, caso algo dê errado. Assim como volumes, a capacidade reservada é criada a partir de pools ou grupos de volumes.

#### Copiar objetos de serviço que usam capacidade reservada

A capacidade reservada é o mecanismo de storage subjacente usado por esses objetos de serviço de cópia:

- Grupos de instantâneos
- Leitura/gravação de volumes instantâneos
- Volumes de membros do grupo de consistência
- Volumes de pares espelhados

Ao criar ou expandir esses objetos de serviço de cópia, você deve criar uma nova capacidade reservada a partir de um pool ou grupo de volumes. A capacidade reservada geralmente é de 40% do volume base para operações de snapshot e 20% do volume base para operações de espelhamento assíncrono. A capacidade reservada, no entanto, varia dependendo do número de alterações nos dados originais.

#### Volumes finos e capacidade reservada

Para um volume fino, se a capacidade máxima comunicada de 256 TIB tiver sido atingida, não poderá aumentar a sua capacidade. Certifique-se de que a capacidade reservada do volume fino está definida para um tamanho maior do que a capacidade máxima comunicada. (Um volume fino é sempre provisionado de forma fina, o que significa que a capacidade é alocada à medida que os dados estão sendo gravados no volume.)

Se você criar capacidade reservada usando um thin volume em um pool, revise as seguintes ações e resultados na capacidade reservada:

- Se a capacidade reservada de um volume fino falhar, o próprio volume fino não será automaticamente transferido para o estado Failed (Falha). No entanto, como todas as operações de e/S em um volume fino exigem acesso ao volume de capacidade reservada, as operações de e/S sempre farão com que uma condição de verificação seja retornada ao host solicitante. Se o problema subjacente com o volume de capacidade reservada puder ser resolvido, o volume de capacidade reservada será retornado a um estado ideal e o volume fino ficará funcional novamente.
- Se você usar um volume thin existente para concluir um par espelhado assíncrono, esse volume fino será reinicializado com um novo volume de capacidade reservada. Somente blocos provisionados no lado primário são transferidos durante o processo de sincronização inicial.

#### Alertas de capacidade

O objeto de serviço de cópia tem um aviso de capacidade configurável e um limite de alerta, bem como uma resposta configurável quando a capacidade reservada está cheia.

Quando a capacidade reservada de um volume de objeto de serviço de cópia está próxima do ponto de preenchimento, um alerta é emitido para o usuário. Por padrão, esse alerta é emitido quando o volume da capacidade reservada estiver 75% cheio; no entanto, você pode ajustar esse ponto de alerta para cima ou para baixo, conforme necessário. Se você receber esse alerta, poderá aumentar a capacidade do volume de capacidade reservada nesse momento. Cada objeto de serviço de cópia pode ser configurado independentemente a este respeito.

#### Volumes de capacidade reservados órfãos

Um volume de capacidade reservada órfão é um volume que não está mais armazenando dados para operações de serviço de cópia porque seu objeto de serviço de cópia associado foi excluído. Quando o objeto de serviço de cópia foi excluído, seu volume de capacidade reservada também deve ter sido excluído. No entanto, o volume da capacidade reservada não foi eliminado.

Como os volumes de capacidade reservada órfãos não são acessados por nenhum host, eles são candidatos à recuperação. Exclua manualmente o volume de capacidade reservada órfã para que você possa usar sua capacidade para outras operações.

O System Manager alerta-o sobre volumes de capacidade reservada órfãos com uma mensagem "recuperar capacidade não utilizada" na área notificações na página inicial. Você pode clicar em **recuperar capacidade não utilizada** para exibir a caixa de diálogo recuperar capacidade não utilizada, onde você pode excluir o volume de capacidade reservada órfã.

#### Caraterísticas da capacidade reservada

- A capacidade atribuída à capacidade reservada deve ser considerada durante a criação do volume para manter uma capacidade livre suficiente.
- A capacidade reservada pode ser menor do que o volume base (o tamanho mínimo é de 8 MIB).
- Algum espaço é consumido por metadados, mas é muito pouco (192 KiB), por isso não precisa ser levado em consideração ao determinar o tamanho do volume de capacidade reservada.
- A capacidade reservada não é diretamente legível ou gravável de um host.
- Existe capacidade reservada para cada volume de snapshot de leitura/gravação, grupo de snapshot, volume de membro do grupo de consistência e volume de par espelhado.

### Aumentar a capacidade reservada

Você pode aumentar a capacidade reservada, que é a capacidade alocada fisicamente usada para qualquer operação de serviço de cópia em um objeto de armazenamento.

Para operações de snapshot, geralmente é de 40% do volume base; para operações de espelhamento assíncrono, geralmente é de 20% do volume base. Normalmente, você aumenta a capacidade reservada quando recebe um aviso de que a capacidade reservada do objeto de armazenamento está ficando cheia.

#### Antes de começar

- O volume no pool ou grupo de volumes deve ter um status ideal e não deve estar em nenhum estado de modificação.
- A capacidade livre deve existir no pool ou grupo de volumes que você deseja usar para aumentar a capacidade.

  Se não houver capacidade livre em nenhum pool ou grupo de volumes, você poderá adicionar capacidade não atribuída na forma de unidades não utilizadas a um pool ou grupo de volumes.

**Sobre esta tarefa**

Você pode aumentar a capacidade reservada somente em incrementos de 8 GiB para os seguintes objetos de armazenamento:

- Grupo de instantâneos
- Volume do Snapshot
- Volume do membro do grupo de consistência
- Volume do par espelhado

Use uma porcentagem alta se você acredita que o volume primário sofrerá muitas mudanças ou se a vida útil de uma operação de serviço de cópia específica será muito longa.

Não é possível aumentar a capacidade reservada para um volume instantâneo que seja somente leitura. Somente os volumes snapshot que são leitura-gravação exigem capacidade reservada.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione a guia **capacidade reservada**.
3. Selecione o objeto de armazenamento para o qual deseja aumentar a capacidade reservada e clique em **aumentar a capacidade**.

   A caixa de diálogo aumentar capacidade reservada é exibida.

4. Utilize a caixa de rotação para ajustar a percentagem de capacidade.

   Se a capacidade livre não existir no pool ou no grupo de volumes que contém o objeto de armazenamento selecionado e o array de armazenamento tiver capacidade não atribuída, você poderá criar um novo pool ou grupo de volumes. Em seguida, você pode tentar novamente essa operação usando a nova capacidade livre nesse pool ou grupo de volume.

5. Clique em **aumentar**.

**Resultados**

O System Manager executa as seguintes ações:

- Aumenta a capacidade reservada para o objeto de armazenamento.
- Exibe a capacidade reservada recém-adicionada.

**Diminuir a capacidade reservada**

Você usa a opção diminuir capacidade para diminuir a capacidade reservada para os seguintes objetos de armazenamento: Grupo de snapshot, volume de snapshot e volume de membro do grupo de consistência. Você pode diminuir a capacidade reservada somente pelo(s) valor(s) usado(s) para aumentá-la.

**Antes de começar**

- O objeto de storage deve conter mais de um volume de capacidade reservado.
- O objeto de storage não deve ser um volume de par espelhado.

- Se o objeto de storage for um volume instantâneo, ele deverá ser um volume instantâneo desativado.
- Se o objeto de armazenamento for um grupo de instantâneos, não deve conter quaisquer imagens instantâneas associadas.

**Sobre esta tarefa**

Reveja as seguintes diretrizes:

- Você pode remover volumes de capacidade reservada somente na ordem inversa em que foram adicionados.
- Não é possível diminuir a capacidade reservada para um volume instantâneo que seja somente leitura porque não tem nenhuma capacidade reservada associada. Somente os volumes snapshot que são leitura-gravação exigem capacidade reservada.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Clique na guia **capacidade reservada**.
3. Selecione o objeto de armazenamento para o qual você deseja diminuir a capacidade reservada e clique em **diminuir a capacidade**.

   A caixa de diálogo diminuir capacidade reservada é exibida.

4. Selecione a quantidade de capacidade pela qual você deseja diminuir a capacidade reservada e clique em **diminuir**.

**Resultados**

O System Manager executa as seguintes ações:

- Atualiza a capacidade do objeto de armazenamento.
- Exibe a capacidade reservada recém-atualizada para o objeto de armazenamento.
- Quando você diminui a capacidade de um volume de snapshot, o System Manager faz a transição automática do volume de snapshot para um estado Desativado. Desativado significa que o volume instantâneo não está atualmente associado a uma imagem instantânea e, portanto, não pode ser atribuído a um host para e/S.

### Altere as definições de capacidade reservada para um grupo de instantâneos

Pode alterar as definições de um grupo de instantâneos para alterar o seu nome, as definições de eliminação automática, o número máximo de imagens instantâneas permitidas, o ponto percentual no qual o Gestor do sistema envia uma notificação de alerta de capacidade reservada ou a política a utilizar quando a capacidade reservada atinge a sua percentagem máxima definida.

Durante a criação de um grupo de instantâneos, a capacidade reservada é criada para armazenar os dados de todas as imagens instantâneas contidas no grupo.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Clique na guia **capacidade reservada**.
3. Selecione o grupo de instantâneos que pretende editar e, em seguida, clique em **Ver/Editar definições**.

A caixa de diálogo Configurações do grupo instantâneo é exibida.

4. Altere as definições do grupo de instantâneos conforme adequado.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| **Configurações do grupo de instantâneos** | Nome |
| O nome do grupo instantâneo. É necessário especificar um nome para o grupo de instantâneos. | Eliminação automática |
| Uma definição que mantém o número total de imagens instantâneas no grupo em ou abaixo de um máximo definido pelo utilizador. Quando esta opção está ativada, o Gestor do sistema elimina automaticamente a imagem instantânea mais antiga do grupo sempre que é criado um novo instantâneo, de modo a cumprir o número máximo de imagens instantâneas permitidas para o grupo. | Limite de imagem instantânea |
| Um valor configurável que especifica o número máximo de imagens instantâneas permitidas para um grupo de instantâneos. | Agendamento do Snapshot |
| Se Sim, uma programação é definida para criar automaticamente instantâneos. | • Configurações de capacidade reservada* |

| Definição | Descrição |
| --- | --- |
| Alerta-me quando… | Use a caixa giratório para ajustar o ponto percentual no qual o System Manager envia uma notificação de alerta quando a capacidade reservada para um grupo de instantâneos estiver quase cheia.<br><br>Quando a capacidade reservada para o grupo de instantâneos excede o limite especificado, o System Manager envia um alerta, permitindo que você aumente a capacidade reservada ou exclua objetos desnecessários. |
| Política de capacidade reservada completa | Você pode escolher uma das seguintes políticas:<br><br>• **Limpar imagem de snapshot mais antiga** — o System Manager limpa automaticamente a imagem de snapshot mais antiga do grupo de snapshot, que libera a capacidade reservada da imagem de snapshot para reutilização dentro do grupo.<br>• **Rejeitar gravações no volume base** — quando a capacidade reservada atinge sua porcentagem máxima definida, o System Manager rejeita qualquer solicitação de gravação de e/S para o volume base que acionou o acesso à capacidade reservada. |
| **Objetos associados** | Volume base |
| O nome do volume base utilizado para o grupo. Um volume base é a origem a partir da qual uma imagem instantânea é criada. Pode ser um volume grosso ou fino e é normalmente atribuído a um host. O volume base pode residir em um grupo de volumes ou em um pool de discos. | Imagens instantâneas |

5. Clique em **Salvar** para aplicar as alterações às configurações do grupo de instantâneos.

#### Altere as configurações de capacidade reservada para um volume instantâneo

Você pode alterar as configurações de um volume instantâneo para ajustar o ponto percentual no qual o sistema envia uma notificação de alerta quando a capacidade reservada para um volume instantâneo estiver quase cheia.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Clique na guia **capacidade reservada**.

3. Selecione o volume instantâneo que deseja editar e clique em **Exibir/Editar configurações**.

   A caixa de diálogo Configurações de capacidade reservada do volume instantâneo é exibida.

4. Altere as configurações de capacidade reservada para o volume instantâneo, conforme apropriado.

   **Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| Alerta-me quando… | Use a caixa giratório para ajustar o ponto percentual no qual o sistema envia uma notificação de alerta quando a capacidade reservada para um volume de membro estiver quase cheia.<br><br>Quando a capacidade reservada para o volume instantâneo excede o limite especificado, o sistema envia um alerta, permitindo-lhe tempo para aumentar a capacidade reservada ou eliminar objetos desnecessários. |

5. Clique em **Salvar** para aplicar as alterações às configurações de capacidade reservada do volume instantâneo.

### Altere as configurações de capacidade reservada para um volume de membro do grupo de consistência

Você pode alterar as configurações de um volume de membro do grupo de consistência para ajustar o ponto percentual no qual o System Manager envia uma notificação de alerta quando a capacidade reservada para um volume de membro estiver quase cheia e para alterar a política a ser usada quando a capacidade reservada atingir sua porcentagem máxima definida.

#### Sobre esta tarefa

Alterar as configurações de capacidade reservada para um volume de membro individual também altera as configurações de capacidade reservada para todos os volumes associados a um grupo de consistência.

#### Passos

1. Selecione **armazenamento › pools & grupos de volume**.
2. Clique na guia **capacidade reservada**.
3. Selecione o volume do membro do grupo de consistência que você deseja editar e clique em **Exibir/Editar configurações**.

   A caixa de diálogo Configurações de capacidade reservada do volume do membro é exibida.

4. Altere as configurações de capacidade reservada para o volume do membro, conforme apropriado.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| Alerta-me quando… | Use a caixa giratório para ajustar o ponto percentual no qual o System Manager envia uma notificação de alerta quando a capacidade reservada para um volume de membro estiver quase cheia.<br><br>Quando a capacidade reservada para o volume do membro excede o limite especificado, o System Manager envia um alerta, permitindo-lhe tempo para aumentar a capacidade reservada ou eliminar objetos desnecessários.<br><br>Alterar a configuração Alerta para um volume de membro irá alterá-la para *todos* volumes de membros que pertencem ao mesmo grupo de consistência. |
| Política de capacidade reservada completa | Você pode escolher uma das seguintes políticas:<br><br>• **Limpar imagem de snapshot mais antiga** — o System Manager limpa automaticamente a imagem de snapshot mais antiga do grupo consistência, que libera a capacidade reservada do membro para reutilização dentro do grupo.<br>• **Rejeitar gravações no volume base** — quando a capacidade reservada atinge sua porcentagem máxima definida, o System Manager rejeita qualquer solicitação de gravação de e/S para o volume base que acionou o acesso à capacidade reservada. |

5. Clique em **Salvar** para aplicar suas alterações.

**Resultados**

O System Manager altera as configurações de capacidade reservada para o volume do membro, bem como as configurações de capacidade reservada para todos os volumes do membro no grupo consistência.

### Altere as configurações de capacidade reservada para um volume de par espelhado

Você pode alterar as configurações de um volume de par espelhado para ajustar o ponto percentual no qual o System Manager envia uma notificação de alerta quando a capacidade reservada para um volume de par espelhado estiver quase cheia.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione a guia **capacidade reservada**.
3. Selecione o volume do par espelhado que você deseja editar e clique em **Exibir/Editar configurações**.

   A caixa de diálogo Configurações de capacidade reservada do volume do par espelhado é exibida.

4. Altere as configurações de capacidade reservada para o volume do par espelhado, conforme apropriado.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| Alerta-me quando… | Use a caixa giratório para ajustar o ponto percentual no qual o System Manager envia uma notificação de alerta quando a capacidade reservada para um par espelhado estiver quase cheia.<br><br>Quando a capacidade reservada para o par espelhado excede o limite especificado, o System Manager envia um alerta, permitindo que você aumente a capacidade reservada.<br><br>Alterar a configuração Alerta para um par espelhado altera a configuração Alerta para todos os pares espelhados que pertencem ao mesmo grupo de consistência de espelho. |

5. Clique em **Salvar** para aplicar suas alterações.

### Cancelar imagem instantânea pendente

Você pode cancelar uma imagem instantânea pendente antes de ser concluída. Os instantâneos ocorrem de forma assíncrona, e o status do instantâneo está pendente até que o instantâneo seja concluído. A imagem instantânea é concluída assim que a operação de sincronização for concluída.

#### Sobre esta tarefa

Uma imagem instantânea está em um estado pendente devido às seguintes condições simultâneas:

- O volume base de um grupo de instantâneos ou um ou mais volumes de membros de um grupo de consistência que contém esta imagem de instantâneo é membro de um grupo de espelhos assíncrono.
- O volume ou os volumes estão atualmente em uma operação de sincronização de espelhamento assíncrono.

#### Passos

1. Selecione **armazenamento › pools & grupos de volume**.
2. Clique na guia **capacidade reservada**.
3. Selecione o grupo de instantâneos para o qual pretende cancelar uma imagem de instantâneo pendente e, em seguida, clique em **tarefas incomuns › Cancelar imagem de instantâneo pendente**.
4. Clique em **Sim** para confirmar que deseja cancelar a imagem de instantâneo pendente.

### Eliminar grupo instantâneo

Você exclui um grupo de instantâneos quando deseja excluir permanentemente seus dados e removê-los do sistema. A exclusão de um grupo de snapshot reclama a capacidade reservada para reutilização no pool ou no grupo de volumes.

#### Sobre esta tarefa

Quando um grupo de instantâneos é eliminado, todas as imagens de instantâneos no grupo também são

eliminadas.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Clique na guia **capacidade reservada**.
3. Selecione o grupo de instantâneos que pretende eliminar e, em seguida, clique em **tarefas pouco comuns › Eliminar grupo de instantâneos**.

   É exibida a caixa de diálogo confirmar Excluir grupo de instantâneos.

4. Digite `delete` para confirmar.

**Resultados**

O System Manager executa as seguintes ações:

- Elimina todas as imagens instantâneas associadas ao grupo de instantâneos.
- Desativa todos os volumes instantâneos associados às imagens do grupo de instantâneos.
- Exclui a capacidade reservada que existe para o grupo de instantâneos.

## FAQs

**O que é um grupo de volume?**

Um grupo de volumes é um contentor para volumes com caraterísticas compartilhadas. Um grupo de volumes tem uma capacidade definida e um nível RAID. Você pode usar um grupo de volumes para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um grupo de volumes ou de um pool.)

**O que é uma piscina?**

Um pool é um conjunto de unidades que é agrupado logicamente. Você pode usar um pool para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um pool ou de um grupo de volumes.)

Os pools podem eliminar a necessidade de administradores monitorarem o uso de cada host para determinar quando é provável que eles fiquem sem espaço de armazenamento e evitem interrupções convencionais de redimensionamento de disco. Quando um pool se aproxima do esgotamento, unidades adicionais podem ser adicionadas ao pool sem interrupções e o crescimento da capacidade é transparente para o host.

Com pools, os dados são redistribuídos automaticamente para manter o equilíbrio. Ao distribuir informações de paridade e capacidade extra em todo o pool, cada unidade no pool pode ser usada para reconstruir uma unidade com falha. Essa abordagem não usa unidades hot spare dedicadas; em vez disso, a capacidade de preservação (sobressalente) é reservada em todo o pool. Em caso de falha da unidade, os segmentos em outras unidades são lidos para recriar os dados. Uma nova unidade é escolhida para gravar cada segmento que estava em uma unidade com falha, de modo que a distribuição de dados entre as unidades seja mantida.

**O que é a capacidade reservada?**

A capacidade reservada é a capacidade alocada fisicamente que armazena dados para objetos de serviço de cópia, como imagens snapshot, volumes de membros do grupo de

consistência e volumes de pares espelhados.

O volume de capacidade reservada associado a uma operação de serviço de cópia reside em um pool ou em um grupo de volumes. Você cria capacidade reservada de um pool ou grupo de volumes.

**O que é segurança FDE/FIPS?**

A segurança FDE/FIPS refere-se a unidades com capacidade segura que criptografam dados durante gravações e descriptografam dados durante leituras usando uma chave de criptografia exclusiva. Essas unidades com capacidade de segurança evitam o acesso não autorizado aos dados em uma unidade que é fisicamente removida do storage array.

As unidades com capacidade segura podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard). As unidades FIPS foram submetidas a testes de certificação.

> Para volumes que exigem suporte FIPS, use apenas unidades FIPS. A combinação de unidades FIPS e FDE em um grupo de volumes ou pool resultará no tratamento de todas as unidades como unidades FDE. Além disso, uma unidade FDE não pode ser adicionada ou usada como sobressalente em um grupo de volumes ou pool totalmente FIPS.

**O que é verificação de redundância?**

Uma verificação de redundância determina se os dados em um volume em um pool ou grupo de volumes são consistentes. Os dados de redundância são usados para reconstruir rapidamente informações em uma unidade de substituição se uma das unidades no pool ou grupo de volumes falhar.

Você pode executar essa verificação somente em um pool ou grupo de volume de cada vez. Uma verificação de redundância de volume executa as seguintes ações:

- Verifica os blocos de dados em um volume RAID 3, um volume RAID 5 ou um volume RAID 6 e, em seguida, verifica as informações de redundância para cada bloco. (O RAID 3 só pode ser atribuído a grupos de volume usando a interface de linha de comando.)
- Compara os blocos de dados em unidades espelhadas RAID 1.
- Retorna erros de redundância se os dados forem considerados inconsistentes pelo firmware do controlador.

> Executar imediatamente uma verificação de redundância no mesmo pool ou grupo de volumes pode causar um erro. Para evitar esse problema, aguarde um a dois minutos antes de executar outra verificação de redundância no mesmo pool ou grupo de volume.

**Quais são as diferenças entre pools e grupos de volumes?**

Um pool é semelhante a um grupo de volume, com as seguintes diferenças.

- Os dados em um pool são armazenados aleatoriamente em todas as unidades do pool, ao contrário dos dados em um grupo de volumes, que é armazenado no mesmo conjunto de unidades.
- Um pool apresenta menos degradação da performance quando uma unidade falha e leva menos tempo para reconstruir.

- Uma piscina tem capacidade de preservação incorporada; portanto, não requer unidades hot spare dedicadas.
- Um pool permite que um grande número de unidades seja agrupado.
- Um pool não precisa de um nível RAID especificado.

**Por que eu gostaria de configurar manualmente um pool?**

Os exemplos a seguir descrevem por que você deseja configurar manualmente um pool.

- Se você tiver vários aplicativos em seu storage array e não quiser que eles concorram para os mesmos recursos de unidade, considere criar manualmente um pool menor para um ou mais aplicativos.

  Você pode atribuir apenas um ou dois volumes em vez de atribuir a carga de trabalho a um pool grande que tenha muitos volumes para distribuir os dados. A criação manual de um pool separado dedicado ao workload de uma aplicação específica pode permitir que as operações de storage array tenham performance mais rápida, com menos contenção.

  Para criar manualmente um pool: Selecione **armazenamento** e, em seguida, selecione **pools e grupos de volume**. Na guia All Capacity (todas as capacidades), clique em **Create › Pool** (criar [Pool]).

- Se houver vários pools do mesmo tipo de unidade, uma mensagem será exibida indicando que o System Manager não pode recomendar as unidades para um pool automaticamente. No entanto, você pode adicionar manualmente as unidades a um pool existente.

  Para adicionar manualmente unidades a um pool existente: Na página pools & grupos de volume, selecione o pool e clique em **Adicionar capacidade**.

**Por que os alertas de capacidade são importantes?**

Alertas de capacidade indicam quando adicionar unidades a um pool. Um pool precisa de capacidade livre suficiente para executar com sucesso as operações do storage array. Você pode evitar interrupções nessas operações configurando o System Manager para enviar alertas quando a capacidade livre de um pool atingir ou exceder uma porcentagem especificada.

Você define essa porcentagem quando cria um pool usando a opção **Configuração automática do pool** ou a opção **criar pool**. Se você escolher a opção automática, as configurações padrão determinarão automaticamente quando você receber notificações de alerta. Se você optar por criar manualmente o pool, poderá determinar as configurações de notificação de alerta; ou, se preferir, poderá aceitar as configurações padrão. Você pode ajustar essas configurações mais tarde no **Configurações › Alertas**.

Quando a capacidade livre no pool atinge a porcentagem especificada, uma notificação de alerta é enviada usando o método especificado na configuração de alerta.

**Por que não posso aumentar minha capacidade de preservação?**

Se você criou volumes em toda a capacidade utilizável disponível, talvez não consiga aumentar a capacidade de preservação.

Capacidade de preservação é a quantidade de capacidade (número de unidades) reservada em um pool para dar suporte a possíveis falhas de unidade. Quando um pool é criado, o sistema reserva automaticamente uma

quantidade padrão de capacidade de preservação, dependendo do número de unidades no pool. Se você tiver criado volumes em toda a capacidade utilizável disponível, não poderá aumentar a capacidade de preservação sem adicionar capacidade ao pool adicionando unidades ou excluindo volumes.

Você pode alterar a capacidade de preservação de **pools & grupos de volume**. Selecione o pool que você deseja editar. Clique em **Exibir/Editar configurações** e selecione a guia **Configurações**.

A capacidade de preservação é especificada como um número de unidades, mesmo que a capacidade de preservação real seja distribuída entre as unidades no pool.

**Existe um limite no número de unidades que posso remover de um pool?**

O System Manager define limites para quantas unidades você pode remover de um pool.

- Não é possível reduzir o número de unidades em um pool para ser inferior a 11 unidades.
- Não é possível remover unidades se não houver capacidade livre suficiente no pool para conter os dados das unidades removidas quando esses dados são redistribuídos para as unidades restantes no pool.
- Você pode remover um máximo de 60 unidades de cada vez. Se você selecionar mais de 60 unidades, a opção Remover unidades será desativada. Se precisar remover mais de 60 unidades, repita a operação Remover unidades.

**Quais tipos de Mídia são suportados para uma unidade?**

São suportados os seguintes tipos de material: Unidade de disco rígido (HDD) e disco de estado sólido (SSD).

**Por que algumas unidades não estão aparecendo?**

Na caixa de diálogo Adicionar capacidade, nem todas as unidades estão disponíveis para adicionar capacidade a um pool ou grupo de volumes existente.

As unidades não são qualificadas por nenhum dos seguintes motivos:

- Uma unidade deve ser desatribuída e não ativada para segurança. As unidades que já fazem parte de outro pool, de outro grupo de volume ou configuradas como hot spare não são elegíveis. Se uma unidade não for atribuída, mas estiver ativada para segurança, você deverá apagar manualmente essa unidade para que ela se torne elegível.
- Uma unidade que esteja em um estado não ótimo não é elegível.
- Se a capacidade de uma unidade for muito pequena, ela não será elegível.
- O tipo de Mídia da unidade deve corresponder em um pool ou grupo de volume. Não é possível misturar o seguinte:
  - Unidades de disco rígido (HDDs) com discos de estado sólido (SSDs)
  - NVMe com unidades SAS
  - Unidades com tamanhos de bloco de volume de 512 bytes e 4KiB
- Se um pool ou grupo de volumes contiver todas as unidades com capacidade de segurança, as unidades com capacidade de segurança não serão listadas.
- Se um pool ou grupo de volumes contiver todas as unidades FIPS (Federal Information Processing Standards), as unidades não FIPS não serão listadas.

- Se um pool ou grupo de volumes contiver todas as unidades compatíveis com Data Assurance (DA) e houver pelo menos um volume habilitado PARA DA no pool ou grupo de volumes, uma unidade que não seja capaz de DA não é elegível, portanto, ela não pode ser adicionada a esse pool ou grupo de volumes. No entanto, se não houver um volume habilitado PARA DA no pool ou grupo de volumes, uma unidade que não seja capaz de DA pode ser adicionada a esse pool ou grupo de volumes. Se você decidir misturar essas unidades, lembre-se de que não é possível criar nenhum volume habilitado PARA DA.

A capacidade pode ser aumentada em seu storage array adicionando novas unidades ou excluindo pools ou grupos de volumes.

**Como faço para manter a proteção contra perda de prateleira/gaveta?**

Para manter a proteção contra perda de gaveta/gaveta para um pool ou grupo de volumes, use os critérios especificados na tabela a seguir.

| Nível | Critérios para proteção contra perda de prateleira/gaveta | Número mínimo de prateleiras/gavetas necessário |
|---|---|---|
| Piscina | Para gavetas, o pool não deve conter mais de duas unidades em uma única gaveta.<br><br>Para gavetas, o pool deve incluir um número igual de unidades de cada gaveta. | 6 para prateleiras<br><br>5 para gavetas |
| RAID 6 | O grupo de volumes não contém mais do que duas unidades em um único compartimento ou gaveta. | 3 |
| RAID 3 ou RAID 5 | Cada unidade no grupo de volume está localizada em uma gaveta ou gaveta separada. | 3 |
| RAID 1 | Cada unidade em um par espelhado deve estar localizada em uma gaveta ou gaveta separada. | 2 |
| RAID 0 | Não é possível obter proteção contra perda de prateleira/gaveta. | Não aplicável |

A proteção contra perda de gaveta/gaveta não será mantida se uma unidade já tiver falhado no pool ou no grupo de volumes. Nessa situação, perder o acesso a um compartimento de unidades ou gaveta e, consequentemente, outra unidade no pool ou grupo de volume, causa perda de dados.

**Qual é o posicionamento ideal da unidade para pools e grupos de volume?**

Ao criar pools e grupos de volume, certifique-se de equilibrar a seleção de unidade entre

os slots de unidade superior e inferior.

Para os controladores EF600 e EF300, os slots de unidade 0-11 são conetados a uma ponte PCI, enquanto os slots 12-23 são conetados a uma ponte PCI diferente. Para um desempenho ideal, você deve equilibrar a seleção de unidade para incluir um número aproximadamente igual de unidades dos slots superior e inferior. Esse posicionamento garante que seus volumes não atinjam um limite de largura de banda mais cedo do que o necessário.

#### Que nível RAID é melhor para a minha aplicação?

Para maximizar o desempenho de um grupo de volumes, você deve selecionar o nível RAID apropriado. Você pode determinar o nível RAID apropriado conhecendo as porcentagens de leitura e gravação dos aplicativos que estão acessando o grupo de volumes. Use a página desempenho para obter essas porcentagens.

##### Níveis de RAID e desempenho do aplicativo

O RAID depende de uma série de configurações, chamadas *levels*, para determinar como os dados de usuário e redundância são gravados e recuperados das unidades. Cada nível de RAID fornece recursos de desempenho diferentes. Os aplicativos com uma alta porcentagem de leitura terão bom desempenho usando volumes RAID 5 ou volumes RAID 6 devido ao excelente desempenho de leitura das configurações RAID 5 e RAID 6.

Os aplicativos com uma baixa porcentagem de leitura (com uso intenso de gravação) não funcionam tão bem nos volumes RAID 5 ou RAID 6. O desempenho degradado é o resultado da maneira como um controlador grava dados e dados de redundância nas unidades em um grupo de volumes RAID 5 ou em um grupo de volumes RAID 6.

Selecione um nível RAID com base nas seguintes informações.

**RAID 0**

- **Descrição**
  - Modo de distribuição não redundante.
- **Como funciona**
  - O RAID 0 distribui os dados em todas as unidades do grupo de volumes.
- * Recursos de proteção de dados*
  - O RAID 0 não é recomendado para necessidades de alta disponibilidade. O RAID 0 é melhor para dados não críticos.
  - Se uma única unidade falhar no grupo de volumes, todos os volumes associados falharão e todos os dados serão perdidos.
- **Requisitos de número de unidade**
  - É necessário um mínimo de uma unidade para RAID nível 0.
  - Os grupos de volume RAID 0 podem ter mais de 30 unidades.
  - Você pode criar um grupo de volumes que inclua todas as unidades no storage array.

**RAID 1 ou RAID 10**

- **Descrição**

- Modo striping/mirror.

- **Como funciona**
  - O RAID 1 usa o espelhamento de disco para gravar dados em dois discos duplicados simultaneamente.
  - O RAID 10 usa o particionamento de unidades para distribuir dados em um conjunto de pares de unidades espelhadas.
- * Recursos de proteção de dados*
  - RAID 1 e RAID 10 oferecem alto desempenho e a melhor disponibilidade de dados.
  - RAID 1 e RAID 10 usam espelhamento de unidade para fazer uma cópia exata de uma unidade para outra unidade.
  - Se uma das unidades em um par de unidades falhar, o storage array pode alternar instantaneamente para a outra unidade sem perda de dados ou serviço.
  - Uma única falha de unidade faz com que os volumes associados fiquem degradados. A unidade de espelho permite o acesso aos dados.
  - Uma falha de par de unidade em um grupo de volumes faz com que todos os volumes associados falhem e a perda de dados possa ocorrer.
- **Requisitos de número de unidade**
  - É necessário um mínimo de duas unidades para RAID 1: Uma unidade para os dados do usuário e uma unidade para os dados espelhados.
  - Se você selecionar quatro ou mais unidades, o RAID 10 será configurado automaticamente no grupo de volumes: Duas unidades para dados de usuário e duas unidades para os dados espelhados.
  - Você deve ter um número par de unidades no grupo de volumes. Se você não tiver um número par de unidades e tiver algumas unidades não atribuídas restantes, vá para **pools & grupos de volume** para adicionar unidades adicionais ao grupo de volumes e tente novamente a operação.
  - Os grupos de volumes RAID 1 e RAID 10 podem ter mais de 30 unidades. É possível criar um grupo de volumes que inclua todas as unidades do storage array.

**RAID 5**

- **Descrição**
  - Modo de e/S elevado.
- **Como funciona**
  - Os dados do usuário e as informações redundantes (paridade) são distribuídos pelas unidades.
  - A capacidade equivalente de uma unidade é usada para informações redundantes.
- * Recursos de proteção de dados*
  - Se uma única unidade falhar em um grupo de volumes RAID 5, todos os volumes associados ficarão degradados. As informações redundantes permitem que os dados ainda sejam acessados.
  - Se duas ou mais unidades falharem em um grupo de volumes RAID 5, todos os volumes associados falharão e todos os dados serão perdidos.
- **Requisitos de número de unidade**
  - Você precisa ter no mínimo três unidades no grupo de volumes.
  - Normalmente, você está limitado a um máximo de 30 unidades no grupo de volumes.

### RAID 6

- **Descrição**
  - Modo de e/S elevado.
- **Como funciona**
  - Os dados do usuário e as informações redundantes (paridade dupla) são distribuídos entre as unidades.
  - A capacidade equivalente de duas unidades é usada para informações redundantes.
- * Recursos de proteção de dados*
  - Se uma ou duas unidades falharem em um grupo de volumes RAID 6, todos os volumes associados ficam degradados, mas as informações redundantes permitem que os dados ainda sejam acessados.
  - Se três ou mais unidades falharem em um grupo de volumes RAID 6, todos os volumes associados falharão e todos os dados serão perdidos.
- **Requisitos de número de unidade**
  - Você precisa ter no mínimo cinco unidades no grupo de volumes.
  - Normalmente, você está limitado a um máximo de 30 unidades no grupo de volumes.

Não é possível alterar o nível RAID de um pool. A interface do usuário configura automaticamente pools como RAID 6.

#### Níveis de RAID e proteção de dados

RAID 1, RAID 5 e RAID 6 escrevem dados de redundância no suporte de dados da unidade para tolerância a falhas. Os dados de redundância podem ser uma cópia dos dados (espelhados) ou um código de correção de erros derivado dos dados. Você pode usar os dados de redundância para reconstruir rapidamente as informações em uma unidade de substituição se uma unidade falhar.

Você configura um único nível RAID em um único grupo de volumes. Todos os dados de redundância para esse grupo de volumes são armazenados dentro do grupo de volumes. A capacidade do grupo de volumes é a capacidade agregada das unidades membros menos a capacidade reservada para dados de redundância. A quantidade de capacidade necessária para redundância depende do nível RAID usado.

### O que é o Data Assurance?

A Data Assurance (DA) implementa a norma T10 Protection Information (PI), que aumenta a integridade dos dados verificando e corrigindo erros que possam ocorrer à medida que os dados são transferidos ao longo do caminho de e/S.

O uso típico do recurso Data Assurance verificará a parte do caminho de e/S entre os controladores e as unidades. As capacidades DA são apresentadas no nível de grupo de volume e pool.

Quando esse recurso está ativado, o storage de armazenamento anexa códigos de verificação de erros (também conhecidos como verificações de redundância cíclica ou CRCs) a cada bloco de dados no volume. Depois que um bloco de dados é movido, o storage array usa esses códigos CRC para determinar se ocorreram erros durante a transmissão. Os dados potencialmente corrompidos não são gravados no disco nem devolvidos ao host. Se você quiser usar o recurso DA, selecione um pool ou grupo de volume que seja capaz DE DA quando você criar um novo volume (procure "Sim" ao lado de "DA" na tabela de candidatos ao grupo de grupo de volume e grupo de volume).

Certifique-se de atribuir esses volumes habilitados PARA DA a um host usando uma interface de e/S capaz de DA. As interfaces de e/S capazes de DA incluem Fibre Channel, SAS, iSCSI em TCP/IP, NVMe/FC, NVMe/IB, NVMe/RoCE e iSER em InfiniBand (extensões iSCSI para RDMA/IB). DA não é compatível com SRP em InfiniBand.

**O que é seguro (Drive Security)?**

O Drive Security é um recurso que impede o acesso não autorizado aos dados em unidades habilitadas para segurança quando removido do storage array. Essas unidades podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).

**O que eu preciso saber sobre o aumento da capacidade reservada?**

Normalmente, você deve aumentar a capacidade quando receber um aviso de que a capacidade reservada corre o risco de ficar cheia. Você pode aumentar a capacidade reservada apenas em incrementos de 8 GiB.

- Você precisa ter capacidade livre suficiente no pool ou no grupo de volumes para que possa ser expandido, se necessário.

  Se não houver capacidade livre em nenhum pool ou grupo de volumes, você poderá adicionar capacidade não atribuída na forma de unidades não utilizadas a um pool ou grupo de volumes.

- O volume no pool ou grupo de volumes deve ter um status ideal e não deve estar em nenhum estado de modificação.
- A capacidade livre deve existir no pool ou grupo de volumes que você deseja usar para aumentar a capacidade.
- Não é possível aumentar a capacidade reservada para um volume instantâneo que seja somente leitura. Somente os volumes snapshot que são leitura-gravação exigem capacidade reservada.

Para operações de snapshot, a capacidade reservada geralmente é de 40% do volume base. Para operações de espelhamento assíncrono, a capacidade reservada é de 20% do volume base. Use uma porcentagem maior se você acredita que o volume base sofrerá muitas mudanças ou se a expetativa de vida estimada da operação de serviço de cópia de um objeto de armazenamento será muito longa.

**Por que não posso escolher outra quantia para diminuir?**

Você pode diminuir a capacidade reservada somente pelo valor usado para aumentá-la. A capacidade reservada para volumes membros só pode ser removida na ordem inversa em que foram adicionados.

Não é possível diminuir a capacidade reservada para um objeto de armazenamento se existir uma destas condições:

- Se o objeto de storage for um volume de par espelhado.
- Se o objeto de armazenamento contiver apenas um volume para a capacidade reservada. O objeto de storage deve conter pelo menos dois volumes para a capacidade reservada.
- Se o objeto de armazenamento for um volume instantâneo desativado.
- Se o objeto de armazenamento contiver uma ou mais imagens instantâneas associadas.

Você pode remover volumes para capacidade reservada somente na ordem inversa em que foram adicionados.

Não é possível diminuir a capacidade reservada para um volume instantâneo que seja somente leitura porque não tem nenhuma capacidade reservada associada. Somente os volumes snapshot que são leitura-gravação exigem capacidade reservada.

#### Por que eu preciso de capacidade reservada para cada volume de membro?

Cada volume de membro em um grupo de consistência de snapshot deve ter sua própria capacidade reservada para salvar quaisquer modificações feitas pelo aplicativo host no volume base sem afetar a imagem de snapshot do grupo de consistência referenciada. A capacidade reservada fornece ao aplicativo host acesso de gravação a uma cópia dos dados contidos no volume do membro designado como leitura-gravação.

Uma imagem instantânea de grupo de consistência não é diretamente lida ou escrita acessível aos hosts. Em vez disso, a imagem instantânea é usada para salvar apenas os dados capturados do volume base.

Durante a criação de um volume instantâneo de grupo de consistência designado como leitura-gravação, o System Manager cria uma capacidade reservada para cada volume de membro no grupo de consistência. Essa capacidade reservada fornece ao aplicativo host acesso de gravação a uma cópia dos dados contidos na imagem instantânea do grupo de consistência.

#### Como posso visualizar e interpretar todas as estatísticas de cache SSD?

Você pode ver estatísticas nominais e estatísticas detalhadas para cache SSD. As estatísticas nominais são um subconjunto das estatísticas detalhadas.

As estatísticas detalhadas só podem ser visualizadas quando você exporta todas as estatísticas SSD para um `.csv` arquivo. Ao rever e interpretar as estatísticas, tenha em mente que algumas interpretações são derivadas olhando para uma combinação de estatísticas.

##### Estatísticas nominais

Para exibir estatísticas de cache SSD, selecione **armazenamento › pools & grupos de volume**. Selecione o cache SSD para o qual deseja exibir estatísticas e, em seguida, selecione **mais › View Statistics**. As estatísticas nominais são apresentadas na caixa de diálogo View SSD Cache Statistics (Ver estatísticas de cache SSD).

A lista a seguir inclui estatísticas nominais, que são um subconjunto das estatísticas detalhadas.

| Estatística nominal | Descrição |
| --- | --- |
| Lê/escreve | O número total de leituras de host ou gravações de host nos volumes habilitados para cache SSD. Compare as leituras relativas às gravações. As leituras precisam ser maiores do que as gravações para uma operação de cache SSD eficaz. Quanto maior a proporção de leituras para gravações, melhor a operação do cache. |
| Cache hits | Uma contagem do número de acessos de cache. |

| Estatística nominal | Descrição |
| --- | --- |
| Acertos de cache (%) | Derivado de hits de cache / (lê e escreve). A porcentagem de acerto do cache deve ser superior a 50 por cento para operação efetiva do cache SSD. Um pequeno número pode indicar várias coisas:<br>• A proporção de leituras para gravações é muito pequena<br>• As leituras não são repetidas<br>• A capacidade do cache é muito pequena |
| Alocação de cache (%) | A quantidade de armazenamento em cache SSD alocada, expressa como uma porcentagem do armazenamento em cache SSD disponível para este controlador. Derivado de bytes alocados / bytes disponíveis. A porcentagem de alocação de cache normalmente aparece como 100 por cento. Se esse número for inferior a 100 por cento, significa que o cache não foi aquecido ou a capacidade do cache SSD é maior do que todos os dados que estão sendo acessados. Neste último caso, uma capacidade de cache SSD menor poderia fornecer o mesmo nível de desempenho. Observe que isso não indica que os dados armazenados em cache foram colocados no cache SSD; é simplesmente uma etapa de preparação antes que os dados possam ser colocados no cache SSD. |
| Utilização de cache (%) | A quantidade de armazenamento em cache SSD que contém dados de volumes ativados, expressa como uma porcentagem de armazenamento em cache SSD alocada. Este valor representa a utilização ou densidade do cache SSD derivado de bytes de dados do usuário / bytes alocados. A porcentagem de utilização do cache normalmente é inferior a 100%, talvez muito menor. Esse número mostra a porcentagem da capacidade do cache SSD que é preenchida com dados de cache. Esse número é inferior a 100 por cento porque cada unidade de alocação do cache SSD, o bloco cache SSD, é dividido em unidades menores chamadas sub-blocos, que são preenchidos de forma um pouco independente. Um número maior geralmente é melhor, mas os ganhos de desempenho podem ser significativos mesmo com um número menor. |

#### Estatísticas detalhadas

As estatísticas detalhadas consistem nas estatísticas nominais, mais estatísticas adicionais. Essas estatísticas adicionais são salvas juntamente com as estatísticas nominais, mas, ao contrário das estatísticas nominais, elas não são exibidas na caixa de diálogo View SSD Cache Statistics (Exibir estatísticas de cache SSD). Você pode exibir as estatísticas detalhadas somente depois de exportar as estatísticas para um `.csv` arquivo.

Ao visualizar o `.csv` arquivo, observe que as estatísticas detalhadas são listadas após as estatísticas nominais:

| Estatísticas detalhadas | Descrição |
| --- | --- |
| Ler blocos | O número de blocos no host lê. |
| Escrever blocos | O número de blocos nas gravações do host. |

| Estatísticas detalhadas | Descrição |
| --- | --- |
| Blocos completos | O número de blocos no cache atinge. Os blocos de hit completos indicam o número de blocos que foram lidos inteiramente a partir do cache SSD. O cache SSD só é benéfico para o desempenho para as operações que são hits de cache completo. |
| Acertos parciais | O número de leituras de host onde pelo menos um bloco, mas não todos os blocos, estavam no cache SSD. Um hit parcial é um SSD Cache **miss** onde as leituras foram satisfeitas a partir do volume base. |
| Acessos parciais - blocos | O número de blocos em Partial Hits. Acessos parciais de cache e blocos parciais de acertos de cache resultam de uma operação que tem apenas uma parte de seus dados no cache SSD. Neste caso, a operação deve obter os dados do volume da unidade de disco rígido em cache (HDD). O cache SSD não oferece nenhum benefício de desempenho para esse tipo de acerto. Se a contagem de blocos de acerto de cache parcial for maior do que os blocos de acerto de cache completo, um tipo de caraterística de e/S diferente (sistema de arquivos, banco de dados ou servidor da Web) poderia melhorar o desempenho. Espera-se que haja um número maior de acertos parciais e falhas em comparação com os acertos do cache enquanto o cache SSD está aquecendo. |
| Falha | O número de leituras de host onde nenhum dos blocos estava no cache SSD. Uma falta de cache SSD ocorre quando as leituras foram satisfeitas a partir do volume base. Espera-se que haja um número maior de acertos parciais e falhas em comparação com os acertos do cache enquanto o cache SSD está aquecendo. |
| Misses - quadras | O número de blocos em misses. |
| Preencher ações (leituras do host) | O número de host lê onde os dados foram copiados do volume base para o cache SSD. |
| Preencher ações (leituras do host) - blocos | O número de blocos em ações de preenchimento (Host lê). |
| Preencher ações (gravações do host) | O número de gravações do host onde os dados foram copiados do volume base para o cache SSD. A contagem de ações de preenchimento (gravações de host) pode ser zero para as configurações de cache que não preenchem o cache como resultado de uma operação de e/S de gravação. |
| Preencher ações (gravações do host) - blocos | O número de blocos em ações de preenchimento (gravações do host). |
| Invalidar ações | O número de vezes que os dados foram invalidados ou removidos do cache SSD. Uma operação de invalidação de cache é executada para cada solicitação de gravação do host, cada solicitação de leitura do host com Acesso forçado à Unidade (FUA), cada solicitação de verificação e em algumas outras circunstâncias. |

| Estatísticas detalhadas | Descrição |
| --- | --- |
| Ações de reciclagem | O número de vezes que o bloco cache SSD foi reutilizado para outro volume base e/ou um intervalo de endereçamento de bloco lógico (LBA) diferente. Para uma operação de cache eficaz, o número de reciclagens deve ser pequeno em comparação com o número combinado de operações de leitura e gravação. Se o número de ações de reciclagem estiver próximo ao número combinado de leituras e gravações, o cache SSD está em alta. A capacidade do cache precisa ser aumentada ou a carga de trabalho não é favorável para uso com cache SSD. |
| Bytes disponíveis | O número de bytes disponíveis no cache SSD para uso por este controlador. |
| Bytes alocados | O número de bytes alocados do cache SSD por este controlador. Os bytes alocados a partir do cache SSD podem estar vazios ou podem conter dados de volumes base. |
| Bytes de dados do usuário | O número de bytes alocados no cache SSD que contêm dados de volumes base. Os bytes disponíveis, os bytes alocados e os bytes de dados do usuário são usados para calcular a porcentagem de alocação de cache e a porcentagem de utilização de cache. |

**O que é a capacidade de otimização para pools?**

## As unidades SSD terão vida útil mais longa e melhor desempenho máximo de gravação quando uma parte de sua capacidade não for alocada.

Para unidades associadas a um pool, a capacidade não alocada é composta pela capacidade de preservação de um pool, pela capacidade livre (capacidade não usada por volumes) e por uma parte da capacidade utilizável reservada como capacidade de otimização adicional. A capacidade de otimização adicional garante um nível mínimo de capacidade de otimização, reduzindo a capacidade utilizável, e, como tal, não está disponível para criação de volume.

Quando um pool é criado, uma capacidade de otimização recomendada é gerada, que fornece um equilíbrio de desempenho, vida útil do desgaste e capacidade disponível. O controle deslizante capacidade de otimização adicional localizado na caixa de diálogo Configurações do pool permite ajustes na capacidade de otimização do pool. O ajuste da barra deslizante proporciona um melhor desempenho e vida útil do desgaste à custa da capacidade disponível, ou da capacidade disponível adicional à custa do desempenho e da vida útil do desgaste da transmissão.

O controle deslizante capacidade de otimização adicional está disponível apenas para sistemas de armazenamento EF600 e EF300.

**O que é a capacidade de otimização para grupos de volumes?**

## As unidades SSD terão vida útil mais longa e melhor desempenho máximo de gravação quando uma parte de sua capacidade não for alocada.

Para unidades associadas a um grupo de volumes, a capacidade não alocada é composta pela capacidade livre de um grupo de volumes (capacidade não usada por volumes) e uma parte da capacidade utilizável reservada como capacidade de otimização. A capacidade de otimização adicional garante um nível mínimo de capacidade de otimização, reduzindo a capacidade utilizável, e, como tal, não está disponível para criação de

volume.

Quando um grupo de volumes é criado, uma capacidade de otimização recomendada é gerada, que fornece um equilíbrio de desempenho, vida útil de desgaste e capacidade disponível. O controle deslizante capacidade de otimização adicional na caixa de diálogo Configurações do grupo de volume permite ajustes na capacidade de otimização de um grupo de volume. O ajuste da barra deslizante proporciona um melhor desempenho e vida útil do desgaste à custa da capacidade disponível, ou da capacidade disponível adicional à custa do desempenho e da vida útil do desgaste da transmissão.

O controle deslizante capacidade de otimização adicional está disponível apenas para sistemas de armazenamento EF600 e EF300.

**O que é capaz de provisionamento de recursos?**

## O provisionamento de recursos é um recurso disponível nas matrizes de armazenamento EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente sem processo de inicialização em segundo plano.

Um volume provisionado por recursos é um volume espesso em um grupo ou pool de volumes SSD, em que a capacidade da unidade é alocada (atribuída ao volume) quando o volume é criado, mas os blocos de unidades são deslocalizados (não mapeados). Em comparação, em um volume grosso tradicional, todos os blocos de unidades são mapeados ou alocados durante uma operação de inicialização de volume em segundo plano, a fim de inicializar os campos de informações de proteção do Data Assurance e tornar os dados e a paridade RAID consistentes em cada faixa RAID. Com um volume provisionado de recurso, não há inicialização em segundo plano com tempo. Em vez disso, cada stripe RAID é inicializado na primeira gravação em um bloco de volume no stripe.

Os volumes provisionados por recursos são compatíveis apenas com grupos de volumes e pools de SSD, em que todas as unidades do grupo ou pool são compatíveis com a funcionalidade de recuperação de erro de ativação de bloco lógico (DULBE) desalocada ou não escrita do NVMe. Quando um volume provisionado por recurso é criado, todos os blocos de unidade atribuídos ao volume são desalocados (não mapeados). Além disso, os hosts podem desalocar blocos lógicos no volume usando o comando NVMe Dataset Management ou o comando SCSI Unmap. A desalocação de blocos pode melhorar a vida útil do SSD e aumentar o desempenho máximo de gravação. A melhoria varia de acordo com cada modelo de unidade e capacidade.

**O que eu preciso saber sobre o recurso volumes provisionados por recursos?**

## O provisionamento de recursos é um recurso disponível nas matrizes de armazenamento EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente sem processo de inicialização em segundo plano.

Um volume provisionado por recursos é um volume espesso em um grupo ou pool de volumes SSD, em que a capacidade da unidade é alocada (atribuída ao volume) quando o volume é criado, mas os blocos de unidades são deslocalizados (não mapeados). Em comparação, em um volume grosso tradicional, todos os blocos de unidades são mapeados ou alocados durante uma operação de inicialização de volume em segundo plano, a fim de inicializar os campos de informações de proteção do Data Assurance e tornar os dados e a paridade RAID consistentes em cada faixa RAID. Com um volume provisionado de recurso, não há inicialização em segundo plano com tempo. Em vez disso, cada stripe RAID é inicializado na primeira gravação em um bloco de volume no stripe.

Os volumes provisionados por recursos são compatíveis apenas com grupos de volumes e pools de SSD, em que todas as unidades do grupo ou pool são compatíveis com a funcionalidade de recuperação de erro de ativação de bloco lógico (DULBE) desalocada ou não escrita do NVMe. Quando um volume provisionado por

recurso é criado, todos os blocos de unidade atribuídos ao volume são desalocados (não mapeados). Além disso, os hosts podem desalocar blocos lógicos no volume usando o comando NVMe Dataset Management ou o comando SCSI Unmap. A desalocação de blocos pode melhorar a vida útil do SSD e aumentar o desempenho máximo de gravação. A melhoria varia de acordo com cada modelo de unidade e capacidade.

O provisionamento de recursos é habilitado por padrão em sistemas onde as unidades suportam DULBE. Você pode desativar essa configuração padrão em **pools & grupos de volume**.

# Volumes e workloads

## Visão geral de volumes e workloads

Você pode criar um volume como um contentor no qual aplicativos, bancos de dados e sistemas de arquivos armazenam dados. Ao criar um volume, você também seleciona uma carga de trabalho para personalizar a configuração do storage array para um aplicativo específico.

### O que são volumes e workloads?

Um *volume* é o componente lógico criado com capacidade específica para o host acessar. Embora um volume possa consistir em mais de uma unidade, um volume aparece como um componente lógico para o host. Depois que um volume é definido, você pode adicioná-lo a uma carga de trabalho. Um *Workload* é um objeto de armazenamento que suporta um aplicativo, como SQL Server ou Exchange, que você pode usar para otimizar o armazenamento para esse aplicativo.

Saiba mais:

- "Como os volumes funcionam"
- "Como as cargas de trabalho funcionam"
- "Terminologia de volume"
- "Como a capacidade é alocada para volumes"
- "Ações que podem ser executadas em volumes"

### Como você cria volumes e cargas de trabalho?

Primeiro, você cria uma carga de trabalho. Aceda ao **armazenamento › volumes** e abra um assistente que o orienta através das etapas. Em seguida, crie um volume a partir da capacidade disponível em um pool ou grupo de volumes e atribua a carga de trabalho criada.

Saiba mais:

- "Fluxo de trabalho para criar volumes"
- "Crie workloads"
- "Criar volumes"
- "Adicionar volumes ao workload"

### Informações relacionadas

Saiba mais sobre conceitos relacionados a volumes:

- "Integridade de dados e segurança de dados para volumes"
- "Cache e volumes SSD"
- "Monitoramento de volume fino"

## Conceitos

### Como os volumes funcionam

Os volumes são recipientes de dados que gerenciam e organizam o espaço de armazenamento em seu storage array.

Você cria volumes a partir da capacidade de armazenamento disponível em sua matriz de armazenamento e facilita a organização e o uso dos recursos do sistema. Este conceito é semelhante ao uso de pastas/diretórios em um computador para organizar arquivos para acesso fácil e rápido.

Os volumes são a única camada de dados visível para os hosts. Em um ambiente SAN, os volumes são mapeados para números de unidade lógica (LUNs), que são visíveis para os hosts. Os LUNs armazenam os dados de usuário acessíveis por meio de um ou mais protocolos de acesso ao host compatíveis com o storage array, incluindo FC, iSCSI e SAS.

#### Tipos de volume que você pode criar a partir de pools e grupos de volumes

Os volumes tiram sua capacidade de pools ou grupos de volumes. Você pode criar os seguintes tipos de volumes a partir dos pools ou grupos de volumes que existem no storage array.

- **De pools** — você pode criar volumes de um pool como volumes *totalmente provisionados (espessos)* ou volumes *finamente provisionados (finos).*

> A interface do System Manager não oferece uma opção para criar thin volumes. Se você quiser criar volumes finos, use a interface de linha de comando (CLI).

- **De grupos de volumes** — você pode criar volumes de um grupo de volumes apenas como volumes *totalmente provisionados (espessos)*.

Volumes espessos e volumes finos extraem a capacidade do storage array de maneiras diferentes:

- A capacidade de um volume espesso é alocada quando o volume é criado.
- A capacidade de um volume fino é alocada como dados quando gravados no volume.

O thin Provisioning ajuda a evitar o desperdício de capacidade alocada e pode economizar às empresas em custos iniciais de storage. No entanto, o provisionamento total beneficia de menos latência porque todo o storage é alocado de uma só vez quando volumes espessos são criados.

> Os sistemas de storage EF600 e EF300 não oferecem suporte ao thin Provisioning.

#### Caraterísticas dos volumes

Cada volume em um pool ou grupo de volumes pode ter suas próprias caraterísticas individuais com base em que tipo de dados serão armazenados nele. Algumas dessas caraterísticas incluem:

- **Tamanho do segmento** — Um segmento é a quantidade de dados em kilobytes (KiB) que é armazenada em uma unidade antes que a matriz de armazenamento se mova para a próxima unidade na faixa (grupo

RAID). O tamanho do segmento é igual ou inferior à capacidade do grupo de volume. O tamanho do segmento é fixo e não pode ser alterado para pools.

- * Capacidade* — você cria um volume a partir da capacidade gratuita disponível em um pool ou grupo de volume. Antes de criar um volume, o pool ou grupo de volumes já deve existir e deve ter capacidade livre suficiente para criar o volume.
- **Propriedade do controlador** — todos os storages de armazenamento podem ter um ou dois controladores. Em um array de controlador único, o workload de um volume é gerenciado por um único controlador. Em um array de controladora dupla, um volume terá um controlador preferido (A ou B) que "possua" o volume. Em uma configuração de controladora dupla, a propriedade de volume é ajustada automaticamente usando o recurso balanceamento de carga automático para corrigir quaisquer problemas de balanceamento de carga quando as cargas de trabalho mudam entre os controladores. O balanceamento automático de carga fornece balanceamento automatizado de carga de trabalho de e/S e garante que o tráfego de e/S recebido dos hosts seja gerenciado e balanceado dinamicamente entre os dois controladores.
- * Atribuição de volume* — você pode dar aos hosts acesso a um volume quando você cria o volume ou em um momento posterior. Todo o acesso ao host é gerenciado por meio de um número de unidade lógica (LUN). Os hosts detetam LUNs que, por sua vez, estão atribuídos a volumes. Se você estiver atribuindo um volume a vários hosts, use o software de cluster para garantir que o volume esteja disponível para todos os hosts.

  O tipo de host pode ter limites específicos sobre quantos volumes o host pode acessar. Mantenha essa limitação em mente quando você cria volumes para uso por um host específico.

- * Nome descritivo* — você pode nomear um volume qualquer que seja o nome que você gosta, mas recomendamos fazer o nome descritivo.

Durante a criação do volume, cada volume é alocada a capacidade e recebe um nome, tamanho do segmento (somente grupos de volume), propriedade do controlador e atribuição de volume para host. Os dados de volume são balanceados automaticamente entre os controladores, conforme necessário.

#### Como as cargas de trabalho funcionam

Ao criar um volume, você seleciona uma carga de trabalho para personalizar a configuração do storage array para um aplicativo específico.

Um workload é um objeto de storage compatível com uma aplicação. Você pode definir uma ou mais cargas de trabalho ou instâncias por aplicação. Para alguns aplicativos, o sistema configura a carga de trabalho para conter volumes com caraterísticas de volume subjacentes semelhantes. Essas características de volume são otimizadas com base no tipo de aplicação compatível com o workload. Por exemplo, se você criar uma carga de trabalho que suporte um aplicativo Microsoft SQL Server e, posteriormente, criar volumes para essa carga de trabalho, as caraterísticas de volume subjacentes serão otimizadas para oferecer suporte ao Microsoft SQL Server.

Durante a criação de volume, o sistema solicita que você responda a perguntas sobre o uso de uma carga de trabalho. Por exemplo, se você estiver criando volumes para o Microsoft Exchange, será perguntado quantas caixas de correio você precisa, quais são seus requisitos médios de capacidade de caixa de correio e quantas cópias do banco de dados deseja. O sistema usa essas informações para criar uma configuração de volume ideal para você, que pode ser editada conforme necessário. Opcionalmente, você pode pular esta etapa na sequência de criação de volume.

##### Tipos de workloads

Você pode criar dois tipos de workloads: Específicos da aplicação e outros.

- **Específico da aplicação**. Quando você está criando volumes usando uma carga de trabalho específica da aplicação, o sistema pode recomendar uma configuração de volume otimizada para minimizar a contenção entre a e/S da carga de trabalho do aplicativo e outro tráfego da instância do aplicativo. As características de volume, como tipo de e/S, tamanho do segmento, propriedade da controladora e cache de leitura e gravação, são automaticamente recomendadas e otimizadas para cargas de trabalho criadas para os seguintes tipos de aplicativos.
  - Microsoft SQL Server
  - Microsoft Exchange Server
  - Aplicações de vigilância por vídeo
  - VMware ESXi (para volumes a serem usados com o Virtual Machine File System)

    Você pode revisar a configuração de volume recomendada e editar, adicionar ou excluir os volumes e caraterísticas recomendados pelo sistema usando a caixa de diálogo Adicionar/Editar volumes.
- **Outros** (ou aplicativos sem suporte específico para criação de volume). Outros workloads usam uma configuração de volume que você precisa especificar manualmente quando deseja criar um workload que não esteja associado a uma aplicação específica ou se o sistema não tiver otimização incorporada para a aplicação que você pretende usar no storage array. Você deve especificar manualmente a configuração do volume usando a caixa de diálogo Adicionar/Editar volumes.

#### Visualizações de aplicação e workload

Para visualizar aplicações e workloads, inicie o Gerenciador de sistemas do SANtricity. Nessa interface, você pode exibir informações associadas a uma carga de trabalho específica do aplicativo de algumas maneiras diferentes:

- Você pode selecionar a guia **aplicativos e cargas de trabalho** no bloco volumes para exibir os volumes do storage array agrupados por carga de trabalho e o tipo de aplicativo ao qual a carga de trabalho está associada.
- Você pode selecionar a guia **aplicativos e cargas de trabalho** no bloco desempenho para exibir métricas de desempenho (latência, IOPS e MBs) para objetos lógicos. Os objetos são agrupados por aplicativo e carga de trabalho associada. Ao coletar esses dados de desempenho em intervalos regulares, você pode estabelecer medições de linha de base e analisar tendências, o que pode ajudar a investigar problemas relacionados ao desempenho de e/S.

## Terminologia de volume

Saiba como os termos de volume se aplicam ao storage array.

#### Todos os tipos de volume

| Prazo | Descrição |
| --- | --- |
| Capacidade alocada | Você usa a capacidade alocada para criar volumes e operações de serviços de cópia.<br><br>A capacidade alocada e a capacidade reportada são as mesmas para volumes espessos, mas são diferentes para volumes finos. Para um volume grosso, o espaço fisicamente alocado é igual ao espaço relatado ao host. Para um volume fino, a capacidade relatada é a capacidade relatada aos hosts, enquanto a capacidade alocada é a quantidade de espaço de unidade atualmente alocada para a gravação de dados. |
| Aplicação | Um aplicativo é um software como o SQL Server ou o Exchange. Você define um ou mais workloads para dar suporte a cada aplicação. Para alguns aplicativos, o sistema recomenda automaticamente uma configuração de volume que otimiza o armazenamento. Caraterísticas como tipo de e/S, tamanho do segmento, propriedade do controlador e cache de leitura e gravação estão incluídas na configuração do volume. |
| Capacidade | Capacidade é a quantidade de dados que você pode armazenar em um volume. |
| Propriedade do controlador | A propriedade do controlador define o controlador que é designado para ser o controlador proprietário ou principal do volume. Um volume pode ter um controlador preferido (A ou B) que "possua" o volume. A propriedade do volume é ajustada automaticamente usando o recurso balanceamento de carga automático para corrigir quaisquer problemas de balanceamento de carga quando as cargas de trabalho mudam entre os controladores. O balanceamento de carga automático fornece balanceamento automatizado de carga de trabalho de e/S e garante que o tráfego de e/S recebido dos hosts seja gerenciado e balanceado dinamicamente entre ambos os controladores. |
| Pré-busca de leitura de cache dinâmico | A pré-busca de leitura de cache dinâmico permite que o controlador copie blocos de dados sequenciais adicionais para o cache enquanto ele está lendo blocos de dados de uma unidade para o cache. Esse armazenamento em cache aumenta a chance de que futuras solicitações de dados possam ser preenchidas a partir do cache. A pré-busca de leitura de cache dinâmico é importante para aplicativos Multimídia que usam e/S sequenciais A taxa e a quantidade de dados pré-obtidos no cache são auto-ajustáveis com base na taxa e no tamanho da solicitação das leituras do host. O acesso aleatório não faz com que os dados sejam pré-obtidos no cache. Este recurso não se aplica quando o armazenamento em cache de leitura está desativado.<br><br>Para um volume fino, a pré-busca de leitura de cache dinâmico é sempre desativada e não pode ser alterada. |

| Prazo | Descrição |
| --- | --- |
| Área de capacidade livre | Uma área de capacidade livre é a capacidade livre que pode resultar da exclusão de um volume ou da não utilização de toda a capacidade livre disponível durante a criação do volume. Quando você cria um volume em um grupo de volumes que tenha uma ou mais áreas de capacidade livre, a capacidade do volume é limitada à maior área de capacidade livre nesse grupo de volumes. Por exemplo, se um grupo de volume tiver um total de 15 GiB de capacidade livre, e a maior área de capacidade livre for de 10 GiB, o maior volume que você pode criar é de 10 GiB.<br><br>Ao consolidar a capacidade gratuita, você pode criar volumes adicionais a partir da quantidade máxima de capacidade livre em um grupo de volumes. |
| Host | Um host é um servidor que envia e/S para um volume em um storage array. |
| Cluster de host | Um cluster de host é um grupo de hosts. Você cria um cluster de host para facilitar a atribuição dos mesmos volumes a vários hosts. |
| Unidade hot spare | As unidades hot spare são suportadas apenas com grupos de volume. Uma unidade hot spare não contém dados e funciona como standby no caso de uma unidade falhar nos volumes RAID 1, RAID 3, RAID 5 ou RAID 6 contidos em um grupo de volumes. A unidade hot spare adiciona outro nível de redundância à sua matriz de armazenamento. |
| LUN | Um número de unidade lógica (LUN) é o número atribuído ao espaço de endereço que um host usa para acessar um volume. O volume é apresentado ao host como capacidade na forma de um LUN.<br><br>Cada host tem seu próprio espaço de endereço LUN. Portanto, o mesmo LUN pode ser usado por diferentes hosts para acessar diferentes volumes. |
| Digitalização de multimédia | Uma verificação de Mídia fornece uma maneira de detetar erros de Mídia da unidade antes que eles sejam encontrados durante uma leitura normal ou gravação nas unidades. Uma digitalização de Mídia é executada como uma operação em segundo plano e verifica todos os dados e informações de redundância em volumes de usuário definidos. |
| Namespace | Um namespace é o armazenamento NVM formatado para acesso a bloco. É análogo a uma unidade lógica em SCSI, que se relaciona a um volume no storage array. |
| Piscina | Um pool é um conjunto de unidades que é agrupado logicamente. Você pode usar um pool para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um pool ou de um grupo de volumes.) |
| Capacidade de pool ou grupo de volumes | A capacidade de pool, volume ou grupo de volumes é a capacidade de um storage array que foi atribuída a um pool ou grupo de volumes. Essa capacidade é usada para criar volumes e atender às várias necessidades de capacidade de operações de serviços de cópia e objetos de storage. |

| Prazo | Descrição |
| --- | --- |
| Leia o cache | O cache de leitura é um buffer que armazena dados que foram lidos das unidades. Os dados para uma operação de leitura podem já estar no cache de uma operação anterior, o que elimina a necessidade de acessar as unidades. Os dados permanecem no cache de leitura até que sejam lavados. |
| Capacidade comunicada | Capacidade reportada é a capacidade que é relatada ao host e pode ser acessada pelo host.<br><br>A capacidade reportada e a capacidade alocada são as mesmas para volumes espessos, mas são diferentes para volumes finos. Para um volume grosso, o espaço fisicamente alocado é igual ao espaço relatado ao host. Para um volume fino, a capacidade relatada é a capacidade relatada aos hosts, enquanto a capacidade alocada é a quantidade de espaço de unidade atualmente alocada para a gravação de dados. |
| Tamanho do segmento | Um segmento é a quantidade de dados em kilobytes (KiB) que é armazenada em uma unidade antes que a matriz de armazenamento se mova para a próxima unidade na faixa (grupo RAID). O tamanho do segmento é igual ou inferior à capacidade do grupo de volume. O tamanho do segmento é fixo e não pode ser alterado para pools. |
| Riscar | Striping é uma maneira de armazenar dados na matriz de armazenamento. Striping divide o fluxo de dados em blocos de um determinado tamanho (chamado "tamanho do bloco") e, em seguida, grava esses blocos nas unidades um por um. Essa maneira de armazenamento de dados é usada para distribuir e armazenar dados em várias unidades físicas. Striping é sinônimo de RAID 0 e espalha os dados por todas as unidades em um grupo RAID sem paridade. |
| Volume | Um volume é um contêiner no qual aplicativos, bancos de dados e sistemas de arquivos armazenam dados. É o componente lógico criado para que o host acesse o storage no storage array. |
| Atribuição de volume | A atribuição de volume é como os LUNs do host são atribuídos a um volume. |
| Nome do volume | Um nome de volume é uma cadeia de carateres atribuída ao volume quando é criado. Você pode aceitar o nome padrão ou fornecer um nome mais descritivo indicando o tipo de dados armazenados no volume. |
| Grupo de volume | Um grupo de volumes é um contentor para volumes com caraterísticas compartilhadas. Um grupo de volumes tem uma capacidade definida e um nível RAID. Você pode usar um grupo de volumes para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um grupo de volumes ou de um pool.) |

| Prazo | Descrição |
| --- | --- |
| Workload | Um workload é um objeto de storage compatível com uma aplicação. Você pode definir uma ou mais cargas de trabalho ou instâncias por aplicação. Para alguns aplicativos, o sistema configura a carga de trabalho para conter volumes com caraterísticas de volume subjacentes semelhantes. Essas características de volume são otimizadas com base no tipo de aplicação compatível com o workload. Por exemplo, se você criar uma carga de trabalho que suporte um aplicativo Microsoft SQL Server e, posteriormente, criar volumes para essa carga de trabalho, as caraterísticas de volume subjacentes serão otimizadas para oferecer suporte ao Microsoft SQL Server. |
| Cache de gravação | O cache de gravação é um buffer que armazena dados do host que ainda não foram gravados nas unidades. Os dados permanecem no cache de gravação até que sejam gravados nas unidades. O armazenamento em cache de gravação pode aumentar a performance de e/S. |
| Armazenamento em cache com espelhamento | O cache de gravação com espelhamento ocorre quando os dados gravados na memória de cache de um controlador também são gravados na memória de cache do outro controlador. Portanto, se um controlador falhar, o outro pode concluir todas as operações de gravação pendentes. O espelhamento do cache de gravação estará disponível somente se o armazenamento em cache de gravação estiver habilitado e duas controladoras estiverem presentes. O armazenamento em cache de gravação com espelhamento é a configuração padrão na criação de volume. |
| Escreva o armazenamento em cache sem baterias | A configuração de armazenamento de gravação sem baterias permite que o armazenamento em cache continue, mesmo quando as baterias estiverem em falta, falharem, descarregadas completamente ou não estiverem totalmente carregadas. Normalmente, a escolha do armazenamento em cache sem baterias não é recomendada, pois os dados podem ser perdidos se perder energia. Normalmente, o armazenamento em cache de gravação é desligado temporariamente pelo controlador até que as baterias sejam carregadas ou uma bateria com falha seja substituída. |

**Específico para volumes finos**

O System Manager não oferece uma opção para criar thin volumes. Se você quiser criar volumes finos, use a interface de linha de comando (CLI).

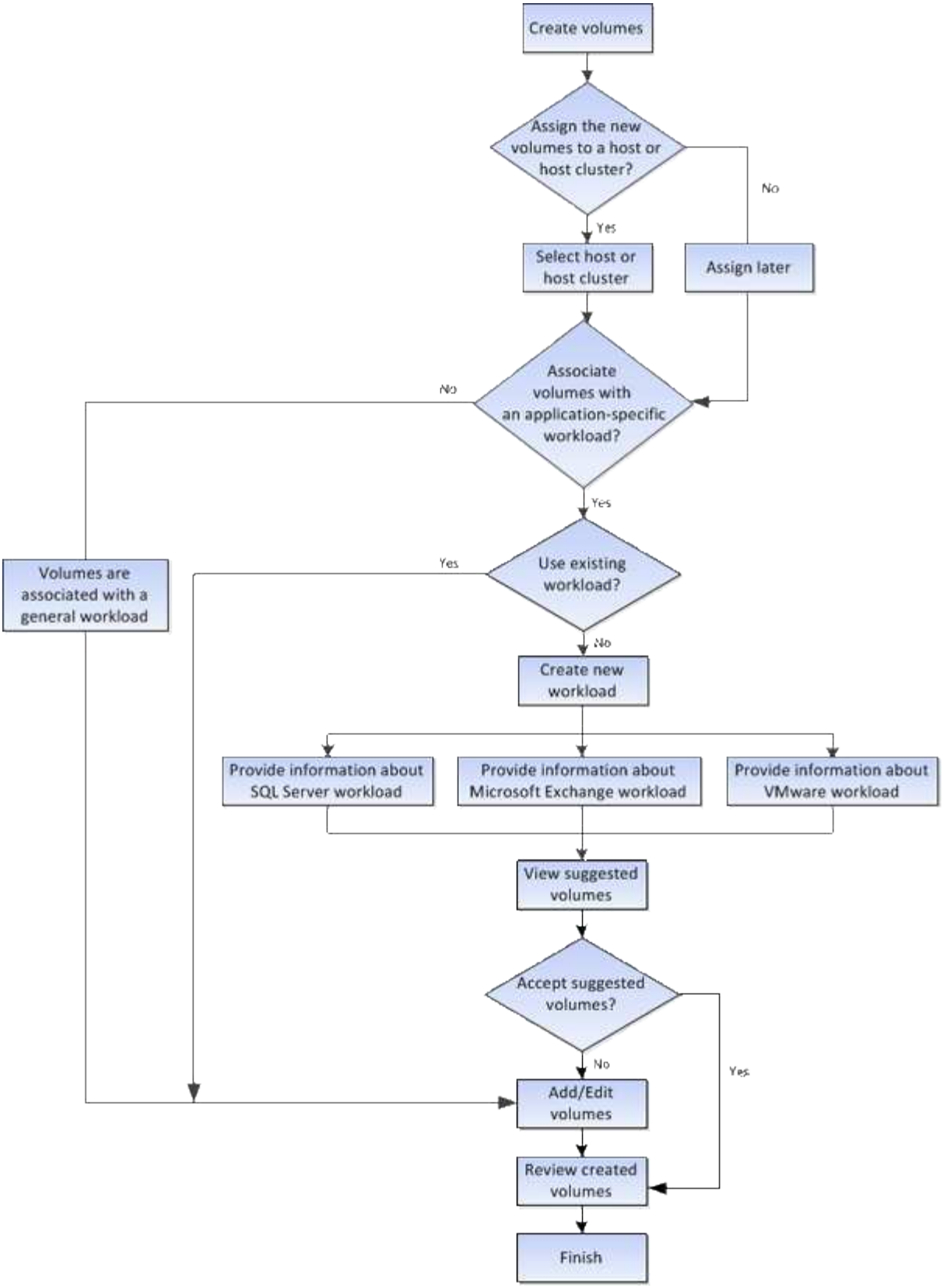
Os volumes finos não estão disponíveis no sistema de armazenamento EF600 ou EF300.

| Prazo | Descrição |
| --- | --- |
| Limite de capacidade alocado | O limite de capacidade alocado é o limite de quão grande a capacidade física alocada para um volume fino pode crescer. |
| Capacidade escrita | Capacidade escrita é a quantidade de capacidade que foi escrita a partir da capacidade reservada alocada para volumes finos. |

| Prazo | Descrição |
| --- | --- |
| Limite de aviso | Você pode definir um alerta de limite de aviso a ser emitido quando a capacidade alocada para um volume fino atingir a porcentagem cheia (o limite de aviso). |

**Fluxo de trabalho para criar volumes**

No System Manager, você pode criar volumes seguindo estas etapas.




**Integridade de dados e segurança de dados para volumes**

Pode ativar os volumes para utilizar a funcionalidade Data Assurance (DA) e a funcionalidade Drive Security (Segurança da unidade). Esses recursos são apresentados no nível de grupo de volume e pool.

#### Garantia de dados

A Data Assurance (DA) implementa a norma T10 Protection Information (PI), que aumenta a integridade dos dados verificando e corrigindo erros que possam ocorrer à medida que os dados são transferidos ao longo do caminho de e/S. O uso típico do recurso Data Assurance verificará a parte do caminho de e/S entre os controladores e as unidades. As capacidades DA são apresentadas no nível de grupo de volume e pool.

Quando esse recurso está ativado, o storage de armazenamento anexa códigos de verificação de erros (também conhecidos como verificações de redundância cíclica ou CRCs) a cada bloco de dados no volume. Depois que um bloco de dados é movido, o storage array usa esses códigos CRC para determinar se ocorreram erros durante a transmissão. Os dados potencialmente corrompidos não são gravados no disco nem devolvidos ao host. Se você quiser usar o recurso DA, selecione um pool ou grupo de volume que seja capaz DE DA quando você criar um novo volume (procure "Sim" ao lado de "DA" na tabela de candidatos ao grupo de grupo de volume e grupo de volume).

#### Segurança da unidade

O Drive Security é um recurso que impede o acesso não autorizado aos dados em unidades habilitadas para segurança quando removido do storage array. Essas unidades podem ser unidades com criptografia total de disco (FDE) ou unidades certificadas para atender aos padrões federais de processamento de informações 140-2 nível 2 (unidades FIPS).

### Como o Drive Security funciona no nível da unidade

Uma unidade com capacidade segura, FDE ou FIPS, criptografa os dados durante gravações e descriptografa dados durante leituras. Essa criptografia e descriptografia não afetam o desempenho ou o fluxo de trabalho do usuário. Cada unidade tem sua própria chave de criptografia exclusiva, que nunca pode ser transferida da unidade.

### Como o Drive Security funciona no nível do volume

Ao criar um pool ou grupo de volumes a partir de unidades com capacidade segura, também é possível ativar a Segurança da unidade para esses pools ou grupos de volumes. A opção Segurança da unidade torna as unidades e os grupos de volume e pools associados seguros-*enabled*. Um pool ou grupo de volumes pode conter unidades com capacidade de segurança e não seguras, mas todas as unidades devem ser seguras para usar seus recursos de criptografia.

### Como implementar o Drive Security

Para implementar o Drive Security, execute as etapas a seguir.

1. Equipe seu storage array com unidades com capacidade segura, unidades FDE ou FIPS. (Para volumes que exigem suporte FIPS, use apenas unidades FIPS. A combinação de unidades FIPS e FDE em um grupo de volumes ou pool resultará no tratamento de todas as unidades como unidades FDE. Além disso, uma unidade FDE não pode ser adicionada ou usada como sobressalente em um grupo ou pool de volumes totalmente FIPS.)
2. Crie uma chave de segurança, que é uma cadeia de carateres que é compartilhada pelo controlador e unidades para acesso de leitura/gravação. Você pode criar uma chave interna a partir da memória persistente do controlador ou uma chave externa de um servidor de gerenciamento de chaves. Para o gerenciamento de chaves externas, a autenticação deve ser estabelecida com o servidor de gerenciamento de chaves.
3. Ative a segurança da unidade para pools e grupos de volumes:
    - Crie um pool ou grupo de volumes (procure **Sim** na coluna **compatível com segurança** na tabela candidatos).

- Selecione um pool ou grupo de volumes quando criar um novo volume (procure **Sim** ao lado de **compatível com segurança** na tabela de candidatos ao grupo de grupos de volumes e pool).

  Com o recurso Segurança da unidade, você cria uma chave de segurança compartilhada entre as unidades e os controladores habilitados para segurança em um storage de armazenamento. Sempre que a alimentação das unidades é desligada e ligada, as unidades ativadas por segurança mudam para um estado de Segurança bloqueada até que o controlador aplique a chave de segurança.

### Cache e volumes SSD

Você pode adicionar um volume ao cache SSD como uma maneira de melhorar o desempenho somente leitura. Cache SSD consiste em um conjunto de unidades de disco de estado sólido (SSD) que você agrupa logicamente em seu storage array.

#### Volumes

Mecanismos simples de e/S de volume são usados para mover dados de e para o cache SSD. Depois que os dados são armazenados em cache e armazenados nos SSDs, as leituras subsequentes desses dados são executadas no cache SSD, eliminando assim a necessidade de acessar o volume do HDD.

Cache SSD é um cache secundário para uso com o cache primário na memória dinâmica de acesso aleatório (DRAM) da controladora.

- No cache primário, os dados são armazenados na DRAM após uma leitura do host.
- No cache SSD, os dados são copiados de volumes e armazenados em dois volumes RAID internos (um por controlador) que são criados automaticamente quando você cria um cache SSD.

Os volumes RAID internos são usados para fins de processamento de cache interno. Esses volumes não são acessíveis ou exibidos na interface do usuário. No entanto, esses dois volumes contam com o número total de volumes permitidos no storage array.

Qualquer volume atribuído para usar o cache SSD de um controlador não é elegível para uma transferência automática de balanceamento de carga.

#### Recurso de segurança da unidade

Para usar cache SSD em um volume que também esteja usando a Segurança da unidade (ativada para segurança), os recursos de segurança da unidade do volume e o cache SSD devem corresponder. Se não corresponderem, o volume não será ativado com segurança.

### Ações que podem ser executadas em volumes

Você pode executar várias ações diferentes em um volume: Aumentar a capacidade, excluir, copiar, inicializar, redistribuir, alterar a propriedade, alterar as configurações de cache e alterar as configurações de digitalização de Mídia.

#### Aumentar a capacidade

Você pode expandir a capacidade de um volume de duas maneiras:

- Use a capacidade gratuita disponível no pool ou grupo de volumes.

Você adiciona capacidade a um volume selecionando **armazenamento › pools e grupos de volume › Adicionar capacidade**.

- Adicione capacidade não atribuída (na forma de unidades não utilizadas) ao pool ou grupo de volumes do volume. Use esta opção quando não houver capacidade livre no pool ou grupo de volumes.

  Você adiciona capacidade não atribuída ao pool ou grupo de volumes selecionando **armazenamento › pools e grupos de volume › Adicionar capacidade**.

  Se a capacidade livre não estiver disponível no pool ou no grupo de volumes, você não poderá aumentar a capacidade do volume. Você deve aumentar primeiro o tamanho do pool ou do grupo de volumes ou excluir volumes não utilizados.

Depois de expandir a capacidade de volume, você deve aumentar manualmente o tamanho do sistema de arquivos para corresponder. A forma como você faz isso depende do sistema de arquivos que você está usando. Consulte a documentação do sistema operacional do host para obter detalhes.

#### Eliminar

Normalmente, você exclui volumes se os volumes tiverem sido criados com os parâmetros ou a capacidade errados, não atenderem mais às necessidades de configuração de storage ou forem imagens snapshot que não são mais necessárias para backup ou teste de aplicativos. A exclusão de um volume aumenta a capacidade livre no pool ou grupo de volumes.

A exclusão de volumes causa a perda de todos os dados nesses volumes. A exclusão de um volume também excluirá quaisquer imagens instantâneas associadas, programações e volumes instantâneos e removerá quaisquer relações de espelhamento.

#### Cópia

Ao copiar volumes, você cria uma cópia pontual de dois volumes separados, o volume de origem e o volume de destino, no mesmo storage array. Pode copiar volumes selecionando **armazenamento › volumes › Serviços de cópia › volume de cópia**.

#### Inicializar

A inicialização de um volume apaga todos os dados do volume. Um volume é inicializado automaticamente quando é criado pela primeira vez. No entanto, o Recovery Guru pode aconselhar que você inicialize manualmente um volume para recuperar de certas condições de falha. Ao inicializar um volume, o volume mantém suas configurações WWN, atribuições de host, capacidade alocada e capacidade reservada. Ele também mantém as mesmas configurações de garantia de dados (DA) e configurações de segurança.

Pode inicializar volumes selecionando **armazenamento › volumes › mais › Inicializar volumes**.

#### Redistribuir

Você redistribui volumes para mover volumes de volta para os proprietários de controladores preferenciais. Normalmente, os drivers multipath movem volumes do proprietário da controladora preferida quando ocorre um problema ao longo do caminho de dados entre o host e o storage array.

A maioria dos drivers multipath de host tenta acessar cada volume em um caminho para o proprietário do controlador preferido. No entanto, se esse caminho preferido ficar indisponível, o driver multipath no host fará failover para um caminho alternativo. Esse failover pode fazer com que a propriedade do volume mude para o controlador alternativo. Depois de resolver a condição que causou o failover, alguns hosts podem mover

automaticamente a propriedade do volume de volta para o proprietário do controlador preferido, mas, em alguns casos, talvez seja necessário redistribuir manualmente os volumes.

Pode redistribuir volumes selecionando **armazenamento › volumes › mais › redistribuir volumes**.

#### Alterar a propriedade do volume

Alterar a propriedade de um volume altera a propriedade preferida do controlador do volume. O proprietário do controlador preferido de um volume está listado no **armazenamento › volumes › Ver/Editar Definições › separador Avançadas**.

Pode alterar a propriedade de um volume selecionando **armazenamento › volumes › mais › alterar propriedade**.

### Espelhamento e propriedade de volume

Se o volume primário do par espelhado for de propriedade da controladora A, o volume secundário também será de propriedade da controladora A do storage array remoto. Alterar o proprietário do volume primário mudará automaticamente o proprietário do volume secundário para garantir que ambos os volumes sejam propriedade do mesmo controlador. As alterações de propriedade atuais no lado primário propagam-se automaticamente para as alterações de propriedade atuais correspondentes no lado secundário.

Se um grupo de consistência de espelho contiver um volume secundário local e a propriedade do controlador for alterada, o volume secundário será automaticamente transferido de volta para o proprietário do controlador original na primeira operação de gravação. Não é possível alterar a propriedade do controlador de um volume secundário usando a opção **alterar propriedade**.

### Copiar volume e propriedade de volume

Durante uma operação de volume de cópia, o mesmo controlador deve possuir o volume de origem e o volume de destino. Às vezes, ambos os volumes não têm o mesmo controlador preferido quando a operação de volume de cópia é iniciada. Portanto, a propriedade do volume de destino é automaticamente transferida para o controlador preferido do volume de origem. Quando a cópia de volume é concluída ou interrompida, a propriedade do volume de destino é restaurada para o controlador preferido.

Se a propriedade do volume de origem for alterada durante a operação de volume de cópia, a propriedade do volume de destino também será alterada. Em certos ambientes de sistema operacional, pode ser necessário reconfigurar o driver de host multipath antes de usar um caminho de e/S. (Alguns drivers multipath requerem uma edição para reconhecer o caminho de e/S. Consulte a documentação do driver para obter mais informações.)

#### Altere as configurações de cache

A memória cache é uma área de armazenamento temporário volátil (RAM) no controlador que tem um tempo de acesso mais rápido do que a Mídia da unidade. Se você usar a memória cache, você pode aumentar o desempenho geral de e/S por causa destes motivos:

- Os dados solicitados do host para uma leitura podem já estar no cache de uma operação anterior, eliminando assim a necessidade de acesso à unidade.
- Gravar dados é gravado inicialmente no cache, o que libera o aplicativo para continuar em vez de esperar que os dados sejam gravados na unidade.

Selecione **armazenamento › volumes › mais › alterar definições de cache** para alterar as seguintes definições de cache:

- **Cache de leitura e gravação** — o cache de leitura é um buffer que armazena dados lidos das unidades. Os dados para uma operação de leitura podem já estar no cache de uma operação anterior, o que elimina a necessidade de acessar as unidades. Os dados permanecem no cache de leitura até que sejam lavados.

  O cache de gravação é um buffer que armazena dados do host que ainda não foram gravados nas unidades. Os dados permanecem no cache de gravação até que sejam gravados nas unidades. O armazenamento em cache de gravação pode aumentar a performance de e/S.

- **Armazenamento em cache com espelhamento** — o armazenamento em cache com espelhamento ocorre quando os dados gravados na memória cache de um controlador também são gravados na memória de cache do outro controlador. Portanto, se um controlador falhar, o outro pode concluir todas as operações de gravação pendentes. O espelhamento do cache de gravação estará disponível somente se o armazenamento em cache de gravação estiver habilitado e duas controladoras estiverem presentes. O armazenamento em cache de gravação com espelhamento é a configuração padrão na criação de volume.
- **Armazenamento em cache sem baterias** — a configuração armazenamento em cache sem baterias permite que o armazenamento em cache continue, mesmo quando as baterias estiverem faltando, falharem, descarregadas completamente ou não estiverem totalmente carregadas. Normalmente, a escolha do armazenamento em cache sem baterias não é recomendada, pois os dados podem ser perdidos se perder energia. Normalmente, o armazenamento em cache de gravação é desligado temporariamente pelo controlador até que as baterias sejam carregadas ou uma bateria com falha seja substituída.

  Esta configuração estará disponível somente se você tiver habilitado o armazenamento em cache de gravação. Esta definição não está disponível para volumes finos.

- * Pré-busca de cache de leitura dinâmica* — Pré-busca de leitura de cache dinâmico permite que o controlador copie blocos de dados sequenciais adicionais para o cache enquanto ele está lendo blocos de dados de uma unidade para o cache. Esse armazenamento em cache aumenta a chance de que futuras solicitações de dados possam ser preenchidas a partir do cache. A pré-busca de leitura de cache dinâmico é importante para aplicativos Multimídia que usam e/S sequenciais A taxa e a quantidade de dados pré-obtidos no cache são auto-ajustáveis com base na taxa e no tamanho da solicitação das leituras do host. O acesso aleatório não faz com que os dados sejam pré-obtidos no cache. Este recurso não se aplica quando o armazenamento em cache de leitura está desativado.

  Para um volume fino, a pré-busca de leitura de cache dinâmico é sempre desativada e não pode ser alterada.

#### Alterar as definições de digitalização de multimédia

As digitalizações de Mídia detetam e reparam erros de Mídia em blocos de disco que são raramente lidos por aplicativos. Esta verificação pode impedir que ocorra perda de dados se outras unidades no pool ou grupo de volumes falharem, uma vez que os dados para unidades com falha são reconstruídos usando informações de redundância e dados de outras unidades no pool ou grupo de volumes.

As digitalizações multimédia são executadas continuamente a uma taxa constante, com base na capacidade a digitalizar e na duração da digitalização. As digitalizações em segundo plano podem ser temporariamente suspensas por uma tarefa de fundo de prioridade mais alta (por exemplo, reconstrução), mas serão retomadas com a mesma taxa constante.

Pode ativar e definir a duração durante a qual a digitalização de multimédia é executada selecionando **armazenamento › volumes › mais › alterar definições de digitalização de multimédia**.

Um volume só é lido quando a opção de digitalização de material está ativada para a matriz de armazenamento e para esse volume. Se a verificação de redundância também estiver ativada para esse volume, as informações de redundância no volume serão verificadas quanto à consistência com os dados, desde que o volume tenha redundância. A verificação de Mídia com verificação de redundância é ativada por padrão para cada volume quando é criado.

Se for encontrado um erro de meio irrecuperável durante a verificação, os dados serão reparados usando informações de redundância, se disponíveis. Por exemplo, as informações de redundância estão disponíveis em volumes RAID 5 ideais ou em volumes RAID 6 ideais ou que só têm uma unidade com falha. Se o erro irrecuperável não puder ser reparado usando informações de redundância, o bloco de dados será adicionado ao log de setor ilegível. Os erros de meio corrigíveis e incorrigíveis são reportados ao log de eventos.

Se a verificação de redundância encontrar uma inconsistência entre os dados e as informações de redundância, ela será reportada ao log de eventos.

### Como a capacidade é alocada para volumes

As unidades do seu storage array fornecem a capacidade de armazenamento físico para os seus dados. Antes de começar a armazenar dados, você deve configurar a capacidade alocada em componentes lógicos conhecidos como pools ou grupos de volume. Você usa esses objetos de storage para configurar, armazenar, manter e preservar dados em seu storage array.

#### Uso da capacidade para criar e expandir volumes

Você pode criar volumes a partir da capacidade não atribuída ou da capacidade livre em um pool ou grupo de volumes.

- Ao criar um volume a partir da capacidade não atribuída, você pode criar um pool ou grupo de volumes e o volume ao mesmo tempo.
- Ao criar um volume a partir da capacidade livre, você está criando um volume adicional em um pool ou grupo de volumes já existente.

Depois de expandir a capacidade de volume, você deve aumentar manualmente o tamanho do sistema de arquivos para corresponder. A forma como você faz isso depende do sistema de arquivos que você está usando. Consulte a documentação do sistema operacional do host para obter detalhes.

#### Tipos de capacidade para volumes espessos e volumes finos

Você pode criar volumes espessos ou volumes finos. A capacidade reportada e a capacidade alocada são as mesmas para volumes espessos, mas são diferentes para volumes finos.

- Para um volume grosso, a capacidade relatada do volume é igual à quantidade de capacidade de armazenamento físico alocada. Toda a quantidade de capacidade de armazenamento físico deve estar presente. O espaço fisicamente alocado é igual ao espaço que é relatado ao host.

  Normalmente, você define a capacidade reportada do volume grosso para ser a capacidade máxima para a qual você acha que o volume vai crescer. Os volumes espessos fornecem performance alta e previsível para as aplicações, principalmente porque toda a capacidade de usuário é reservada e alocada na criação.

- Para um volume fino, a capacidade relatada é a capacidade relatada aos hosts, enquanto a capacidade alocada é a quantidade de espaço de unidade atualmente alocada para a gravação de dados.

A capacidade reportada pode ser maior do que a capacidade alocada no storage array. Os volumes finos podem ser dimensionados para acomodar o crescimento sem considerar os ativos atualmente disponíveis.

O Gerenciador de sistema do SANtricity não oferece uma opção para criar thin volumes. Se você quiser criar volumes finos, use a interface de linha de comando (CLI).

#### Limites de capacidade para volumes espessos

A capacidade mínima para um volume espesso é de 1 MIB e a capacidade máxima é determinada pelo número e capacidade das unidades no pool ou grupo de volumes.

Ao aumentar a capacidade reportada para um volume espesso, tenha em mente as seguintes diretrizes:

- Você pode especificar até três casas decimais (por exemplo, 65,375 GiB).
- A capacidade precisa ser inferior (ou igual a) ao máximo disponível no grupo de volumes.

  Quando você cria um volume, alguma capacidade adicional é pré-alocada para migração de tamanho de segmento dinâmico (DSS). A migração DSS é um recurso do software que permite alterar o tamanho do segmento de um volume.

- Volumes maiores que 2 TIB são suportados por alguns sistemas operacionais host (a capacidade máxima relatada é determinada pelo sistema operacional host). Na verdade, alguns sistemas operacionais host suportam até 128 volumes TIB. Consulte a documentação do sistema operacional do host para obter detalhes adicionais.

#### Limites de capacidade para volumes finos

Você pode criar thin volumes com uma grande capacidade relatada e uma capacidade alocada relativamente pequena, o que é benéfico para a utilização e a eficiência do storage. Os thin volumes podem ajudar a simplificar a administração de storage porque a capacidade alocada pode aumentar à medida que as necessidades da aplicação mudam, sem interromper a aplicação, possibilitando uma melhor utilização do storage.

Além da capacidade reportada e da capacidade alocada, os volumes finos também contêm capacidade escrita. Capacidade escrita é a quantidade de capacidade que foi escrita a partir da capacidade reservada alocada para volumes finos.

A tabela a seguir lista os limites de capacidade de um volume fino.

| Tipo de capacidade | Tamanho mínimo | Tamanho máximo |
|---|---|---|
| Comunicado | 32 MIB | 256 TIB |
| Alocado | 4 MIB | 64 TIB |

Para um volume fino, se a capacidade máxima comunicada de 256 TIB tiver sido atingida, não poderá aumentar a sua capacidade. Certifique-se de que a capacidade reservada do volume fino está definida para um tamanho maior do que a capacidade máxima comunicada.

O sistema expande automaticamente a capacidade alocada com base no limite de capacidade alocado. O limite de capacidade alocado permite limitar o crescimento automático do volume fino abaixo da capacidade reportada. Quando a quantidade de dados gravados se aproxima da capacidade alocada, você pode alterar o limite de capacidade alocada.

Para alterar o limite de capacidade alocada, selecione **armazenamento › volumes › separador Thin volume Monitoring › Change Limit** (monitorização de volume fino > alterar limite).

Como o System Manager não aloca a capacidade total quando cria um volume fino, pode haver capacidade livre insuficiente no pool. Espaço insuficiente pode bloquear gravações no pool, não apenas para os volumes finos, mas também para outras operações que exigem capacidade do pool (por exemplo, imagens de snapshot ou volumes de snapshot). No entanto, você ainda pode executar operações de leitura a partir do pool. Se esta situação ocorrer, recebe um aviso de limite de alerta.

#### Monitoramento de volume fino

Você pode monitorar thin volumes em busca de espaço e gerar alertas apropriados para evitar condições de fora da capacidade.

Ambientes com thin Provisioning podem alocar mais espaço lógico do que o storage físico subjacente. Pode selecionar o separador **armazenamento › volumes › monitorização de volume fino** para monitorizar quanto crescimento os seus volumes finos têm antes de atingirem o limite máximo de capacidade atribuída.

Você pode usar a exibição Thin Monitoring para executar as seguintes ações:

- Defina o limite que restringe a capacidade alocada à qual um volume fino pode expandir-se automaticamente.
- Defina o ponto percentual em que um alerta (limite de aviso excedido) é enviado para a área notificações na página inicial quando um volume fino estiver próximo do limite máximo de capacidade alocada.

Para aumentar a capacidade de um volume fino, aumente sua capacidade reportada.

> O System Manager não oferece uma opção para criar thin volumes. Se você quiser criar volumes finos, use a interface de linha de comando (CLI).

> Os volumes finos não estão disponíveis no sistema de armazenamento EF600 ou EF300.

#### Comparação entre volumes grossos e volumes finos

Um volume grosso é sempre totalmente provisionado, o que significa que toda a capacidade é alocada quando o volume é criado. Um volume fino é sempre provisionado de forma fina, o que significa que a capacidade é alocada à medida que os dados estão sendo gravados no volume.

> O System Manager não oferece uma opção para criar thin volumes. Se você quiser criar volumes finos, use a interface de linha de comando (CLI).

| Tipo de volume | Descrição |
| --- | --- |
| Volumes grossos | • Volumes espessos são criados a partir de um pool ou grupo de volumes.<br>• Com volumes espessos, uma grande quantidade de espaço de armazenamento é fornecida antecipadamente, antes de futuras necessidades de storage.<br>• Os volumes espessos são criados com todo o tamanho do volume pré-alocado no armazenamento físico no momento em que o volume é criado. Essa pré-alocação significa que a criação de um volume de 100 GiB realmente consome 100 GiB de capacidade alocada em suas unidades. No entanto, o espaço pode permanecer sem uso, causando subutilização da capacidade de storage.<br>• Ao criar volumes espessos, certifique-se de não alocar a capacidade em excesso para um único volume. A alocação excessiva de capacidade para um único volume pode consumir rapidamente todo o storage físico do sistema.<br>• Tenha em mente que a capacidade de storage também é necessária para serviços de cópia (imagens snapshot, volumes snapshot, cópias de volume e espelhamento assíncrono). Assim, não aloque toda a capacidade para volumes espessos. Espaço insuficiente pode bloquear gravações no pool ou grupo de volumes. Se esta situação ocorrer, receberá um aviso de limite de alerta de capacidade livre. |
| Volumes finos | • Os volumes finos são criados apenas a partir de um pool, não de um grupo de volumes.<br>• Os volumes finos devem ser RAID 6.<br>• Os volumes finos não estão disponíveis no sistema de armazenamento EF600 ou EF300.<br>• Você deve usar a CLI para criar thin volumes.<br>• Ao contrário dos volumes espessos, o espaço necessário para o volume fino não é alocado durante a criação, mas é fornecido, sob demanda em um momento posterior.<br>• Um volume fino permite que você superaloque seu tamanho. Ou seja, você pode atribuir um tamanho de LUN maior que o tamanho do volume. Em seguida, você pode expandir o volume conforme necessário (se necessário, adicionando unidades no processo) sem expandir o tamanho do LUN e, portanto, sem desconetar os usuários.<br>• Você pode usar a recuperação de espaço em bloco de provisionamento reduzido (UNMAP) para recuperar blocos de um volume provisionado com thin no storage array por meio de um comando SCSI UNMAP emitido pelo host. Um storage array compatível com thin Provisioning pode reutilizar o espaço recuperado para atender às solicitações de alocação de algum outro volume thin Provisioning no mesmo storage array, o que permite melhores relatórios sobre o consumo de espaço em disco e uso mais eficiente dos recursos. |

#### Restrições de volume fino

Os thin volumes suportam todas as operações como volumes espessos, com as seguintes exceções:

- Não é possível alterar o tamanho do segmento de um volume fino.
- Não é possível ativar a verificação de redundância de pré-leitura para um volume fino.
- Não é possível usar um volume fino como o volume de destino em uma operação volume de cópia.
- Você pode alterar o limite de capacidade alocada e o limite de aviso de um volume fino apenas no lado principal de um par espelhado assíncrono. Quaisquer alterações a estes parâmetros no lado primário são propagadas automaticamente para o lado secundário.

## Configurar o armazenamento

### Crie workloads

É possível criar workloads para qualquer tipo de aplicação.

#### Sobre esta tarefa

Um workload é um objeto de storage compatível com uma aplicação. Você pode definir uma ou mais cargas de trabalho ou instâncias por aplicação.

#### Passos

1. Selecione **armazenamento › volumes**.
2. Selecione **criar › carga de trabalho**.

   A caixa de diálogo criar carga de trabalho de aplicativo é exibida.

3. Use a lista suspensa para selecionar o tipo de aplicativo para o qual você deseja criar a carga de trabalho e digite um nome de carga de trabalho.
4. Clique em **criar**.

#### Depois de terminar

Você está pronto para adicionar capacidade de storage ao workload criado. Use a opção **Create volume** para criar um ou mais volumes para um aplicativo e alocar quantidades específicas de capacidade para cada volume.

### Criar volumes

Você cria volumes para adicionar capacidade de storage a um workload específico da aplicação e para tornar os volumes criados visíveis para um host ou cluster de host específico. Além disso, a sequência de criação de volume fornece opções para alocar quantidades específicas de capacidade para cada volume que você deseja criar.

#### Sobre esta tarefa

A maioria dos tipos de aplicações é predefinida para uma configuração de volume definida pelo utilizador. Alguns tipos de aplicativos têm uma configuração inteligente aplicada na criação de volume. Por exemplo, se você estiver criando volumes para o aplicativo Microsoft Exchange, será perguntado quantas caixas de correio você precisa, quais são os requisitos médios de capacidade de caixa postal e quantas cópias do banco de dados deseja. O System Manager usa essas informações para criar uma configuração de volume ideal para você, que pode ser editada conforme necessário.

O processo para criar um volume é um procedimento de várias etapas.

#### Passo 1: Selecione host para um volume

Você cria volumes para adicionar capacidade de storage a um workload específico da aplicação e para tornar os volumes criados visíveis para um host ou cluster de host específico. Além disso, a sequência de criação de volume fornece opções para alocar quantidades específicas de capacidade para cada volume que você deseja criar.

**Antes de começar**

- Existem hosts válidos ou clusters de host sob o bloco hosts.
- Identificadores de porta de host foram definidos para o host.
- Antes de criar um volume habilitado PARA DA, a conexão de host que você está planejando usar deve suportar DA. Se qualquer uma das conexões de host nos controladores do storage array não suportar DA, os hosts associados não poderão acessar dados em volumes habilitados PARA DA.

**Sobre esta tarefa**

Tenha estas diretrizes em mente quando atribuir volumes:

- O sistema operacional de um host pode ter limites específicos sobre quantos volumes o host pode acessar. Mantenha essa limitação em mente quando você cria volumes para uso por um host específico.
- Você pode definir uma atribuição para cada volume na matriz de armazenamento.
- Os volumes atribuídos são compartilhados entre controladores no storage array.
- O mesmo número de unidade lógica (LUN) não pode ser usado duas vezes por um host ou um cluster de host para acessar um volume. Você deve usar um LUN exclusivo.
- Se você quiser acelerar o processo de criação de volumes, você pode pular a etapa de atribuição do host para que os volumes recém-criados sejam inicializados offline.

> ⓘ A atribuição de um volume a um host falhará se você tentar atribuir um volume a um cluster de host que esteja em conflito com uma atribuição estabelecida para um host nos clusters de host.

**Passos**

1. Selecione **armazenamento › volumes**.
2. Selecione **criar › volume**.

   A caixa de diálogo criar volumes é exibida.

3. Na lista suspensa, selecione um host ou cluster de host específico ao qual você deseja atribuir volumes ou escolha atribuir o cluster de host ou host posteriormente.
4. Para continuar a sequência de criação de volume para o host ou cluster de host selecionado, clique em **Next** e vá para Etapa 2: Selecione uma carga de trabalho para um volume.

   A caixa de diálogo Selecionar carga de trabalho é exibida.

#### Etapa 2: Selecione uma carga de trabalho para um volume

Selecione uma carga de trabalho para personalizar a configuração do storage array para um aplicativo específico, como Microsoft SQL Server, Microsoft Exchange, aplicativos de vigilância por vídeo ou VMware. Você pode selecionar "outro aplicativo" se o aplicativo que você pretende usar neste storage array não estiver

listado.

**Sobre esta tarefa**

Esta tarefa descreve como criar volumes para uma carga de trabalho existente.

- *Quando você está criando volumes usando uma carga de trabalho específica do aplicativo*, o sistema pode recomendar uma configuração de volume otimizada para minimizar a contenção entre a e/S da carga de trabalho do aplicativo e outro tráfego da instância do aplicativo. Você pode revisar a configuração de volume recomendada e editar, adicionar ou excluir os volumes e caraterísticas recomendados pelo sistema usando a caixa de diálogo Adicionar/Editar volumes.
- *Quando você estiver criando volumes usando "outros"* aplicativos (ou aplicativos sem suporte específico para criação de volume), especifique manualmente a configuração de volume usando a caixa de diálogo Adicionar/Editar volumes.

**Passos**

1. Execute um dos seguintes procedimentos:
   - Selecione a opção **criar volumes para uma carga de trabalho existente** para criar volumes para uma carga de trabalho existente.
   - Selecione a opção **criar uma nova carga de trabalho** para definir uma nova carga de trabalho para um aplicativo compatível ou para "outros" aplicativos.
     - Na lista suspensa, selecione o nome do aplicativo para o qual deseja criar a nova carga de trabalho.

       Selecione uma das entradas "outras" se a aplicação que pretende utilizar nesta matriz de armazenamento não estiver listada.
     - Insira um nome para a carga de trabalho que deseja criar.
2. Clique em **seguinte**.
3. Se sua carga de trabalho estiver associada a um tipo de aplicativo compatível, insira as informações solicitadas; caso contrário, vá para Passo 3: Adicionar ou editar volumes.

#### Passo 3: Adicionar ou editar volumes

O System Manager pode sugerir uma configuração de volume com base na aplicação ou na carga de trabalho selecionada. Essa configuração de volume é otimizada com base no tipo de aplicação compatível com o workload. Você pode aceitar a configuração de volume recomendada ou editá-la conforme necessário. Se você selecionou um dos "outros" aplicativos, você deve especificar manualmente os volumes e as caraterísticas que deseja criar.

**Antes de começar**

- Os pools ou grupos de volumes devem ter capacidade livre suficiente.
- O número máximo de volumes permitido num grupo de volumes é 256.
- O número máximo de volumes permitidos em um pool depende do modelo do sistema de armazenamento:
  - 2.048 volumes (séries EF600 e E5700)
  - 1.024 volumes (EF300)
  - 512 volumes (série E2800)
- Para criar um volume habilitado para Data Assurance (DA), a conexão de host que você está planejando usar deve suportar DA.

**Selecionar um pool ou grupo de volumes com capacidade segura**

Se você quiser criar um volume habilitado PARA DA, selecione um pool ou grupo de volumes que seja capaz de DA (procure **Yes** ao lado de "DA" na tabela de candidatos a grupo de grupo de volume e pool).

As capacidades DA são apresentadas no nível de grupo de volume e pool no System Manager. A proteção DA verifica e corrige erros que podem ocorrer à medida que os dados são transferidos através dos controladores para as unidades. A seleção de um pool ou grupo de volume compatível com DA para o novo volume garante que quaisquer erros sejam detetados e corrigidos.

Se qualquer uma das conexões de host nos controladores do storage array não suportar DA, os hosts associados não poderão acessar dados em volumes habilitados PARA DA.

- Para criar um volume habilitado para segurança, uma chave de segurança deve ser criada para o storage array.

**Selecionar um pool ou grupo de volumes com capacidade segura**

Se você quiser criar um volume habilitado para segurança, selecione um pool ou grupo de volumes que seja capaz de proteger (procure **Sim** ao lado de "compatível com segurança" na tabela de candidatos ao grupo de volumes e pool).

Os recursos de segurança da unidade são apresentados no nível de grupo de volume e pool no System Manager. Unidades com capacidade segura evitam o acesso não autorizado aos dados em uma unidade que é fisicamente removida do storage array. Uma unidade habilitada para segurança criptografa os dados durante gravações e descriptografa os dados durante leituras usando uma chave de criptografia exclusiva_.

Um pool ou grupo de volumes pode conter unidades com capacidade de segurança e não seguras, mas todas as unidades devem ser seguras para usar seus recursos de criptografia.

- Para criar um volume provisionado por recursos, todas as unidades devem ser unidades NVMe com a opção Desalocadas ou não escritas Logical Block Error (DULBE).

**Sobre esta tarefa**

Crie volumes a partir de pools ou grupos de volumes. A caixa de diálogo Adicionar/Editar volumes mostra todos os pools qualificados e grupos de volumes na matriz de armazenamento. Para cada pool qualificado e grupo de volumes, o número de unidades disponíveis e a capacidade total gratuita são exibidos.

Para alguns workloads específicos da aplicação, cada pool ou grupo de volumes qualificado mostra a capacidade proposta com base na configuração de volume sugerida e mostra a capacidade livre restante no GiB. Para outros workloads, a capacidade proposta aparece quando você adiciona volumes a um pool ou grupo de volumes e especifica a capacidade relatada.

**Passos**

1. Escolha uma dessas ações com base se você selecionou outra ou uma carga de trabalho específica do aplicativo:
   - **Other** — clique em **Add new volume** em cada pool ou grupo de volumes que você deseja usar para criar um ou mais volumes.

**Detalhes do campo**

| Campo | Descrição |
| --- | --- |
| Nome do volume | Um volume recebe um nome padrão pelo System Manager durante a sequência de criação de volume. Você pode aceitar o nome padrão ou fornecer um nome mais descritivo indicando o tipo de dados armazenados no volume. |
| Capacidade comunicada | Defina a capacidade do novo volume e as unidades de capacidade a utilizar (MIB, GiB ou TIB). Para volumes espessos, a capacidade mínima é de 1 MIB e a capacidade máxima é determinada pelo número e capacidade das unidades no pool ou grupo de volumes.<br><br>Tenha em mente que a capacidade de storage também é necessária para serviços de cópia (imagens snapshot, volumes snapshot, cópias de volume e espelhos remotos). Portanto, não aloca toda a capacidade a volumes padrão.<br><br>A capacidade em um pool é alocada em incrementos de 4 GiB ou 8 GiB, dependendo do tipo de unidade. Qualquer capacidade que não seja um múltiplo de 4 ou 8 GiB é alocada, mas não utilizável. Para garantir que toda a capacidade possa ser utilizável, especifique a capacidade em incrementos de 4 GiB ou 8 GiB. Se existir capacidade inutilizável, a única forma de a recuperar é aumentar a capacidade do volume. |
| Tamanho do bloco de volume (somente EF300 e EF600) | Mostra os tamanhos de bloco que podem ser criados para o volume:<br><br>• 512 — 512 bytes<br>• 4K — 4.096 bytes |

| Campo | Descrição |
| --- | --- |
| Tamanho do segmento | Mostra a definição para o dimensionamento de segmentos, que aparece apenas para volumes num grupo de volumes. Você pode alterar o tamanho do segmento para otimizar o desempenho.<br><br>• Transições permitidas de tamanho de segmento* — o System Manager determina as transições de tamanho de segmento permitidas. Os tamanhos de segmento que são transições inadequadas do tamanho de segmento atual não estão disponíveis na lista suspensa. As transições permitidas geralmente são o dobro ou metade do tamanho atual do segmento. Por exemplo, se o tamanho atual do segmento de volume for 32 KiB, um novo tamanho de segmento de volume de 16 KiB ou 64 KiB será permitido.<br><br>**Volumes habilitados para cache SSD** — você pode especificar um tamanho de segmento de 4 KiB para volumes habilitados para cache SSD. Certifique-se de selecionar o tamanho de segmento de 4 KiB apenas para volumes habilitados para cache SSD que lidam com operações de e/S de bloco pequeno (por exemplo, tamanhos de bloco de e/S KiB 16 ou menores). O desempenho pode ser afetado se você selecionar 4 KiB como o tamanho do segmento para volumes habilitados para cache SSD que lidam com operações sequenciais de blocos grandes.<br><br>**Quantidade de tempo para alterar o tamanho do segmento** — a quantidade de tempo para alterar o tamanho do segmento de um volume depende dessas variáveis:<br><br>• A carga de e/S do host<br>• A prioridade de modificação do volume<br>• O número de unidades no grupo de volumes<br>• O número de canais da unidade<br>• O poder de processamento dos controladores do storage array<br><br>Quando você altera o tamanho do segmento de um volume, o desempenho de e/S é afetado, mas seus dados permanecem disponíveis. |
| Com capacidade segura | **Yes** aparece ao lado de "Secure-Capable" somente se as unidades no pool ou grupo de volumes forem seguras.<br><br>O Drive Security impede o acesso não autorizado aos dados em uma unidade que é fisicamente removida do storage array. Esta opção só está disponível quando o recurso Segurança da unidade estiver ativado e uma chave de segurança estiver configurada para o storage de armazenamento.<br><br>Um pool ou grupo de volumes pode conter unidades com capacidade de segurança e não seguras, mas todas as unidades devem ser seguras para usar seus recursos de criptografia. |

| Campo | Descrição |
| --- | --- |
| DA | **Yes** aparece ao lado de "DA" somente se as unidades no pool ou grupo de volume suportarem Data Assurance (DA).<br><br>DA aumenta a integridade dos dados em todo o sistema de storage. O DA permite que o storage array verifique se há erros que possam ocorrer à medida que os dados são transferidos através dos controladores para as unidades. O uso DA para o novo volume garante que quaisquer erros sejam detetados. |
| Recurso provisionado (somente EF300 e EF600) | **Sim** aparece ao lado de "recurso provisionado" somente se as unidades suportarem essa opção. O provisionamento de recursos é um recurso disponível nas matrizes de armazenamento EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente sem processo de inicialização em segundo plano. |

- **Carga de trabalho específica do aplicativo** — clique em **Next** para aceitar os volumes e as caraterísticas recomendados pelo sistema para a carga de trabalho selecionada ou clique em **Edit volumes** para alterar, adicionar ou excluir os volumes e as caraterísticas recomendados pelo sistema para a carga de trabalho selecionada.

**Detalhes do campo**

| Campo | Descrição |
| --- | --- |
| Nome do volume | Um volume recebe um nome padrão pelo System Manager durante a sequência de criação de volume. Você pode aceitar o nome padrão ou fornecer um nome mais descritivo indicando o tipo de dados armazenados no volume. |
| Capacidade comunicada | Defina a capacidade do novo volume e as unidades de capacidade a utilizar (MIB, GiB ou TIB). Para volumes espessos, a capacidade mínima é de 1 MIB e a capacidade máxima é determinada pelo número e capacidade das unidades no pool ou grupo de volumes.<br><br>Tenha em mente que a capacidade de storage também é necessária para serviços de cópia (imagens snapshot, volumes snapshot, cópias de volume e espelhos remotos). Portanto, não aloca toda a capacidade a volumes padrão.<br><br>A capacidade em um pool é alocada em incrementos de 4 GiB ou 8 GiB, dependendo do tipo de unidade. Qualquer capacidade que não seja um múltiplo de 4 ou 8 GiB é alocada, mas não utilizável. Para garantir que toda a capacidade possa ser utilizável, especifique a capacidade em incrementos de 4 GiB ou 8 GiB. Se existir capacidade inutilizável, a única forma de a recuperar é aumentar a capacidade do volume. |
| Tipo de volume | Tipo de volume indica o tipo de volume que foi criado para uma carga de trabalho específica do aplicativo. |
| Tamanho do bloco de volume (somente EF300 e EF600) | Mostra os tamanhos de bloco que podem ser criados para o volume:<br><br>• 512 — 512 bytes<br>• 4K — 4.096 bytes |

| Campo | Descrição |
| --- | --- |
| Tamanho do segmento | Mostra a definição para o dimensionamento de segmentos, que aparece apenas para volumes num grupo de volumes. Você pode alterar o tamanho do segmento para otimizar o desempenho.<br><br>• Transições permitidas de tamanho de segmento* — o System Manager determina as transições de tamanho de segmento permitidas. Os tamanhos de segmento que são transições inadequadas do tamanho de segmento atual não estão disponíveis na lista suspensa. As transições permitidas geralmente são o dobro ou metade do tamanho atual do segmento. Por exemplo, se o tamanho atual do segmento de volume for 32 KiB, um novo tamanho de segmento de volume de 16 KiB ou 64 KiB será permitido.<br><br>**Volumes habilitados para cache SSD** — você pode especificar um tamanho de segmento de 4 KiB para volumes habilitados para cache SSD. Certifique-se de selecionar o tamanho de segmento de 4 KiB apenas para volumes habilitados para cache SSD que lidam com operações de e/S de bloco pequeno (por exemplo, tamanhos de bloco de e/S KiB 16 ou menores). O desempenho pode ser afetado se você selecionar 4 KiB como o tamanho do segmento para volumes habilitados para cache SSD que lidam com operações sequenciais de blocos grandes.<br><br>**Quantidade de tempo para alterar o tamanho do segmento** — a quantidade de tempo para alterar o tamanho do segmento de um volume depende dessas variáveis:<br><br>• A carga de e/S do host<br>• A prioridade de modificação do volume<br>• O número de unidades no grupo de volumes<br>• O número de canais da unidade<br>• A capacidade de processamento das controladoras de storage array quando você altera o tamanho de segmento de um volume, a performance de e/S é afetada, mas seus dados permanecem disponíveis. |

| Campo | Descrição |
| --- | --- |
| Com capacidade segura | **Yes** aparece ao lado de "Secure-Capable" somente se as unidades no pool ou grupo de volumes forem seguras.<br><br>A segurança da unidade impede o acesso não autorizado aos dados em uma unidade que é fisicamente removida do storage array. Esta opção só está disponível quando o recurso de segurança da unidade tiver sido ativado e uma chave de segurança estiver configurada para o storage de armazenamento.<br><br>Um pool ou grupo de volumes pode conter unidades com capacidade de segurança e não seguras, mas todas as unidades devem ser seguras para usar seus recursos de criptografia. |
| DA | **Yes** aparece ao lado de "DA" somente se as unidades no pool ou grupo de volume suportarem Data Assurance (DA).<br><br>DA aumenta a integridade dos dados em todo o sistema de storage. O DA permite que o storage array verifique se há erros que possam ocorrer à medida que os dados são transferidos através dos controladores para as unidades. O uso DA para o novo volume garante que quaisquer erros sejam detetados. |
| Recurso provisionado (somente EF300 e EF600) | **Sim** aparece ao lado de "recurso provisionado" somente se as unidades suportarem essa opção. O provisionamento de recursos é um recurso disponível nas matrizes de armazenamento EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente sem processo de inicialização em segundo plano. |

2. Para continuar a sequência de criação de volume para a aplicação selecionada, clique em **seguinte** e aceda a Etapa 4: Revise a configuração do volume.

#### Etapa 4: Revise a configuração do volume

Reveja um resumo dos volumes que pretende criar e faça as alterações necessárias.

**Passos**

1. Reveja os volumes que pretende criar. Clique em **voltar** para fazer quaisquer alterações.
2. Quando estiver satisfeito com a configuração do volume, clique em **Finish**.

**Resultados**

O System Manager cria os novos volumes nos pools e grupos de volumes selecionados e exibe os novos volumes na tabela todos os volumes.

**Depois de terminar**

- Execute todas as modificações do sistema operacional necessárias no host do aplicativo para que os aplicativos possam usar o volume.
- Execute o utilitário específico do sistema operacional (disponível a partir de um fornecedor de terceiros) e execute o comando SMcli `-identifyDevices` para correlacionar nomes de volume com nomes de storage de host.

  O SMcli está disponível diretamente através do Gerenciador do sistema SANtricity. Esta versão para download do SMcli está disponível nos controladores EF600, EF300, E5700, EF570, E2800 e EF280. Para fazer o download do SMcli no Gerenciador do sistema SANtricity, selecione **Configurações** > **sistema** e **Complementos** > **Interface de linha de comando** .

### Adicionar volumes ao workload

Você pode adicionar um ou mais volumes a um workload novo ou existente para volumes que não estão associados atualmente a um workload.

**Sobre esta tarefa**

Os volumes não são associados a uma carga de trabalho se tiverem sido criados usando a interface de linha de comando (CLI) ou se tiverem sido migrados (importados/exportados) de um storage array diferente.

**Passos**

1. Selecione **armazenamento › volumes**.
2. Selecione a guia **aplicativos e cargas de trabalho**.

   A exibição aplicações e cargas de trabalho é exibida.

3. Selecione **Adicionar à carga de trabalho**.

   A caixa de diálogo Selecionar carga de trabalho é exibida.

4. Execute uma das seguintes ações:
   - **Adicionar volumes a uma carga de trabalho existente** — Selecione esta opção para adicionar volumes a uma carga de trabalho existente.

     Use a lista suspensa para selecionar uma carga de trabalho. O tipo de aplicativo associado da carga de trabalho é atribuído aos volumes que você adiciona a essa carga de trabalho.

   - **Adicionar volumes a uma nova carga de trabalho** — Selecione essa opção para definir uma nova carga de trabalho para um tipo de aplicativo e adicionar volumes à nova carga de trabalho.
5. Selecione **Next** para continuar com a sequência de adição à carga de trabalho.

   A caixa de diálogo Selecionar volumes é exibida.

6. Selecione os volumes que você deseja adicionar à carga de trabalho.
7. Revise os volumes que você deseja adicionar à carga de trabalho selecionada.

8. Quando estiver satisfeito com a configuração da carga de trabalho, clique em **Finish**.

## Gerenciar volumes

### Aumentar a capacidade de um volume

Você pode aumentar a capacidade reportada (a capacidade relatada aos hosts) de um volume usando a capacidade livre disponível no pool ou no grupo de volumes.

#### Antes de começar

- A capacidade livre suficiente está disponível no pool ou grupo de volumes associados ao volume.
- O volume é ótimo e não em nenhum estado de modificação.
- A capacidade máxima reportada de 256 TIB não foi atingida para volumes finos.
- Não há unidades hot spare em uso no volume. (Aplica-se apenas a volumes em grupos de volumes.)

Você só pode expandir a capacidade de volume até 128 TIB em um único momento.

#### Sobre esta tarefa

Lembre-se de quaisquer requisitos de capacidade futuros que você possa ter para outros volumes nesse pool ou grupo de volumes. Certifique-se de que permite uma capacidade livre suficiente para criar imagens instantâneas, volumes instantâneos ou espelhos remotos.

O aumento da capacidade de um volume é suportado apenas em determinados sistemas operacionais. Se você aumentar a capacidade de volume em um sistema operacional host que não é suportado, a capacidade expandida será inutilizável e você não poderá restaurar a capacidade de volume original.

#### Passos

1. Selecione **armazenamento › volumes**.
2. Selecione o volume para o qual deseja aumentar a capacidade e, em seguida, selecione **aumentar a capacidade**.

   A caixa de diálogo confirmar aumento de capacidade é exibida.

3. Selecione **Sim** para continuar.

   É apresentada a caixa de diálogo aumentar capacidade comunicada.

   Esta caixa de diálogo exibe a capacidade atual reportada do volume e a capacidade livre disponível no pool ou grupo de volumes associados do volume.

4. Use a caixa **aumente a capacidade reportada adicionando…** para adicionar capacidade à capacidade reportada disponível atual. Você pode alterar o valor de capacidade para exibir em mebibytes (MIB), gibibytes (GiB) ou tebibytes (TIB).
5. Clique em **aumentar**.

#### Resultados

- O System Manager aumenta a capacidade do volume com base na sua seleção.
- Selecione **Home › View Operations in Progress** (Ver operações em curso) para ver o progresso da

operação de aumento de capacidade que está atualmente em execução para o volume selecionado. Esta operação pode ser demorada e pode afetar o desempenho do sistema.

**Depois de terminar**

Depois de expandir a capacidade de volume, você deve aumentar manualmente o tamanho do sistema de arquivos para corresponder. A forma como você faz isso depende do sistema de arquivos que você está usando. Consulte a documentação do sistema operacional do host para obter detalhes.

### Inicializar volumes

Um volume é inicializado automaticamente quando é criado pela primeira vez. No entanto, o Recovery Guru pode aconselhar que você inicialize manualmente um volume para recuperar de certas condições de falha. Utilize esta opção apenas sob a orientação do suporte técnico. Pode selecionar um ou mais volumes para inicializar.

**Antes de começar**

- Todas as operações de e/S foram interrompidas.
- Todos os dispositivos ou sistemas de arquivos nos volumes que você deseja inicializar devem ser desmontados.
- O volume está no estado ideal e não estão em curso operações de modificação no volume.

> Não é possível cancelar a operação depois de iniciada. Todos os dados de volume são apagados. Não tente esta operação, a menos que o Recovery Guru o aconselhe a fazê-lo. Contacte o suporte técnico antes de iniciar este procedimento.

**Sobre esta tarefa**

Ao inicializar um volume, o volume mantém suas configurações WWN, atribuições de host, capacidade alocada e capacidade reservada. Ele também mantém as mesmas configurações de garantia de dados (DA) e configurações de segurança.

Os seguintes tipos de volumes *não podem* ser inicializados:

- Volume base de um volume instantâneo
- Volume primário em uma relação espelhada
- Volume secundário em uma relação de espelho
- Volume de origem em uma cópia de volume
- Volume de destino em uma cópia de volume
- Volume que já tem uma inicialização em curso

Este tópico aplica-se apenas a volumes padrão criados a partir de pools ou grupos de volumes.

**Passos**

1. Selecione **armazenamento › volumes**.
2. Selecione qualquer volume e, em seguida, selecione **mais › Inicializar volumes**.

   A caixa de diálogo Inicializar volumes é exibida. Todos os volumes na matriz de armazenamento aparecem nesta caixa de diálogo.

3. Selecione um ou mais volumes que deseja inicializar e confirme que deseja executar a operação.

**Resultados**

O System Manager executa as seguintes ações:

- Apaga todos os dados dos volumes que foram inicializados.
- Limpa os índices de bloco, o que faz com que os blocos não escritos sejam lidos como se fossem preenchidos com zero (o volume parece estar completamente vazio).

Selecione **Home › View Operations in Progress** (Ver operações em curso) para ver o progresso da operação de inicialização que está atualmente em execução para o volume selecionado. Esta operação pode ser demorada e pode afetar o desempenho do sistema.

### Redistribuir volumes

Você redistribui volumes para mover volumes de volta para os proprietários de controladores preferenciais. Normalmente, os drivers multipath movem volumes do proprietário da controladora preferida quando ocorre um problema ao longo do caminho de dados entre o host e o storage array.

**Antes de começar**

- Os volumes que você deseja redistribuir não estão em uso, ou erros de e/S ocorrerão.
- Um driver multipath é instalado em todos os hosts usando os volumes que você deseja redistribuir, ou erros de e/S ocorrerão.

  Se você quiser redistribuir volumes sem um driver multipath nos hosts, todas as atividades de e/S nos volumes *enquanto a operação de redistribuição estiver em andamento* devem ser interrompidas para evitar erros de aplicativo.

**Sobre esta tarefa**

A maioria dos drivers multipath de host tenta acessar cada volume em um caminho para o proprietário do controlador preferido. No entanto, se esse caminho preferido ficar indisponível, o driver multipath no host fará failover para um caminho alternativo. Esse failover pode fazer com que a propriedade do volume mude para o controlador alternativo. Depois de resolver a condição que causou o failover, alguns hosts podem mover automaticamente a propriedade do volume de volta para o proprietário do controlador preferido, mas, em alguns casos, talvez seja necessário redistribuir manualmente os volumes.

**Passos**

1. Selecione **armazenamento › volumes**.
2. Selecione **mais › redistribuir volumes**.

   A caixa de diálogo redistribuir volumes é exibida. Todos os volumes na matriz de armazenamento cujo proprietário de controlador preferido não corresponde ao proprietário atual aparecem nesta caixa de diálogo.

3. Selecione um ou mais volumes que deseja redistribuir e confirme que deseja executar a operação.

**Resultados**

O System Manager move os volumes selecionados para seus proprietários de controladores preferidos ou você pode ver uma caixa de diálogo redistribuir volumes desnecessários.

### Alterar a propriedade do controlador de um volume

Você pode alterar a propriedade de um volume do controlador preferido, de modo que a e/S para aplicativos de host seja direcionada pelo novo caminho.

#### Antes de começar

Se você não usar um driver multipath, quaisquer aplicativos de host que estejam usando o volume no momento devem ser desligados. Essa ação impede erros de aplicativo quando o caminho de e/S muda.

#### Sobre esta tarefa

Você pode alterar a propriedade do controlador para um ou mais volumes em um pool ou grupo de volumes.

#### Passos

1. Selecione **armazenamento › volumes**.
2. Selecione qualquer volume e, em seguida, selecione **mais › alterar propriedade**.

   A caixa de diálogo alterar propriedade do volume é exibida. Todos os volumes na matriz de armazenamento aparecem nesta caixa de diálogo.

3. Use a lista suspensa **Preferred Owner** para alterar o controlador preferido para cada volume que você deseja alterar e confirme se deseja executar a operação.

#### Resultados

- O System Manager altera a propriedade do controlador do volume. E/S para o volume agora é direcionado através deste caminho de e/S.
- O volume pode não usar o novo caminho de e/S até que o driver multipath reconfigure para reconhecer o novo caminho. Essa ação geralmente leva menos de cinco minutos.

### Eliminar volume

Normalmente, você exclui volumes se os volumes tiverem sido criados com os parâmetros ou a capacidade errados, não atenderem mais às necessidades de configuração de storage ou forem imagens snapshot que não são mais necessárias para backup ou teste de aplicativos.

A exclusão de um volume aumenta a capacidade livre no pool ou grupo de volumes. Pode selecionar um ou mais volumes para eliminar.

#### Antes de começar

Nos volumes que pretende eliminar, certifique-se do seguinte:

- É feito backup de todos os dados.
- Todas as entradas/saídas (e/S) estão paradas.
- Todos os dispositivos e sistemas de arquivos são desmontados.

#### Sobre esta tarefa

Não é possível eliminar um volume que tenha uma destas condições:

- O volume está a ser inicializado.
- O volume está reconstruindo.

- O volume faz parte de um grupo de volumes que contém uma unidade que está passando por uma operação de cópia.
- O volume está passando por uma operação de modificação, como uma alteração do tamanho do segmento, a menos que o volume esteja agora no status Failed (Falha).
- O volume está mantendo qualquer tipo de reserva persistente.
- O volume é um volume de origem ou um volume de destino em um volume de cópia que tem um status de pendente, em andamento ou Falha.

A exclusão de um volume causa a perda de todos os dados nesses volumes.

Quando um volume excede um determinado tamanho (atualmente 128 TB), a exclusão está sendo executada em segundo plano e o espaço livre pode não estar imediatamente disponível.

**Passos**

1. Selecione **armazenamento › volumes**.
2. Clique em **Excluir**.

   A caixa de diálogo Excluir volumes é exibida.

3. Selecione um ou mais volumes que pretende eliminar e confirme que pretende executar a operação.
4. Clique em **Excluir**.

**Resultados**

O System Manager executa as seguintes ações:

- Elimina quaisquer imagens instantâneas, agendas e volumes instantâneos associados.
- Remove quaisquer relações de espelhamento.
- Aumenta a capacidade livre no pool ou grupo de volume.

### Alterar o limite de capacidade alocado para um volume fino

Para volumes finos capazes de alocar espaço sob demanda, você pode alterar o limite que restringe a capacidade alocada à qual um volume fino pode se expandir automaticamente.

Você também pode alterar o ponto percentual no qual um alerta (limite de aviso excedido) é enviado para a área notificações na página inicial quando um volume fino estiver próximo do limite de capacidade alocado. Pode optar por ativar ou desativar esta notificação de alerta.

Este recurso não está disponível no sistema de armazenamento EF600 ou EF300.

O sistema expande automaticamente a capacidade alocada com base no limite de capacidade alocado. O limite de capacidade alocado permite limitar o crescimento automático do volume fino abaixo da capacidade reportada. Quando a quantidade de dados gravados se aproxima da capacidade alocada, você pode alterar o limite de capacidade alocada.

Ao alterar o limite de capacidade alocada e o limite de aviso de um volume fino, você deve levar em conta o espaço a ser consumido pelos dados do usuário do volume e pelos dados dos serviços de cópia.

**Passos**

1. Selecione **armazenamento › volumes**.
2. Selecione a guia **Thin volume Monitoring**.

   É apresentada a vista Thin volume Monitoring (monitorização de volume fino).

3. Selecione o volume fino que deseja alterar e, em seguida, selecione **alterar limite**.

   A caixa de diálogo alterar limite é exibida. A definição limite de capacidade alocada e limite de aviso para o volume fino selecionado são apresentadas nesta caixa de diálogo.

4. Altere o limite de capacidade alocado e o limite de aviso conforme necessário.

   **Detalhes do campo**

| Definição | Descrição |
|---|---|
| Alterar limite capacidade alocada para… | O limite no qual as gravações falham, impedindo que o volume fino consuma recursos adicionais. Esse limite é uma porcentagem do tamanho da capacidade informada do volume. |
| Alerta-me quando… (limiar de aviso) | Marque a caixa de seleção se desejar que o sistema gere um alerta quando um volume fino estiver próximo do limite de capacidade alocado. O alerta é enviado para a área notificações na página inicial. Esse limite é uma porcentagem do tamanho da capacidade informada do volume.<br><br>Desmarque a caixa de verificação para desativar a notificação de alerta de limite de aviso. |

5. Clique em **Salvar**.

## Gerir definições

### Altere as definições de um volume

Você pode alterar as configurações de um volume, como nome, atribuição de host, tamanho do segmento, prioridade de modificação, cache e assim por diante.

**Antes de começar**

O volume que pretende alterar está no estado ideal.

> Algumas operações podem estar indisponíveis enquanto as alterações nas definições de volume estão em curso

**Passos**

1. Selecione **armazenamento › volumes**.
2. Selecione o volume que pretende alterar e, em seguida, selecione **Ver/Editar definições**.

   A caixa de diálogo Configurações de volume é exibida. As definições de configuração do volume

selecionado são apresentadas nesta caixa de diálogo.

3. Selecione a guia **Basic** para alterar o nome do volume e a atribuição do host.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| Nome | Exibe o nome do volume. Altere o nome de um volume quando o nome atual não for mais significativo ou aplicável. |
| Capacidades | Apresenta a capacidade comunicada e alocada para o volume selecionado.<br><br>A capacidade reportada e a capacidade alocada são as mesmas para volumes espessos, mas são diferentes para volumes finos. Para um volume grosso, o espaço fisicamente alocado é igual ao espaço relatado ao host. Para um volume fino, a capacidade relatada é a capacidade relatada aos hosts, enquanto a capacidade alocada é a quantidade de espaço de unidade atualmente alocada para a gravação de dados. |
| Grupo de pool / volume | Exibe o nome e o nível RAID do pool ou grupo de volumes. Indica se o pool ou grupo de volume é seguro e seguro. |
| Host | Exibe a atribuição de volume. Você atribui um volume a um host ou cluster de host para que ele possa ser acessado para operações de e/S. Essa atribuição concede a um host ou cluster de host acesso a um volume específico ou a um número de volumes em um storage array.<br><br>• **Assigned to** — identifica o cluster de host ou host que tem acesso ao volume selecionado.<br>• **LUN** — Um número de unidade lógica (LUN) é o número atribuído ao espaço de endereço que um host usa para acessar um volume. O volume é apresentado ao host como capacidade na forma de um LUN. Cada host tem seu próprio espaço de endereço LUN. Portanto, o mesmo LUN pode ser usado por diferentes hosts para acessar diferentes volumes.<br><br>Para interfaces NVMe, essa coluna exibe o ID do namespace. Um namespace é o armazenamento NVM formatado para acesso a bloco. É análogo a uma unidade lógica em SCSI, que se relaciona a um volume no storage array. O ID do namespace é o identificador exclusivo da controladora NVMe para o namespace e pode ser definido como um valor entre 1 e 255. É análogo a um número de unidade lógica (LUN) no SCSI. |

| Definição | Descrição |
| --- | --- |
| Identificadores | Exibe os identificadores para o volume selecionado.<br>• * Identificador mundial (WWID)* — Um identificador hexadecimal exclusivo para o volume.<br>• * Identificador exclusivo estendido (EUI)* — um identificador EUI-64 para o volume.<br>• **Identificador do subsistema (SSID)** — o identificador do subsistema da matriz de armazenamento de um volume. |

4. Selecione a guia **Avançado** para alterar configurações adicionais de um volume em um pool ou em um grupo de volumes.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| Informações sobre aplicações e workloads | Durante a criação de volume, você pode criar workloads específicos da aplicação ou outros workloads. Se aplicável, o nome da carga de trabalho, o tipo de aplicativo e o tipo de volume serão exibidos para o volume selecionado.<br><br>Você pode alterar o nome da carga de trabalho, se desejado. |
| Definições de qualidade do serviço | **Disable permanentemente data Assurance** — esta configuração aparece somente se o volume estiver habilitado para Data Assurance (DA). O DA verifica e corrige erros que podem ocorrer à medida que os dados são transferidos através dos controladores para as unidades. Utilize esta opção para desativar permanentemente DA no volume selecionado. Quando desativado, não é possível reativar DA neste volume.<br><br>**Ativar verificação de redundância de pré-leitura** — esta definição aparece apenas se o volume for um volume espesso. As verificações de redundância de pré-leitura determinam se os dados em um volume são consistentes sempre que uma leitura é executada. Um volume que tenha esse recurso ativado retorna erros de leitura se os dados forem determinados como inconsistentes pelo firmware do controlador. |
| Propriedade do controlador | Define o controlador que é designado para ser o controlador proprietário, ou principal, do volume.<br><br>A propriedade do controlador é muito importante e deve ser planejada cuidadosamente. Os controladores devem ser balanceados o mais próximo possível para e/S totais. |

| Definição | Descrição |
| --- | --- |
| Dimensionamento do segmento | Mostra a definição para o dimensionamento de segmentos, que aparece apenas para volumes num grupo de volumes. Você pode alterar o tamanho do segmento para otimizar o desempenho.<br><br>• Transições permitidas de tamanho de segmento* — o System Manager determina as transições de tamanho de segmento permitidas. Os tamanhos de segmento que são transições inadequadas do tamanho de segmento atual não estão disponíveis na lista suspensa. As transições permitidas geralmente são o dobro ou metade do tamanho atual do segmento. Por exemplo, se o tamanho atual do segmento de volume for 32 KiB, um novo tamanho de segmento de volume de 16 KiB ou 64 KiB será permitido.<br><br>**Volumes habilitados para cache SSD** — você pode especificar um tamanho de segmento de 4 KiB para volumes habilitados para cache SSD. Certifique-se de selecionar o tamanho de segmento de 4 KiB apenas para volumes habilitados para cache SSD que lidam com operações de e/S de bloco pequeno (por exemplo, tamanhos de bloco de e/S KiB 16 ou menores). O desempenho pode ser afetado se você selecionar 4 KiB como o tamanho do segmento para volumes habilitados para cache SSD que lidam com operações sequenciais de blocos grandes.<br><br>**Quantidade de tempo para alterar o tamanho do segmento** — a quantidade de tempo para alterar o tamanho do segmento de um volume depende dessas variáveis:<br><br>• A carga de e/S do host<br>• A prioridade de modificação do volume<br>• O número de unidades no grupo de volumes<br>• O número de canais da unidade<br>• A capacidade de processamento das controladoras de storage array quando você altera o tamanho de segmento de um volume, a performance de e/S é afetada, mas seus dados permanecem disponíveis. |
| Prioridade de modificação | Mostra a definição de prioridade de modificação, que só aparece para volumes num grupo de volumes.<br><br>A prioridade de modificação define quanto tempo de processamento é alocado para operações de modificação de volume em relação ao desempenho do sistema. Você pode aumentar a prioridade de modificação de volume, embora isso possa afetar o desempenho do sistema.<br><br>Mova as barras deslizantes para selecionar um nível de prioridade.<br><br>**Taxas de prioridade de modificação** — a taxa de prioridade mais baixa beneficia o desempenho do sistema, mas a operação de modificação demora mais tempo. A taxa de prioridade mais alta beneficia a operação de modificação, mas o desempenho do sistema pode estar comprometido. |

| Definição | Descrição |
| --- | --- |
| Armazenamento em cache | Mostra a configuração de armazenamento em cache, que pode ser alterada para afetar o desempenho geral de e/S de um volume. |
| Cache SSD | Mostra a configuração cache SSD, que pode ser ativada em volumes compatíveis como forma de melhorar o desempenho somente leitura. Os volumes são compatíveis se compartilharem os mesmos recursos de segurança de unidade e garantia de dados.<br><br>**O recurso cache SSD usa um único ou vários discos de estado sólido (SSDs) para implementar um cache de leitura**. O desempenho da aplicação é aprimorado devido aos tempos de leitura mais rápidos para SSDs. Como o cache de leitura está no storage array, o armazenamento em cache é compartilhado em todos os aplicativos que usam o storage array. Basta selecionar o volume que você deseja armazenar em cache e, em seguida, o armazenamento em cache é automático e dinâmico. |

5. Clique em **Salvar**.

   O System Manager altera as definições do volume com base nas suas seleções.

**Depois de terminar**

Selecione **Home › View Operations in Progress** (Ver operações em curso) para ver o progresso das operações de alteração atualmente em execução para o volume selecionado.

### Altere as configurações da carga de trabalho

Você pode alterar o nome de uma carga de trabalho e exibir seu tipo de aplicativo associado. Altere o nome de uma carga de trabalho quando o nome atual não for mais significativo ou aplicável.

**Passos**

1. Selecione **armazenamento › volumes**.
2. Selecione a guia **aplicativos e cargas de trabalho**.

   A exibição aplicações e cargas de trabalho é exibida.

3. Selecione a carga de trabalho que você deseja alterar e selecione **Exibir/Editar configurações**.

   A caixa de diálogo Configurações de aplicativos e cargas de trabalho é exibida.

4. **Opcional:** altere o nome fornecido pelo usuário da carga de trabalho.
5. Clique em **Salvar**.

### Altere as configurações de cache para um volume

Você pode alterar as configurações de cache de leitura e cache de gravação para afetar o desempenho geral de e/S de um volume.

### Sobre esta tarefa

Mantenha estas diretrizes em mente quando você alterar as configurações de cache para um volume:

- Depois de abrir a caixa de diálogo alterar configurações de cache, você pode ver um ícone exibido ao lado das propriedades de cache selecionadas. Este ícone indica que o controlador suspendeu temporariamente as operações de armazenamento em cache.

  Esta ação pode ocorrer quando uma nova bateria está sendo carregada, quando um controlador foi removido ou se uma incompatibilidade nos tamanhos de cache tiver sido detetada pelo controlador. Depois que a condição for desmarcada, as propriedades de cache selecionadas na caixa de diálogo ficam ativas. Se as propriedades de cache selecionadas não estiverem ativas, entre em Contato com o suporte técnico.

- Você pode alterar as configurações de cache para um único volume ou para vários volumes em uma matriz de armazenamento. Você pode alterar as configurações de cache para todos os volumes padrão ou todos os volumes finos ao mesmo tempo.

### Passos

1. Selecione **armazenamento › volumes**.
2. Selecione qualquer volume e, em seguida, selecione **mais › alterar definições de cache**.

   A caixa de diálogo alterar configurações de cache é exibida. Todos os volumes na matriz de armazenamento aparecem nesta caixa de diálogo.

3. Selecione a guia **Basic** para alterar as configurações de armazenamento em cache de leitura e armazenamento em cache de gravação.

   **Detalhes do campo**

   | Definição de cache | Descrição |
   |---|---|
   | Leia o Cache | O cache de leitura é um buffer que armazena dados que foram lidos das unidades. Os dados para uma operação de leitura podem já estar no cache de uma operação anterior, o que elimina a necessidade de acessar as unidades. Os dados permanecem no cache de leitura até que sejam lavados. |
   | Gravar cache | O cache de gravação é um buffer que armazena dados do host que ainda não foram gravados nas unidades. Os dados permanecem no cache de gravação até que sejam gravados nas unidades. O armazenamento em cache de gravação pode aumentar a performance de e/S.<br>O cache é automaticamente lavado após o **Write caching** estar desativado para um volume. |

4. Selecione a guia **Avançado** para alterar as configurações avançadas para volumes espessos. As configurações avançadas de cache estão disponíveis apenas para volumes espessos.

**Detalhes do campo**

| Definição de cache | Descrição |
| --- | --- |
| Pré-gravação de Cache de leitura dinâmica | A pré-busca de leitura de cache dinâmico permite que o controlador copie blocos de dados sequenciais adicionais para o cache enquanto ele está lendo blocos de dados de uma unidade para o cache. Esse armazenamento em cache aumenta a chance de que futuras solicitações de dados possam ser preenchidas a partir do cache. A pré-busca de leitura de cache dinâmico é importante para aplicativos Multimídia que usam e/S sequenciais A taxa e a quantidade de dados pré-obtidos no cache são auto-ajustáveis com base na taxa e no tamanho da solicitação das leituras do host. O acesso aleatório não faz com que os dados sejam pré-obtidos no cache. Este recurso não se aplica quando o armazenamento em cache de leitura está desativado.<br><br>Para um volume fino, a pré-busca de leitura de cache dinâmico é sempre desativada e não pode ser alterada. |
| Escreva a cache sem baterias | A configuração de armazenamento de gravação sem baterias permite que o armazenamento em cache continue, mesmo quando as baterias estiverem em falta, falharem, descarregadas completamente ou não estiverem totalmente carregadas. Normalmente, a escolha do armazenamento em cache sem baterias não é recomendada, pois os dados podem ser perdidos se perder energia. Normalmente, o armazenamento em cache de gravação é desligado temporariamente pelo controlador até que as baterias sejam carregadas ou uma bateria com falha seja substituída.<br><br>* Possível perda de dados * - se você selecionar esta opção e não tiver uma fonte de alimentação universal para proteção, você pode perder dados. Além disso, você pode perder dados se não tiver baterias do controlador e ativar a opção **armazenamento em cache sem baterias**.<br><br>Esta configuração estará disponível somente se você tiver habilitado o armazenamento em cache de gravação. Esta definição não está disponível para volumes finos. |
| Escrever cache com espelhamento | O cache de gravação com espelhamento ocorre quando os dados gravados na memória de cache de um controlador também são gravados na memória de cache do outro controlador. Portanto, se um controlador falhar, o outro pode concluir todas as operações de gravação pendentes. O espelhamento do cache de gravação estará disponível somente se o armazenamento em cache de gravação estiver habilitado e duas controladoras estiverem presentes. O armazenamento em cache de gravação com espelhamento é a configuração padrão na criação de volume.<br><br>Esta configuração estará disponível somente se você tiver habilitado o armazenamento em cache de gravação. Esta definição não está disponível para volumes finos. |

5. Clique em **Salvar** para alterar as configurações de cache.

### Alterar as definições de digitalização de multimédia para um volume

Uma verificação de Mídia é uma operação em segundo plano que verifica todos os dados e informações de redundância no volume. Utilize esta opção para ativar ou desativar as definições de digitalização de multimédia para um ou mais volumes ou para alterar a duração da digitalização.

#### Antes de começar

Entenda o seguinte:

- As digitalizações multimédia são executadas continuamente a uma taxa constante, com base na capacidade a digitalizar e na duração da digitalização. As digitalizações em segundo plano podem ser temporariamente suspensas por uma tarefa de fundo de prioridade mais elevada (por exemplo, reconstrução), mas serão retomadas com a mesma taxa constante.
- Um volume só é lido quando a opção de digitalização de material está ativada para a matriz de armazenamento e para esse volume. Se a verificação de redundância também estiver ativada para esse volume, as informações de redundância no volume serão verificadas quanto à consistência com os dados, desde que o volume tenha redundância. A verificação de Mídia com verificação de redundância é ativada por padrão para cada volume quando é criado.
- Se for encontrado um erro de meio irrecuperável durante a verificação, os dados serão reparados usando informações de redundância, se disponíveis.

  Por exemplo, as informações de redundância estão disponíveis em volumes RAID 5 ideais ou em volumes RAID 6 ideais ou que só têm uma unidade com falha. Se o erro irrecuperável não puder ser reparado usando informações de redundância, o bloco de dados será adicionado ao log de setor ilegível. Os erros de meio corrigíveis e incorrigíveis são reportados ao log de eventos.

  Se a verificação de redundância encontrar uma inconsistência entre os dados e as informações de redundância, ela será reportada ao log de eventos.

#### Sobre esta tarefa

As digitalizações de Mídia detetam e reparam erros de Mídia em blocos de disco que são raramente lidos por aplicativos. Isso pode impedir a perda de dados em caso de falha de unidade, uma vez que os dados para unidades com falha são reconstruídos usando informações de redundância e dados de outras unidades no grupo de volumes ou pool.

Você pode executar as seguintes ações:

- Ative ou desative digitalizações de Mídia em segundo plano para toda a matriz de armazenamento
- Altere a duração da digitalização para toda a matriz de armazenamento
- Ative ou desative a digitalização de multimédia para um ou mais volumes
- Ative ou desative a verificação de redundância para um ou mais volumes

#### Passos

1. Selecione **armazenamento › volumes**.
2. Selecione qualquer volume e, em seguida, selecione **mais › alterar definições de digitalização de multimédia**.

É apresentada a caixa de diálogo alterar as definições de digitalização de multimédia da unidade. Todos os volumes na matriz de armazenamento aparecem nesta caixa de diálogo.

3. Para ativar a digitalização de material, selecione a caixa de verificação **Digitalizar material ao longo de…** .

   A caixa de verificação desativar a digitalização de multimédia suspende todas as definições de digitalização de multimédia.

4. Especifique o número de dias durante os quais pretende que a digitalização de material seja executada.
5. Selecione a caixa de verificação **Media Scan** para cada volume em que pretende efetuar uma digitalização de multimédia.

   O System Manager ativa a opção Verificação de redundância para cada volume no qual você escolhe executar uma digitalização de Mídia. Se houver volumes individuais para os quais você não deseja executar uma verificação de redundância, desmarque a caixa de seleção **Verificação de redundância**.

6. Clique em **Salvar**.

   O Gestor do sistema aplica alterações às verificações de multimédia em segundo plano com base na sua seleção.

## Use serviços de cópia

### Visão geral do volume de cópia

A função volume de cópia permite criar uma cópia pontual de um volume criando dois volumes separados, o volume de origem e o volume de destino, na mesma matriz de armazenamento.

Esta função executa uma cópia byte por byte do volume de origem para o volume de destino, tornando os dados no volume de destino idênticos aos dados no volume de origem.

#### Cópia de dados para maior acesso

À medida que os requisitos de storage para uma alteração de volume, você pode usar a função Copiar volume para copiar dados de pools ou grupos de volumes que usam unidades de capacidade menor para pools ou grupos de volumes que usam unidades de capacidade maior. Por exemplo, você pode usar a função volume de cópia para fazer o seguinte:

- Mover dados para unidades maiores.
- Mude para unidades com uma taxa de transferência de dados mais alta.
- Mudança para unidades que usam novas tecnologias para obter maior desempenho.
- Altere um volume fino para um volume grosso.

Os volumes de origem e destino da cópia devem ter os mesmos tamanhos de bloco lógico/endereçável para host relatados (tamanho do setor).

Os tamanhos de bloco de volume relatados são:

- **Tamanho de bloco nativo** – o tamanho do bloco do volume corresponde ao tamanho do bloco da unidade, 512 ou 4K.

- * Tamanho de bloco emulado 512 * - as unidades são 4K, mas o tamanho de bloco relatado é 512.

#### Altere um volume fino para um volume grosso

Se você quiser alterar um volume fino para um volume espesso, use a operação volume de cópia para criar uma cópia do volume fino. O destino de uma operação de volume de cópia é sempre um volume grosso.

> O System Manager não oferece uma opção para criar thin volumes. Se você quiser criar volumes finos, use a interface de linha de comando (CLI).

#### Dados de backup

A função volume de cópia permite fazer backup de um volume copiando dados de um volume para outro volume na mesma matriz de armazenamento. Você pode usar o volume de destino como um backup para o volume de origem, para teste do sistema ou para fazer backup em outro dispositivo, como uma unidade de fita.

#### Restaure os dados do volume do Snapshot para o volume base

Se precisar restaurar dados para o volume base do volume instantâneo associado, use a função Copiar volume para copiar dados do volume instantâneo para o volume base. Você pode criar uma cópia de volume dos dados no volume instantâneo e, em seguida, copiar os dados para o volume base.

#### Volumes de origem e destino

A tabela a seguir especifica os tipos de volumes que podem ser usados para volumes de origem e destino com a função volume de cópia.

| Tipo de volume | Volume off-line de cópia de volume de origem | Volume de origem de cópia de volume on-line | Volume alvo online e offline |
|---|---|---|---|
| Volume grosso em uma piscina | Sim | Sim | Sim |
| Volume grosso em um grupo de volume | Sim | Sim | Sim |
| Volume fino | Sim, 1 | Sim | Não |
| Volume do Snapshot | Sim, 2 | Não | Não |
| Volume de base do Snapshot | Sim | Sim | Não |
| Volume primário do espelho remoto | Sim, 3 | Sim | Não |

1 o volume-alvo deve ter uma capacidade igual ou superior à capacidade de volume fino reportada.

2 não é possível usar a cópia do volume instantâneo até que a operação de cópia online seja concluída.

3 se o volume de origem for um volume primário, a capacidade do volume de destino deve ser igual ou

superior à capacidade utilizável do volume de origem.

### Tipos de operações de volume de cópia

Você pode executar uma operação *offline* Copy volume ou uma operação *online* Copy volume. Uma operação off-line lê os dados de um volume de origem e os copia para um volume de destino. Uma operação on-line usa um volume snapshot como origem e copia seus dados em um volume de destino.

Para garantir a integridade dos dados, toda a atividade de e/S para o volume de destino é suspensa durante qualquer tipo de operação de volume de cópia. Esta suspensão ocorre porque o estado dos dados no volume alvo é inconsistente até que o procedimento esteja concluído.

As operações de volume de cópia offline e online são descritas abaixo.

#### Operação de volume de cópia offline

A relação volume de cópia offline está entre um volume de origem e um volume de destino. Uma cópia off-line lê os dados do volume de origem e os copia para um volume de destino, enquanto suspende todas as atualizações para o volume de origem com a cópia em andamento. Todas as atualizações do volume de origem são suspensas para evitar que inconsistências cronológicas sejam criadas no volume de destino.

| **O que você precisa saber sobre operações de cópia offline** | |
|---|---|
| Solicitações de leitura e gravação | • Os volumes de origem que estão participando de uma cópia offline estão disponíveis para atividade de e/S somente leitura enquanto uma operação volume de cópia tem um status de em andamento ou pendente.<br>• As solicitações de gravação são permitidas após a conclusão da cópia offline.<br>• Para evitar mensagens de erro protegidas por gravação, não acesse um volume de origem que esteja participando de uma operação de volume de cópia com um status de em andamento. |
| Sistema de arquivos journaling | • Se o volume de origem tiver sido formatado com um sistema de arquivos journaling, qualquer tentativa de emitir uma solicitação de leitura para o volume de origem pode ser rejeitada pelos controladores do storage array e uma mensagem de erro pode aparecer.<br>• O driver do sistema de arquivos journaling emite uma solicitação de gravação antes de tentar emitir a solicitação de leitura. O controlador rejeita a solicitação de gravação e a solicitação de leitura pode não ser emitida devido à solicitação de gravação rejeitada. Essa condição pode resultar na exibição de uma mensagem de erro, que indica que o volume de origem está protegido contra gravação.<br>• Para evitar que esse problema ocorra, não tente acessar um volume de origem que esteja participando de uma cópia off-line enquanto a operação volume de cópia tiver um status de em andamento. |

#### Operação de volume de cópia online

A relação de volume de cópia on-line é entre um volume instantâneo e um volume de destino. Você pode iniciar uma operação volume de cópia enquanto o volume de origem estiver on-line e disponível para gravações de dados. Esta função é obtida criando um instantâneo do volume e usando o instantâneo como o

volume de origem real para a cópia.

Quando você inicia uma operação volume de cópia para um volume de origem, o System Manager cria uma imagem instantânea do volume base e uma relação de cópia entre a imagem instantânea do volume base e um volume de destino. Usar a imagem instantânea como o volume de origem permite que a matriz de armazenamento continue a gravar no volume de origem enquanto a cópia está em andamento.

Durante uma operação de cópia online, ocorre um impactos no desempenho devido ao procedimento copy-on-write. Após a conclusão da cópia on-line, o desempenho do volume base é restaurado.

| **O que você precisa saber sobre operações de cópia online** | |
|---|---|
| Que tipo de volumes podem ser usados? | • O volume para o qual a imagem pontual é criada é conhecido como volume base e deve ser um volume padrão ou um volume fino na matriz de armazenamento.<br>• Um volume de destino pode ser um volume padrão em um grupo de volumes ou um volume padrão em um pool. Um volume de destino não pode ser um volume fino ou um volume base num grupo de instantâneos.<br>• Você pode usar a função volume de cópia on-line para copiar dados de um volume fino para um volume padrão em um pool que reside no mesmo storage array. Mas você não pode usar a função volume de cópia para copiar dados de um volume padrão para um volume fino. |
| Performance de volume base | • Se o volume instantâneo usado como fonte de cópia estiver ativo, o desempenho do volume base será degradado devido a operações de cópia na gravação. Quando a cópia estiver concluída, o instantâneo é desativado e o desempenho do volume base é restaurado. Embora o snapshot esteja desativado, o volume de capacidade reservada e a relação de cópia permanecem intactos. |
| Tipos de volumes criados | • Um volume snapshot e um volume de capacidade reservada são criados durante a operação de cópia on-line.<br>• O volume instantâneo não é um volume real que contém dados; em vez disso, é uma referência aos dados contidos em um volume em um momento específico.<br>• Para cada snapshot que é capturado, um volume de capacidade reservada é criado para armazenar os dados do snapshot. O volume de capacidade reservada é utilizado apenas para gerir a imagem instantânea. |
| Volume de capacidade reservada | • Antes que um bloco de dados no volume de origem seja modificado, o conteúdo do bloco a ser modificado é copiado para o volume de capacidade reservada para a conservação.<br>• Como o volume de capacidade reservada armazena cópias dos dados originais nesses blocos de dados, outras alterações nesses blocos de dados gravam apenas no volume de origem.<br>• A operação de cópia on-line usa menos espaço em disco do que uma cópia física completa porque os únicos blocos de dados armazenados no volume de capacidade reservada são aqueles que foram alterados desde o momento do snapshot. |

## Volume de cópia

Você pode copiar dados de um volume para outro volume no mesmo storage array e criar uma duplicata (clone) física de um volume de origem.

### Antes de começar

- Todas as atividades de e/S para o volume de origem e o volume de destino devem ser interrompidas.
- Todos os sistemas de arquivos no volume de origem e no volume de destino devem ser desmontados.
- Se você já usou o volume de destino em uma operação de volume de cópia antes, não precisará mais desses dados ou que fez backup dos dados.

### Sobre esta tarefa

O volume de origem é o volume que aceita e/S de host e armazena dados de aplicativos. Quando um volume de cópia é iniciado, os dados do volume de origem são copiados na sua totalidade para o volume de destino.

O volume de destino é um volume padrão que mantém uma cópia dos dados do volume de origem. O volume de destino é idêntico ao volume de origem após a conclusão da operação volume de cópia. O volume de destino deve ter a mesma capacidade ou maior que o volume de origem; no entanto, ele pode ter um nível RAID diferente.

### Mais sobre cópias online e offline

#### Cópia online

Uma cópia on-line cria uma cópia pontual de qualquer volume dentro de um storage array, enquanto ainda é possível gravar no volume com a cópia em andamento. Esta função é obtida criando um instantâneo do volume e usando o instantâneo como o volume de origem real para a cópia. O volume para o qual a imagem pontual é criada é conhecido como volume base e pode ser um volume padrão ou um volume fino na matriz de armazenamento.

- Cópia off-line*

Uma cópia off-line lê os dados do volume de origem e os copia para um volume de destino, enquanto suspende todas as atualizações para o volume de origem com a cópia em andamento. Todas as atualizações do volume de origem são suspensas para evitar que inconsistências cronológicas sejam criadas no volume de destino. A relação de cópia de volume off-line está entre um volume de origem e um volume de destino.

Uma operação de volume de cópia substitui os dados no volume de destino e falha em todos os volumes de snapshot associados ao volume de destino, se houver algum.

### Passos

1. Selecione **armazenamento › volumes**.
2. Selecione o volume que pretende utilizar como origem para a operação volume de cópia e, em seguida, selecione **Serviços de cópia › volume de cópia**.

   A caixa de diálogo Copiar volume-Selecionar destino é exibida.

3. Selecione o volume de destino para o qual deseja copiar os dados.

   A tabela mostrada nesta caixa de diálogo lista todos os volumes de destino elegíveis.

4. Use a barra deslizante para definir a prioridade de cópia para a operação volume de cópia.

   A prioridade de cópia determina quanto dos recursos do sistema são usados para concluir a operação volume de cópia em comparação com as solicitações de e/S de serviço.

   **Mais sobre as taxas de prioridade de cópia**

   Existem cinco taxas de prioridade de cópia:

   - Mais baixo
   - Baixo
   - Média
   - Alta
   - Mais alto

   Se a prioridade de cópia estiver definida para a taxa mais baixa, a atividade de e/S será priorizada e a operação volume de cópia demorará mais tempo. Se a prioridade de cópia estiver definida para a taxa mais alta, a operação volume de cópia será priorizada, mas a atividade de e/S para o storage array pode ser afetada.

5. Selecione se pretende criar uma cópia online ou uma cópia offline. Para criar uma cópia on-line, marque a caixa de seleção **manter o volume de origem on-line durante a operação de cópia**.
6. Execute um dos seguintes procedimentos:
   - Para executar uma operação de cópia *online*, clique em **Next** para continuar para a caixa de diálogo **Reserve Capacity**.
   - Para executar uma operação de cópia *offline*, clique em **Finish** para iniciar a cópia offline.
7. Se você optar por criar uma cópia on-line, defina a capacidade reservada necessária para armazenar dados e outras informações para a cópia on-line e clique em **concluir** para iniciar a cópia on-line.

   A tabela de candidatos ao volume exibe apenas os candidatos que suportam a capacidade reservada especificada. A capacidade reservada é a capacidade alocada física usada para qualquer operação de serviço de cópia e objeto de storage. Não é diretamente legível pelo host.

   Alocar a capacidade reservada usando as seguintes diretrizes:

   - A configuração padrão para capacidade reservada é de 40% da capacidade do volume base e, geralmente, essa capacidade é suficiente.
   - A capacidade reservada, no entanto, varia dependendo do número de alterações nos dados originais. Quanto mais tempo um objeto de storage estiver ativo, maior a capacidade reservada.

**Resultados**

O System Manager copia todos os dados do volume de origem para o volume de destino. Após a conclusão da operação volume de cópia, o volume de destino torna-se automaticamente somente leitura para os hosts.

**Depois de terminar**

Selecione **Home › View Operations in Progress** (Ver operações em curso) para ver o progresso da operação Copy volume (volume de cópia). Esta operação pode ser demorada e pode afetar o desempenho do sistema.

### Tome medidas numa operação de volume de cópia

É possível exibir uma operação de volume de cópia em andamento e parar, alterar prioridade, recopiar ou limpar uma operação de volume de cópia.

#### Passos

1. Selecione **Home › View Operations in Progress** (Ver operações em curso).

   A caixa de diálogo operações em andamento é exibida.

2. Localize a operação volume de cópia na qual você deseja executar a ação e clique no link na coluna **ações** para executar uma das seguintes ações.

   Leia todo o texto cautelar fornecido nos diálogos, particularmente ao parar uma operação.

| Ação | Descrição |
|---|---|
| Parar | Você pode parar uma operação de volume de cópia enquanto a operação tiver um status de em andamento, pendente ou Falha.<br><br>Quando o volume de cópia é interrompido, todos os hosts mapeados têm acesso de gravação ao volume de origem. Se os dados forem gravados no volume de origem, os dados no volume de destino não correspondem mais aos dados no volume de origem. |
| Alterar prioridade | Você pode alterar a prioridade de uma operação volume de cópia enquanto a operação tiver um status de em andamento para selecionar a taxa na qual uma operação volume de cópia é concluída. |
| Volte a copiar | Pode voltar a copiar um volume quando tiver parado uma operação de volume de cópia e pretender iniciá-lo novamente ou quando uma operação de volume de cópia tiver falhado ou interrompido. A operação volume de cópia começa a partir do início.<br><br>A ação de recópia substitui os dados existentes no volume de destino e falha em todos os volumes snapshot associados ao volume de destino, se houver algum. |
| Limpar | Você pode remover a operação volume de cópia enquanto a operação tiver um status de em andamento, pendente ou Falha.<br><br>Certifique-se de que pretende efetuar esta operação antes de selecionar **Clear**. Não há diálogo de confirmação. |

## FAQs

### O que é um volume?

Um volume é um contêiner no qual aplicativos, bancos de dados e sistemas de arquivos armazenam dados. É o componente lógico criado para que o host acesse o storage no

storage array.

Um volume é criado a partir da capacidade disponível em um pool ou em um grupo de volumes. Um volume tem uma capacidade definida. Embora um volume possa consistir em mais de uma unidade, um volume aparece como um componente lógico para o host.

**Por que estou vendo um erro de superalocação de capacidade quando tenho capacidade livre suficiente em um grupo de volumes para criar volumes?**

O grupo de volume selecionado pode ter uma ou mais áreas de capacidade livre. Uma área de capacidade livre é a capacidade livre que pode resultar da exclusão de um volume ou da não utilização de toda a capacidade livre disponível durante a criação do volume.

Quando você cria um volume em um grupo de volumes que tenha uma ou mais áreas de capacidade livre, a capacidade do volume é limitada à maior área de capacidade livre nesse grupo de volumes. Por exemplo, se um grupo de volume tiver um total de 15 GiB de capacidade livre, e a maior área de capacidade livre for de 10 GiB, o maior volume que você pode criar é de 10 GiB.

Se um grupo de volume tiver áreas de capacidade livre, o gráfico de grupo de volume contém um link indicando o número de áreas de capacidade livre existentes. Selecione o link para exibir um pop-over que indica a capacidade de cada área.

Ao consolidar a capacidade gratuita, você pode criar volumes adicionais a partir da quantidade máxima de capacidade livre em um grupo de volumes. Você pode consolidar a capacidade livre existente em um grupo de volumes selecionado usando um dos seguintes métodos:

- Quando é detetada pelo menos uma área de capacidade livre para um grupo de volumes, a recomendação "consolidar capacidade livre" aparece na página inicial na área de notificação. Clique no link **consolidar capacidade livre** para iniciar a caixa de diálogo.
- Você também pode selecionar **pools e grupos de volume › tarefas incomuns › consolidar capacidade livre do grupo de volume** para iniciar a caixa de diálogo.

Se você quiser usar uma área de capacidade livre específica em vez da maior área de capacidade livre, use a interface de linha de comando (CLI).

**Como minha carga de trabalho selecionada afeta a criação de volume?**

Durante a criação de volume, você será solicitado a fornecer informações sobre o uso de uma carga de trabalho. O sistema usa essas informações para criar uma configuração de volume ideal para você, que pode ser editada conforme necessário. Opcionalmente, você pode pular esta etapa na sequência de criação de volume.

Um workload é um objeto de storage compatível com uma aplicação. Você pode definir uma ou mais cargas de trabalho ou instâncias por aplicação. Para alguns aplicativos, o sistema configura a carga de trabalho para conter volumes com caraterísticas de volume subjacentes semelhantes. Essas características de volume são otimizadas com base no tipo de aplicação compatível com o workload. Por exemplo, se você criar uma carga de trabalho que suporte um aplicativo Microsoft SQL Server e, posteriormente, criar volumes para essa carga de trabalho, as caraterísticas de volume subjacentes serão otimizadas para oferecer suporte ao Microsoft SQL Server.

- **Específico do aplicativo** — quando você está criando volumes usando uma carga de trabalho específica do aplicativo, o sistema pode recomendar uma configuração de volume otimizada para minimizar a

contenção entre e/S da carga de trabalho do aplicativo e outro tráfego da instância do aplicativo. As características de volume, como tipo de e/S, tamanho do segmento, propriedade da controladora e cache de leitura e gravação, são automaticamente recomendadas e otimizadas para cargas de trabalho criadas para os seguintes tipos de aplicativos.

  - Microsoft SQL Server
  - Microsoft Exchange Server
  - Aplicações de videovigilância
  - VMware ESXi (para volumes a serem usados com o Virtual Machine File System)

    Você pode revisar a configuração de volume recomendada e editar, adicionar ou excluir os volumes e caraterísticas recomendados pelo sistema usando a caixa de diálogo Adicionar/Editar volumes.

- **Outros** (ou aplicativos sem suporte específico para criação de volume) — outras cargas de trabalho usam uma configuração de volume que você deve especificar manualmente quando deseja criar uma carga de trabalho que não esteja associada a um aplicativo específico ou se não houver otimização integrada para o aplicativo que você pretende usar no storage array. Você deve especificar manualmente a configuração do volume usando a caixa de diálogo Adicionar/Editar volumes.

**Por que esses volumes não estão associados a uma carga de trabalho?**

Os volumes não são associados a uma carga de trabalho se tiverem sido criados usando a interface de linha de comando (CLI) ou se tiverem sido migrados (importados/exportados) de um storage array diferente.

**Por que não consigo excluir a carga de trabalho selecionada?**

Essa carga de trabalho consiste em um grupo de volumes que foram criados usando a interface de linha de comando (CLI) ou migrados (importados/exportados) de um storage array diferente. Como resultado, os volumes dessa carga de trabalho não são associados a uma carga de trabalho específica da aplicação, portanto, a carga de trabalho não pode ser excluída.

**Como os workloads específicos da aplicação me ajudam a gerenciar meu storage array?**

As características de volume do workload específico do aplicativo determinam como a carga de trabalho interage com os componentes do storage array e ajudam a determinar a performance do ambiente em uma determinada configuração.

Um aplicativo é um software como o SQL Server ou o Exchange. Você define um ou mais workloads para dar suporte a cada aplicação.

**Como o fornecimento dessas informações ajuda a criar armazenamento?**

As informações da carga de trabalho são usadas para otimizar as caraterísticas do volume, como tipo de e/S, tamanho do segmento e cache de leitura/gravação para a carga de trabalho selecionada. Essas características otimizadas determinam como sua carga de trabalho interage com os componentes do storage array.

Com base nas informações de carga de trabalho fornecidas, o System Manager cria os volumes apropriados e

os coloca nos pools ou grupos de volumes disponíveis atualmente no sistema. O sistema cria os volumes e otimiza suas características com base nas práticas recomendadas atuais para o workload selecionado.

Antes de concluir a criação de volumes para uma determinada carga de trabalho, você pode revisar a configuração de volume recomendada e editar, adicionar ou excluir os volumes e as caraterísticas recomendadas pelo sistema usando a caixa de diálogo Adicionar/Editar volumes.

Consulte a documentação específica da aplicação para obter informações sobre as melhores práticas.

**O que eu preciso fazer para reconhecer a capacidade expandida?**

## Se você aumentar a capacidade de um volume, o host pode não reconhecer imediatamente o aumento da capacidade do volume.

A maioria dos sistemas operacionais reconhece a capacidade de volume expandida e se expande automaticamente após a expansão de volume ser iniciada. No entanto, alguns podem não. Se o sistema operacional não reconhecer automaticamente a capacidade de volume expandido, talvez seja necessário realizar uma nova digitalização ou reinicialização do disco.

Depois de expandir a capacidade do volume, você deve aumentar manualmente o tamanho do sistema de arquivos para corresponder. A forma como você faz isso depende do sistema de arquivos que você está usando.

Consulte a documentação do sistema operacional do host para obter detalhes adicionais.

**Por que não vejo todos os meus pools e/ou grupos de volume?**

## Qualquer pool ou grupo de volume para o qual você não pode mover o volume não é exibido na lista.

Pools ou grupos de volumes não são elegíveis por nenhum dos seguintes motivos:

- Os recursos de garantia de dados (DA) de um pool ou grupo de volumes não correspondem.
- Um pool ou grupo de volume está em um estado não ideal.
- A capacidade de um pool ou grupo de volume é muito pequena.

**O que é o tamanho do segmento?**

## Um segmento é a quantidade de dados em kilobytes (KiB) que é armazenada em uma unidade antes que a matriz de armazenamento se mova para a próxima unidade na faixa (grupo RAID). O tamanho do segmento aplica-se apenas a grupos de volume, não a pools.

O tamanho do segmento é definido pelo número de blocos de dados que contém. Ao determinar o tamanho do segmento, você deve saber que tipo de dados você armazenará em um volume. Se um aplicativo normalmente usa pequenas leituras e gravações aleatórias (IOPS), um tamanho de segmento menor normalmente funciona melhor. Como alternativa, se o aplicativo tiver leituras e gravações sequenciais grandes (throughput), um tamanho de segmento grande geralmente é melhor.

Se um aplicativo usa pequenas leituras e gravações aleatórias ou grandes leituras e gravações sequenciais, o storage array tem melhor desempenho se o tamanho do segmento for maior do que o tamanho típico de bloco de dados. Isso normalmente torna mais fácil e rápido para as unidades acessarem os dados, o que é

importante para um melhor desempenho do storage array.

#### Ambientes em que a performance do IOPS é importante

Em um ambiente de operações de e/S por segundo (IOPS), o storage array tem melhor desempenho se você usar um tamanho de segmento maior do que o tamanho típico do bloco de dados (" chunk'") que é lido/escrito em uma unidade. Isso garante que cada bloco seja escrito em uma única unidade.

#### Ambientes onde a taxa de transferência é importante

Em um ambiente de taxa de transferência, o tamanho do segmento deve ser uma fração uniforme do total de unidades de dados e o tamanho típico de bloco de dados (tamanho de e/S). Isso espalha os dados como um único stripe entre as unidades do grupo de volumes, levando a leituras e gravações mais rápidas.

### O que é a propriedade preferida do controlador?

A propriedade preferencial do controlador define o controlador designado para ser o controlador proprietário ou principal do volume.

A propriedade do controlador é muito importante e deve ser planejada cuidadosamente. Os controladores devem ser balanceados o mais próximo possível para e/S totais.

Por exemplo, se um controlador lê principalmente blocos de dados grandes e sequenciais e o outro controlador tiver blocos de dados pequenos com leituras e gravações frequentes, as cargas são muito diferentes. Saber quais volumes contêm que tipo de dados permite equilibrar as transferências de e/S igualmente em ambas as controladoras.

### Quando eu gostaria de usar a seleção atribuir host mais tarde?

Se você quiser acelerar o processo de criação de volumes, você pode pular a etapa de atribuição do host para que os volumes recém-criados sejam inicializados offline.

Os volumes recém-criados devem ser inicializados. O sistema pode iniciá-los usando um de dois modos — um processo de inicialização em segundo plano formato disponível imediato (IAF) ou um processo offline.

Quando você mapeia um volume para um host, ele força qualquer volume inicializando nesse grupo a transição para a inicialização em segundo plano. Esse processo de inicialização em segundo plano permite e/S de host concorrente, que às vezes pode ser demorado.

Quando nenhum dos volumes de um grupo de volumes é mapeado, a inicialização offline é realizada. O processo off-line é muito mais rápido do que o processo em segundo plano.

### O que eu preciso saber sobre os requisitos de tamanho de bloco de host?

Para sistemas EF300 e EF600, um volume pode ser definido para suportar um tamanho de bloco de 512 bytes ou 4KiB (também chamado de "tamanho do setor"). Você deve definir o valor correto durante a criação do volume. Se possível, o sistema sugere o valor padrão apropriado.

Antes de definir o tamanho do bloco de volume, leia as seguintes limitações e diretrizes.

- Alguns sistemas operacionais e máquinas virtuais (especialmente VMware, neste momento) exigem um tamanho de bloco de 512 bytes e não suportam 4KiB, portanto, certifique-se de conhecer os requisitos do

host antes de criar um volume. Normalmente, você pode obter o melhor desempenho definindo um volume para apresentar um tamanho de bloco de 4KiB KB; no entanto, certifique-se de que seu host permita blocos de 4KiB KB (ou 4Kn KB).

- O tipo de unidades que você selecionar para o seu pool ou grupo de volumes também determina quais tamanhos de bloco de volume são suportados, da seguinte forma:
  - Se você criar um grupo de volumes usando unidades que gravam em blocos de 512 bytes, então você só poderá criar volumes com blocos de 512 bytes.
  - Se você criar um grupo de volumes usando unidades que gravam em blocos 4KiB, poderá criar volumes com blocos 512 ou 4KiB.
- Se o array tiver uma placa de interface de host iSCSI, todos os volumes estarão limitados a blocos de 512 bytes (independentemente do tamanho do bloco do grupo de volumes). Isso se deve a uma implementação de hardware específica.
- Não é possível alterar um tamanho de bloco depois de definido. Se você precisar alterar um tamanho de bloco, exclua o volume e recriá-lo.

# Hosts e clusters de host

## Visão geral dos clusters de hosts e host

Você pode configurar hosts e clusters de host, que definem as conexões entre o storage array e os servidores de dados.

### O que são hosts e clusters de host?

Um *host* é um servidor que envia e/S para um volume em um storage array. Um cluster *host* é um grupo de hosts, que você pode criar para atribuir os mesmos volumes a vários hosts.

Saiba mais:

- "Terminologia do host"
- "Volumes de acesso"
- "Número máximo de LUNs"

### Como configuro hosts e clusters de host?

Para definir conexões de host, você pode ir para **armazenamento › hosts** para configurar manualmente o host. Se quiser que dois ou mais hosts compartilhem o acesso ao mesmo conjunto de volumes, você poderá definir um cluster e atribuir os volumes a esse cluster.

Saiba mais:

- "Criação manual do host"
- "Como os volumes são atribuídos a hosts e clusters de host"
- "Fluxo de trabalho para criação de host e atribuição de volume"
- "Criar host manualmente"
- "Criar cluster de host"
- "Atribuir volumes aos hosts"

### Informações relacionadas

Saiba mais sobre as tarefas relacionadas aos hosts:

- "Definir o balanceamento de carga automático"
- "Definir relatórios de conetividade de host"
- "Altere o tipo de host padrão"

## Conceitos

### Terminologia do host

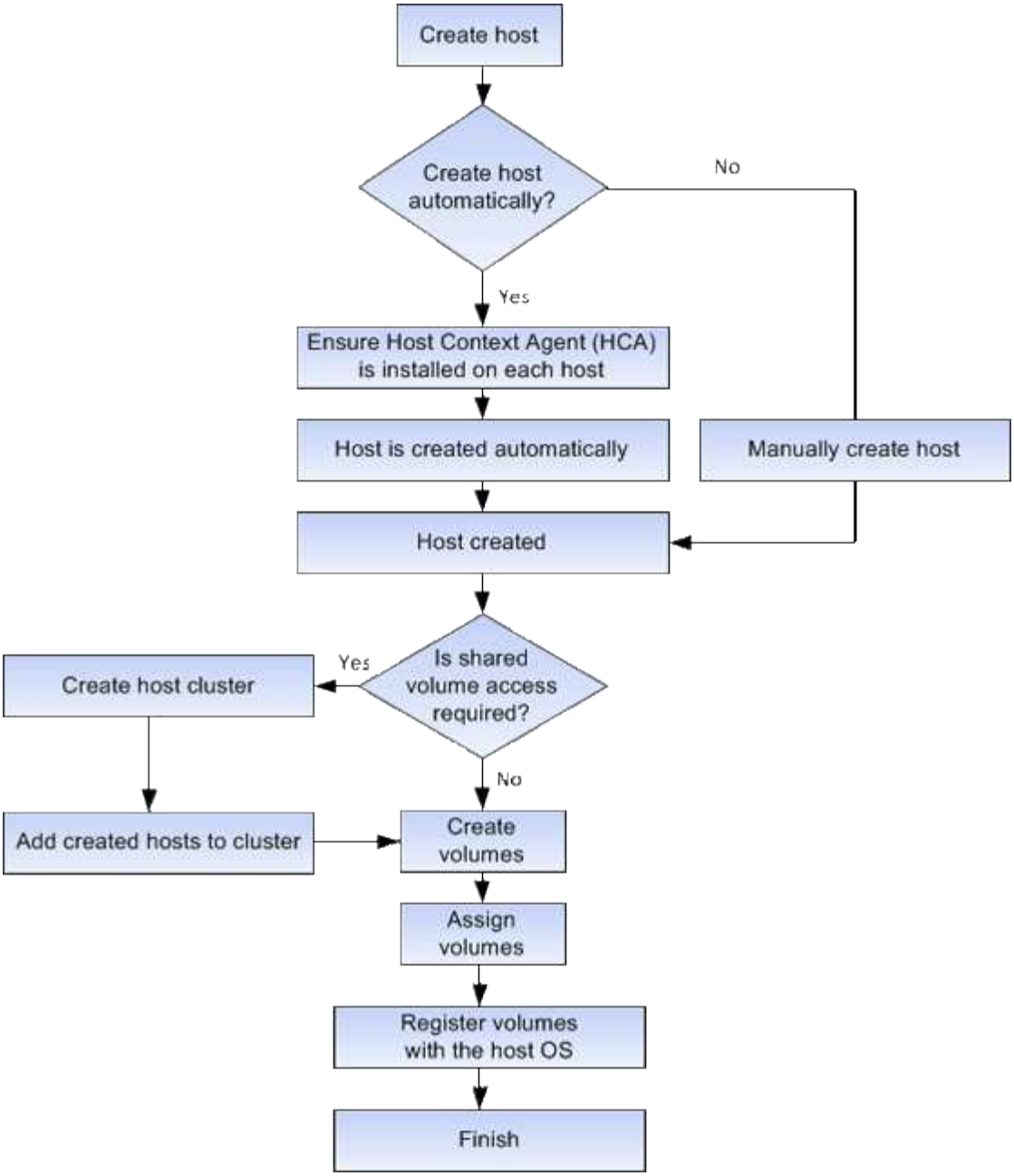
Saiba como os termos do host se aplicam ao storage array.

| Componente | Definição |
|---|---|
| Host | Um host é um servidor que envia e/S para um volume em um storage array. |
| Nome do host | O nome do host deve ser igual ao nome do sistema do host. |
| Cluster de host | Um cluster de host é um grupo de hosts. Você cria um cluster de host para facilitar a atribuição dos mesmos volumes a vários hosts. |
| Protocolo de interface de host | Um protocolo de interface de host é a conexão (como Fibre Channel, iSCSI, etc.) entre os controladores e os hosts. |
| HBA ou placa de interface de rede (NIC) | Um adaptador de barramento de host (HBA) é uma placa que reside em um host e contém uma ou mais portas de host. |
| Porta de host | Uma porta de host é uma porta em um adaptador de barramento de host (HBA) que fornece a conexão física a um controlador e é usada para operações de e/S. |
| Identificador da porta do host | Um identificador de porta de host é um nome único em todo o mundo associado a cada porta de host em um adaptador de barramento de host (HBA).<br>• Os identificadores de porta de host iSCSI (Internet Small Computer System Interface) devem ter entre 1 e 233 carateres. Os identificadores de porta de host iSCSI são exibidos no formato IQN padrão (por exemplo, `iqn.xxx.com.xxx:8b3ad` ).<br>• Os identificadores de porta de host não iSCSI, como Fibre Channel e Serial Attached SCSI (SAS), são exibidos como delimitados por dois pontos após cada dois carateres (por exemplo, `xx:yy:zz` ). Os identificadores de porta de host Fibre Channel devem ter 16 carateres. |
| Tipo de sistema operacional de host | O tipo de sistema operacional do host é uma configuração que define como os controladores no storage array reagem à e/S dependendo do sistema operacional (ou variante) do host. Isso também é chamado às vezes *host type* para breve. |

| Componente | Definição |
| --- | --- |
| Porta de host do controlador | Uma porta de host do controlador é uma porta no controlador que fornece a conexão física a um host e é usada para operações de e/S. |
| LUN | Um número de unidade lógica (LUN) é o número atribuído ao espaço de endereço que um host usa para acessar um volume. O volume é apresentado ao host como capacidade na forma de um LUN.<br><br>Cada host tem seu próprio espaço de endereço LUN. Portanto, o mesmo LUN pode ser usado por diferentes hosts para acessar diferentes volumes. |

#### Fluxo de trabalho para criação de host e atribuição de volume

A figura a seguir ilustra como configurar o acesso ao host.




**Criação manual do host**

A criação de um host é uma das etapas necessárias para que o storage array saiba quais hosts estão conetados a ele e para permitir o acesso de e/S aos volumes. Você só pode criar um host manualmente.

#### Criação manual

A criação manual de host permite que você verifique se os identificadores de porta de host detetados pelos controladores de storage array estão associados corretamente aos hosts.

Durante a criação manual do host, você associa identificadores de porta do host selecionando-os em uma lista ou inserindo-os manualmente. Depois de criar um host, você poderá atribuir volumes a ele ou adicioná-lo a um cluster de host se desejar compartilhar o acesso a volumes.

### Como os volumes são atribuídos a hosts e clusters de host

Para que um host ou cluster de host envie e/S para um volume, você deve atribuir o volume ao host ou cluster de host.

Você pode selecionar um host ou cluster de host ao criar um volume ou atribuir um volume a um host ou cluster de host posteriormente. Um cluster de host é um grupo de hosts. Você cria um cluster de host para facilitar a atribuição dos mesmos volumes a vários hosts.

Atribuir volumes a hosts é flexível, permitindo que você atenda às suas necessidades de armazenamento específicas.

- * Host autônomo, não parte de um cluster de host* — você pode atribuir um volume a um host individual. O volume só pode ser acessado por um host.
- **Host cluster** — você pode atribuir um volume a um cluster de host. O volume pode ser acessado por todos os hosts no cluster de host.
- **Host dentro de um cluster de host** — você pode atribuir um volume a um host individual que faz parte de um cluster de host. Mesmo que o host faça parte de um cluster de host, o volume pode ser acessado apenas pelo host individual e não por nenhum outro host no cluster de host.

Quando os volumes são criados, os números de unidade lógica (LUNs) são atribuídos automaticamente. O LUN serve como o "endereço" entre o host e o controlador durante as operações de e/S. Você pode alterar LUNs depois que o volume é criado.

### Volumes de acesso

Um volume de acesso é um volume configurado de fábrica no storage array que é usado para comunicação com o storage array e o host por meio da conexão de e/S do host. O volume de acesso requer um LUN (Logical Unit Number).

O volume de acesso é usado na seguinte instância:

- **Gerenciamento na banda** — o volume de acesso é usado para uma conexão na banda para gerenciar o storage array. Isso só pode ser feito se você estiver gerenciando o storage array com a interface de linha de comando (CLI).

> O gerenciamento na banda não está disponível para sistemas de storage EF600 ou EF300.

Um volume de acesso é criado automaticamente na primeira vez que você atribui um volume a um host. Por exemplo, se você atribuir volume_1 e volume_2 a um host, ao visualizar os resultados dessa atribuição, verá três volumes (volume_1, volume_2 e Access).

Se você não estiver criando automaticamente hosts ou gerenciando um storage array na banda com a CLI, não precisará do volume de acesso e poderá liberar o LUN excluindo o volume de acesso. Essa ação remove a atribuição de volume para LUN, bem como quaisquer conexões de gerenciamento na banda para o host.

### Número máximo de LUNs

O storage array tem um número máximo de LUNs que podem ser usados para cada host.

O número máximo depende do sistema operacional do host. A matriz de armazenamento rastreia o número

de LUNs usados. Se você tentar atribuir um volume a um host que exceda o número máximo de LUNs, o host não poderá acessar o volume.

#### Tipo de sistema operacional de host padrão

O tipo de host padrão é usado pelo storage array quando os hosts são conetados inicialmente. Ele define como os controladores no storage array funcionam com o sistema operacional do host quando os volumes são acessados.

Você pode alterar o tipo de host se houver a necessidade de alterar o modo como o storage array opera, em relação aos hosts que estão conetados a ele. Geralmente, você alterará o tipo de host padrão antes de conetar os hosts ao storage array ou quando conetar hosts adicionais.

Tenha em mente estas diretrizes:

- Se todos os hosts que você planeja se conetar ao storage de armazenamento tiverem o mesmo sistema operacional (ambiente de host homogêneo), altere o tipo de host para corresponder ao sistema operacional.
- Se houver hosts com sistemas operacionais diferentes que você planeja se conetar ao storage array (ambiente de host heterogêneo), altere o tipo de host para corresponder à maioria dos sistemas operacionais dos hosts.

  Por exemplo, se você estiver conetando oito hosts diferentes ao storage array e seis desses hosts estiverem executando um sistema operacional Windows, você deverá selecionar o Windows como o tipo de sistema operacional de host padrão.

- Se a maioria dos hosts conetados tiver uma combinação de diferentes sistemas operacionais, altere o tipo de host para padrão de fábrica.

  Por exemplo, se você estiver conetando oito hosts diferentes ao storage array e dois desses hosts estiverem executando um sistema operacional Windows, três estiverem executando um sistema operacional VMware e outros três estiverem executando um sistema operacional Linux, você deverá selecionar padrão de fábrica como o tipo de sistema operacional padrão de host.

## Configurar o acesso ao host

#### Criar host manualmente

Para hosts que não podem ser descobertos automaticamente, você pode criar manualmente um host. A criação de um host é uma das etapas necessárias para que o storage array saiba quais hosts estão conetados a ele e para permitir o acesso de e/S aos volumes.

#### Sobre esta tarefa

Mantenha estas diretrizes em mente quando você cria um host:

- Você deve definir as portas de identificador de host que estão associadas ao host.
- Certifique-se de fornecer o mesmo nome que o nome do sistema atribuído pelo host.
- Esta operação não é bem-sucedida se o nome que você escolher já estiver em uso.

- O comprimento do nome não pode exceder 30 carateres.

**Passos**

1. Selecione **armazenamento › hosts**.
2. Clique em **criar › Host**.

   A caixa de diálogo criar host é exibida.

3. Selecione as configurações para o host, conforme apropriado.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| Nome | Digite um nome para o novo host. |
| Tipo de sistema operacional de host | Selecione o sistema operacional que está sendo executado no novo host na lista suspensa. |
| Tipo de interface de host | (Opcional) se você tiver mais de um tipo de interface de host compatível com seu storage array, selecione o tipo de interface de host que deseja usar. |
| Portas de host | Execute um dos seguintes procedimentos:<br>• **Selecione Interface I/o**<br>Geralmente, as portas do host devem ter feito login e estar disponíveis na lista suspensa. Você pode selecionar os identificadores de porta do host na lista.<br>• **Manual add**<br>Se um identificador de porta do host não for exibido na lista, isso significa que a porta do host não foi conetada. Um utilitário HBA ou o utilitário iniciador iSCSI podem ser usados para localizar os identificadores de porta do host e associá-los ao host.<br>Você pode inserir manualmente os identificadores de porta do host ou copiá-los/colá-los do utilitário (um de cada vez) no campo **Host Ports**.<br>Você deve selecionar um identificador de porta de host de cada vez para associá-lo ao host, mas pode continuar a selecionar quantos identificadores estão associados ao host. Cada identificador é exibido no campo **Host Ports**. Se necessário, você também pode remover um identificador selecionando **X** ao lado dele. |

| Definição | Descrição |
| --- | --- |
| Iniciador CHAP | (Opcional) se você selecionou ou inseriu manualmente uma porta de host com um IQN iSCSI e se quiser exigir que um host que tente acessar a matriz de armazenamento para se autenticar usando o Challenge Handshake Authentication Protocol (CHAP), marque a caixa de seleção **iniciador CHAP**. Para cada porta de host iSCSI selecionada ou inserida manualmente, faça o seguinte:<br>• Insira o mesmo segredo CHAP que foi definido em cada iniciador de host iSCSI para autenticação CHAP. Se você estiver usando autenticação CHAP mútua (autenticação bidirecional que permite que um host se valide para o storage array e para que um storage array se valide para o host), você também deve definir o segredo CHAP para o storage array na configuração inicial ou alterando as configurações.<br>• Deixe o campo em branco se você não precisar de autenticação de host.<br>Atualmente, o único método de autenticação iSCSI usado pelo System Manager é CHAP. |

4. Clique em **criar**.

**Resultados**

Depois que o host é criado com êxito, o sistema cria um nome padrão para cada porta de host configurada para o host (rótulo do usuário).

O alias predefinido é`Hostname_Port Number` >. Por exemplo, o alias padrão para a primeira porta criada para `host IPT is IPT_1`.

### Criar cluster de host

Você cria um cluster de host quando dois ou mais hosts exigem acesso de e/S aos mesmos volumes.

**Sobre esta tarefa**

Tenha essas diretrizes em mente ao criar um cluster de host:

- Esta operação não é iniciada a menos que haja dois ou mais hosts disponíveis para criar o cluster.
- Os hosts em clusters de host podem ter sistemas operacionais diferentes (heterogêneos).
- Os hosts NVMe nos clusters de host não podem ser misturados a hosts não NVMe.
- Para criar um volume habilitado para Data Assurance (DA), a conexão de host que você está planejando usar deve suportar DA.

  Se qualquer uma das conexões de host nos controladores do storage array não suportar DA, os hosts associados não poderão acessar dados em volumes habilitados PARA DA.

- Esta operação não é bem-sucedida se o nome que você escolher já estiver em uso.
- O comprimento do nome não pode exceder 30 carateres.

**Passos**

1. Selecione **armazenamento › hosts**.
2. Selecione **criar › Host Cluster**.

   A caixa de diálogo criar cluster de host é exibida.

3. Selecione as configurações do cluster de host, conforme apropriado.

   **Detalhes do campo**

| Definição | Descrição |
|---|---|
| Nome | Digite o nome do novo cluster de host. |
| Selecione hosts para compartilhar o acesso ao volume | Selecione dois ou mais hosts na lista suspensa. Apenas os hosts que ainda não fazem parte de um cluster de host aparecem na lista. |

4. Clique em **criar**.

   Se os hosts selecionados estiverem conetados a tipos de interface que tenham diferentes recursos de Data Assurance (DA), uma caixa de diálogo será exibida com a mensagem de que DA estará indisponível no cluster de host. Essa indisponibilidade impede que volumes habilitados PARA DA sejam adicionados ao cluster de host. Selecione **Sim** para continuar ou **não** para cancelar.

   DA aumenta a integridade dos dados em todo o sistema de storage. O DA permite que o storage array verifique se há erros que possam ocorrer quando os dados são movidos entre os hosts e as unidades. O uso DA para o novo volume garante que quaisquer erros sejam detetados.

**Resultados**

O novo cluster de host aparece na tabela com os hosts atribuídos nas linhas abaixo.

### Atribuir volumes aos hosts

É necessário atribuir um volume a um host ou a um cluster de host para que ele possa ser usado para operações de e/S. Essa atribuição concede a um host ou cluster de host acesso a um ou mais volumes em um storage array.

**Sobre esta tarefa**

Tenha estas diretrizes em mente quando atribuir volumes a hosts:

- Você pode atribuir um volume a apenas um host ou cluster de host de cada vez.
- Os volumes atribuídos são compartilhados entre controladores no storage array.
- O mesmo número de unidade lógica (LUN) não pode ser usado duas vezes por um host ou um cluster de host para acessar um volume. Você deve usar um LUN exclusivo.
- Para novos grupos de volumes, se você esperar até que todos os volumes sejam criados e inicializados antes de atribuí-los a um host, o tempo de inicialização do volume será reduzido. Tenha em mente que uma vez que um volume associado ao grupo de volumes é mapeado, *all* volumes reverterá para a

inicialização mais lenta. Você pode verificar o progresso da inicialização a partir do **Home › operações em andamento**.

A atribuição de um volume falha nestas condições:

- Todos os volumes são atribuídos.
- O volume já está atribuído a outro host ou cluster de host.

A capacidade de atribuir um volume não está disponível nestas condições:

- Não existem hosts ou clusters de host válidos.
- Nenhum identificador de porta de host foi definido para o host.
- Todas as atribuições de volume foram definidas.

Todos os volumes não atribuídos são exibidos durante esta tarefa, mas as funções para hosts com ou sem Garantia de dados (DA) se aplicam da seguinte forma:

- Para um host compatível com DA, você pode selecionar volumes habilitados PARA DA ou não habilitados PARA DA.
- Para um host que não é capaz de DA, se você selecionar um volume que é habilitado PARA DA, um aviso indica que o sistema deve DESLIGAR automaticamente DA no volume antes de atribuir o volume ao host.

**Passos**

1. Selecione **armazenamento › hosts**.
2. Selecione o host ou cluster de host ao qual você deseja atribuir volumes e clique em **atribuir volumes**.

   É apresentada uma caixa de diálogo que lista todos os volumes que podem ser atribuídos. Você pode classificar qualquer uma das colunas ou digitar algo na caixa **filtro** para facilitar a localização de volumes específicos.

3. Marque a caixa de seleção ao lado de cada volume que você deseja atribuir ou marque a caixa de seleção no cabeçalho da tabela para selecionar todos os volumes.
4. Clique em **Assign** para concluir a operação.

**Resultados**

Depois de atribuir com êxito um volume ou volumes a um host ou a um cluster de host, o sistema executa as seguintes ações:

- O volume atribuído recebe o próximo número de LUN disponível. O host usa o número LUN para acessar o volume.
- O nome do volume fornecido pelo usuário aparece nas listagens de volume associadas ao host. Se aplicável, o volume de acesso configurado de fábrica também aparece nas listagens de volume associadas ao host.

## Gerenciar hosts e clusters

### Altere o tipo de host padrão

Use a configuração alterar sistema operacional padrão do host para alterar o tipo de host padrão no nível do storage de armazenamento. Geralmente, você alterará o tipo de host

padrão antes de conetar os hosts ao storage array ou quando conetar hosts adicionais.

**Sobre esta tarefa**

Tenha em mente estas diretrizes:

- Se todos os hosts que você planeja se conetar ao storage de armazenamento tiverem o mesmo sistema operacional (ambiente de host homogêneo), altere o tipo de host para corresponder ao sistema operacional.
- Se houver hosts com sistemas operacionais diferentes que você planeja se conetar ao storage array (ambiente de host heterogêneo), altere o tipo de host para corresponder à maioria dos sistemas operacionais dos hosts.

  Por exemplo, se você estiver conetando oito hosts diferentes ao storage array e seis desses hosts estiverem executando um sistema operacional Windows, você deverá selecionar o Windows como o tipo de sistema operacional de host padrão.

- Se a maioria dos hosts conetados tiver uma combinação de diferentes sistemas operacionais, altere o tipo de host para padrão de fábrica.

  Por exemplo, se você estiver conetando oito hosts diferentes ao storage array e dois desses hosts estiverem executando um sistema operacional Windows, três estiverem executando um sistema operacional VMware e outros três estiverem executando um sistema operacional Linux, você deverá selecionar padrão de fábrica como o tipo de sistema operacional padrão de host.

**Passos**

1. Selecione **Definições › sistema**.
2. Role para baixo até **Configurações adicionais** e clique em **alterar o tipo de sistema operacional padrão do host**.
3. Selecione o tipo de sistema operacional do host que você deseja usar como padrão.
4. Clique em **alterar**.

### Anular atribuição de volumes

Desmarque a atribuição de volumes de hosts ou clusters de host se você não precisar mais de acesso de e/S a esse volume a partir do cluster de host ou host.

**Sobre esta tarefa**

Mantenha estas diretrizes em mente quando você anular a atribuição de um volume:

- Se você estiver removendo o último volume atribuído de um cluster de host e o cluster de host também tiver hosts com volumes atribuídos específicos, certifique-se de remover ou mover essas atribuições antes de remover a última atribuição para o cluster de host.
- Se um cluster de host, um host ou uma porta de host for atribuído a um volume registrado no sistema operacional, você deverá limpar esse Registro antes de remover esses nós.

**Passos**

1. Selecione **armazenamento › hosts**.
2. Selecione o host ou cluster de host que você deseja editar e clique em **UnAssign volumes**.

   É apresentada uma caixa de diálogo que mostra todos os volumes que estão atualmente atribuídos.

3. Marque a caixa de seleção ao lado de cada volume que você deseja cancelar a atribuição ou marque a caixa de seleção no cabeçalho da tabela para selecionar todos os volumes.
4. Clique em **UnAssign**.

**Resultados**

- Os volumes que não foram atribuídos estão disponíveis para uma nova atribuição.
- Até que as alterações sejam configuradas no host, o volume ainda é reconhecido pelo sistema operacional do host.

### Excluir host ou cluster de host

Você pode excluir um host ou cluster de host.

**Sobre esta tarefa**

Tenha estas diretrizes em mente quando você excluir um host ou um cluster de host:

- Quaisquer atribuições específicas de volume são excluídas e os volumes associados estão disponíveis para uma nova atribuição.
- Se o host fizer parte de um cluster de host que tenha suas próprias atribuições específicas, o cluster de host não será afetado. No entanto, se o host fizer parte de um cluster de host que não tenha outras atribuições, o cluster de host e quaisquer outros hosts ou identificadores de porta de host associados herdarão quaisquer atribuições padrão.
- Quaisquer identificadores de porta de host que foram associados ao host tornam-se indefinidos.

**Passos**

1. Selecione **armazenamento › hosts**.
2. Selecione o host ou cluster de host que você deseja excluir e clique em **Excluir**.

   É apresentada a caixa de diálogo de confirmação.

3. Confirme se deseja executar a operação e clique em **Excluir**.

**Resultados**

Se você excluir um host, o sistema executará as seguintes ações:

- Exclui o host e, se aplicável, o remove do cluster de host.
- Remove o acesso a quaisquer volumes atribuídos.
- Retorna os volumes associados a um estado não atribuído.
- Retorna qualquer identificador de porta de host associado ao host para um estado não associado.

Se você excluir um cluster de host, o sistema executará as seguintes ações:

- Exclui o cluster de host e seus hosts associados (se houver).
- Remove o acesso a quaisquer volumes atribuídos.
- Retorna os volumes associados a um estado não atribuído.
- Retorna todos os identificadores de porta de host associados aos hosts para um estado não associado.

### Definir relatórios de conetividade de host

Você pode ativar os relatórios de conetividade do host para que o storage array monitore continuamente a conexão entre os controladores e os hosts configurados e, em seguida, alerte se a conexão for interrompida. Esta funcionalidade está ativada por predefinição.

#### Sobre esta tarefa

Se você desativar os relatórios de conetividade do host, o sistema não monitora mais os problemas de conetividade ou driver multipath com um host conetado ao storage array.

> A desativação do relatório de conetividade do host também desativa o balanceamento automático de carga, que monitora e equilibra a utilização de recursos do controlador.

#### Passos

1. Selecione **Definições › sistema**.
2. Role para baixo até **Configurações adicionais** e clique em **Ativar/Desativar relatórios de conetividade do host**.

   O texto abaixo dessa opção indica se ela está atualmente ativada ou desativada.

   Abre-se uma caixa de diálogo de confirmação.

3. Clique em **Yes** para continuar.

   Ao selecionar esta opção, pode alternar a funcionalidade entre activado/desativado.

## Gerir definições

### Altere as configurações de um host

É possível alterar o nome, o tipo de sistema operacional de host e os clusters de host associados a um host.

#### Passos

1. Selecione **armazenamento › hosts**.
2. Selecione o host que você deseja editar e clique em **Exibir/Editar configurações**.

   É apresentada uma caixa de diálogo que mostra as definições atuais do anfitrião.

3. Se ainda não estiver selecionado, clique na guia **Propriedades**.
4. Altere as definições conforme adequado.

**Detalhes do campo**

| Definição | Descrição |
|---|---|
| Nome | Você pode alterar o nome fornecido pelo usuário do host. É necessário especificar um nome para o host. |
| Cluster de host associado | Você pode escolher uma das seguintes opções:<br>• **None** — o host permanece um host autônomo. Se o host foi associado a um cluster de host, o sistema removerá o host do cluster.<br>• **<Host Cluster>** — o sistema associa o host ao cluster selecionado. |
| Tipo de sistema operacional de host | Você pode alterar o tipo de sistema operacional em execução no host que você definiu. |

5. Clique em **Salvar**.

### Altere as configurações de um cluster de host

Você pode alterar o nome do cluster de host ou adicionar ou remover hosts em um cluster de host.

**Passos**

1. Selecione **armazenamento › hosts**.
2. Selecione o cluster de host que deseja editar e clique em **Exibir/Editar configurações**.

   É apresentada uma caixa de diálogo que mostra as definições atuais do cluster de anfitrião.

3. Altere as configurações do cluster de host conforme apropriado.

**Detalhes do campo**

| Definição | Descrição |
|---|---|
| Nome | Você pode especificar o nome fornecido pelo usuário do cluster de host. É necessário especificar um nome para um cluster. |
| Hosts associados | Para adicionar um host, clique na caixa **hosts associados** e selecione um nome de host na lista suspensa. Não é possível inserir manualmente um nome de host.<br><br>Para excluir um host, clique no **X** ao lado do nome do host. |

4. Clique em **Salvar**.

### Alterar identificadores de porta do host para um host

Altere os identificadores de porta do host quando você quiser alterar o rótulo de usuário em um identificador de porta do host, adicionar um novo identificador de porta do host ao host ou excluir um identificador de porta do host do host.

#### Sobre esta tarefa

Ao alterar identificadores de porta do host, tenha em mente as seguintes diretrizes:

- **Add** — quando você adiciona uma porta de host, você está associando o identificador de porta de host ao host que você criou para se conetar ao seu storage array. Você pode inserir manualmente as informações da porta usando um utilitário HBA (adaptador de barramento do host).
- * Editar* — você pode editar as portas do host para mover (associar) uma porta de host para um host diferente. Você pode ter movido o adaptador de barramento do host ou o iniciador iSCSI para um host diferente, então você deve mover (associar) a porta do host para o novo host.
- **Delete** — você pode excluir portas de host para remover (não associar) portas de host de um host.

#### Passos

1. Selecione **armazenamento › hosts**.
2. Selecione o host ao qual as portas serão associadas e clique em **Exibir/Editar configurações**.

   Se quiser adicionar portas a um host em um cluster de host, expanda o cluster de host e selecione o host desejado. Não é possível adicionar portas no nível do cluster de host.

   É apresentada uma caixa de diálogo que mostra as definições atuais do anfitrião.

3. Clique na guia **Host Ports**.

   A caixa de diálogo mostra os identificadores de porta do host atual.

4. Altere as configurações do identificador da porta do host conforme apropriado.

| Definição | Descrição |
| --- | --- |
| Porta do host | Você pode escolher uma das seguintes opções:<br>• **Add** — Use Add para associar um novo identificador de porta de host ao host. O comprimento do nome do identificador da porta do host é determinado pela tecnologia da interface do host. Os nomes dos identificadores de porta de host Fibre Channel e Infiniband devem ter 16 carateres. Os nomes dos identificadores de porta de host iSCSI têm um máximo de 223 carateres. A porta deve ser única. Não é permitido um número de porta que já tenha sido configurado.<br>• **Delete** — Use Delete para remover (não associar) um identificador de porta de host. A opção Excluir não remove fisicamente a porta do host. Essa opção remove a associação entre a porta do host e o host. A menos que você remova o adaptador de barramento do host ou o iniciador iSCSI, a porta do host ainda é reconhecida pelo controlador.<br>Se você excluir um identificador de porta do host, ele não estará mais associado a esse host. Além disso, o host perde o acesso a qualquer um de seus volumes atribuídos por meio desse identificador de porta do host. |
| Etiqueta | Para alterar o nome da etiqueta da porta, clique no ícone **Editar** (lápis). O nome da etiqueta da porta deve ser exclusivo. Não é permitido um nome de rótulo que já tenha sido configurado. |
| Segredo de CHAP | Aparece apenas para hosts iSCSI. Você pode definir ou alterar o segredo CHAP para os iniciadores (hosts iSCSI).<br>O System Manager usa o método CHAP (Challenge Handshake Authentication Protocol), que valida a identidade de alvos e iniciadores durante o link inicial. A autenticação é baseada em uma chave de segurança compartilhada chamada CHAP secret. |

5. Clique em **Salvar**.

## FAQs

**O que são hosts e clusters de host?**

Um host é um servidor que envia e/S para um volume em um storage array. Um cluster de host é um grupo de hosts. Você cria um cluster de host para facilitar a atribuição dos mesmos volumes a vários hosts.

Você define um host separadamente. Pode ser uma entidade independente ou ser adicionada a um cluster de host. Você pode atribuir volumes a um host individual ou um host pode fazer parte de um cluster de host que compartilha o acesso a um ou mais volumes com outros hosts no cluster de host.

O cluster de host é uma entidade lógica que você cria no Gerenciador de sistema do SANtricity. Você deve adicionar hosts ao cluster de host antes de poder atribuir volumes.

#### Por que eu precisaria criar um cluster de host?

Você precisa criar um cluster de host se quiser que dois ou mais hosts compartilhem o acesso ao mesmo conjunto de volumes. Normalmente, os hosts individuais têm software de cluster instalado neles para coordenar o acesso ao volume.

#### Como sei qual tipo de sistema operacional do host está correto?

O campo Host Operating System Type (tipo de sistema operativo anfitrião) contém o sistema operativo do anfitrião. Você pode selecionar o tipo de host recomendado na lista suspensa.

Os tipos de host que aparecem na lista suspensa dependem do modelo do storage array e da versão do firmware. As versões mais recentes exibem as opções mais comuns primeiro, que são as mais prováveis de serem apropriadas. A aparência nesta lista não implica que a opção seja totalmente suportada.

Para obter mais informações sobre o suporte ao host, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Alguns dos seguintes tipos de host podem aparecer na lista:

| Tipo de sistema operacional do host | Sistema operacional (SO) e driver multipath |
|---|---|
| Linux DM-MP (Kernel 3,10 ou posterior) | Suporta sistemas operacionais Linux usando uma solução de failover multipath Device Mapper com um Kernel 3,10 ou posterior. |
| VMware ESXi | Oferece suporte aos sistemas operacionais VMware ESXi que executam a arquitetura NMP (NMP) nativa usando o módulo SATP_ALUA interno de política de tipo de matriz de armazenamento da VMware. |
| Windows (em cluster ou não em cluster) | Oferece suporte a configurações em cluster ou não em cluster do Windows que não estejam executando o driver de multipathing ATTO. |
| ATTO Cluster (todos os sistemas operacionais) | Suporta todas as configurações de cluster usando o driver ATTO Technology, Inc., multipathing. |
| Linux (Veritas DMP) | Suporta sistemas operacionais Linux usando uma solução de multipathing Veritas DMP. |
| Linux (ATTO) | Suporta sistemas operacionais Linux usando um ATTO Technology, Inc., driver multipathing. |
| Mac os (ATTO) | Suporta versões do Mac os usando um ATTO Technology, Inc., driver multipathing. |
| Windows (ATTO) | Suporta sistemas operacionais Windows usando um ATTO Technology, Inc., driver multipathing. |

| Tipo de sistema operacional do host | Sistema operacional (SO) e driver multipath |
| --- | --- |
| FlexArray (ALUA) | Suporta um sistema NetApp FlexArray usando ALUA para multipathing. |
| SVC DA IBM | Suporta uma configuração do IBM SAN volume Controller. |
| Predefinição de fábrica | Reservado para a inicialização inicial do storage array. Se o tipo de sistema operacional do host estiver definido como padrão de fábrica, altere-o para corresponder ao sistema operacional do host e ao driver multipath executados no host conetado. |
| Linux DM-MP (Kernel 3,9 ou anterior) | Suporta sistemas operacionais Linux usando uma solução de failover multipath Device Mapper com um Kernel 3,9 ou anterior. |
| Janela agrupada (obsoleta) | Se o tipo de sistema operacional do host estiver definido para esse valor, use a configuração Windows (em cluster ou não em cluster). |

**O que são HBAs e portas adaptadoras?**

Um adaptador de barramento de host (HBA) é uma placa que reside em um host e contém uma ou mais portas de host. Uma porta de host é uma porta em um adaptador de barramento de host (HBA) que fornece a conexão física a um controlador e é usada para operações de e/S.

As portas do adaptador no HBA são chamadas de portas de host. A maioria dos HBAs tem uma ou duas portas de host. O HBA tem um identificador mundial único (WWID), e cada porta de host HBA tem um WWID exclusivo. Os identificadores de porta do host são usados para associar o HBA apropriado ao host físico quando você estiver criando manualmente o host por meio do Gerenciador de sistema do SANtricity.

**Como faço para corresponder as portas do host a um host?**

Se você estiver criando manualmente um host, primeiro deverá usar o utilitário HBA (adaptador de barramento de host) apropriado disponível no host para determinar os identificadores de porta de host associados a cada HBA instalado no host.

Quando tiver essas informações, selecione os identificadores de porta do host que fizeram login no storage array na lista fornecida na caixa de diálogo criar host.

Certifique-se de selecionar os identificadores de porta de host apropriados para o host que você está criando. Se você associar os identificadores de porta do host errados, poderá causar acesso não intencional de outro host a esses dados.

**Como faço para criar segredos CHAP?**

Se você configurar a autenticação CHAP (Challenge Handshake Authentication Protocol) em qualquer host iSCSI conetado à matriz de armazenamento, será necessário inserir novamente esse segredo CHAP iniciador para cada host iSCSI.

Para fazer isso, você pode usar o System Manager como parte da operação criar host ou através da opção Exibir/Editar configurações.

Se você estiver usando a autenticação mútua CHAP, você também deve definir um segredo CHAP de destino para o storage array na página Configurações e digitar novamente esse segredo CHAP de destino em cada host iSCSI.

**Qual é o cluster padrão?**

O cluster padrão é uma entidade definida pelo sistema que permite que qualquer identificador de porta de host não associado que tenha feito logon no storage array tenha acesso aos volumes atribuídos ao cluster padrão. Um identificador de porta de host não associado é uma porta de host que não está logicamente associada a um host específico, mas é fisicamente instalada em um host e conetada ao storage array.

> Se você quiser que os hosts tenham acesso específico a determinados volumes no storage array, *não* use o cluster padrão. Em vez disso, você deve associar os identificadores de porta do host aos respetivos hosts. Esta tarefa pode ser feita manualmente durante a operação criar host. Em seguida, você atribui volumes a um host individual ou a um cluster de host.

Você deve *somente* usar o cluster padrão em situações especiais em que seu ambiente de armazenamento externo é propício para permitir que todos os hosts e todos os identificadores de porta de host conetados à matriz de armazenamento tenham acesso a todos os volumes (modo de acesso total) sem fazer especificamente os hosts conhecidos pela matriz de armazenamento ou pela interface de usuário.

Inicialmente, você pode atribuir volumes apenas ao cluster padrão por meio da interface de linha de comando (CLI). No entanto, depois de atribuir pelo menos um volume ao cluster padrão, essa entidade (chamada cluster padrão) é exibida na interface do usuário, onde você pode gerenciar essa entidade.

**O que é o relatório de conetividade do host?**

Quando o relatório de conetividade do host é ativado, o storage array monitora continuamente a conexão entre os controladores e os hosts configurados e, em seguida, alerta você se a conexão for interrompida.

Interrupções na conexão podem ocorrer se houver um cabo solto, danificado ou ausente, ou outro problema com o host. Nessas situações, o sistema pode abrir uma mensagem Recovery Guru:

- **Redundância de host perdida** — abre se qualquer controlador não puder se comunicar com o host.
- **Host Type Incorrect** — abre se o tipo de host for especificado incorretamente na matriz de armazenamento, o que pode resultar em problemas de failover.

Você pode querer desativar o relatório de conetividade do host em situações em que a reinicialização de um controlador pode levar mais tempo do que o tempo limite da conexão. Desativar esse recurso suprime as mensagens Gurus de recuperação.

> A desativação do relatório de conetividade do host também desativa o balanceamento automático de carga, que monitora e equilibra o uso de recursos do controlador. No entanto, se você reativar os relatórios de conetividade do host, o recurso de balanceamento de carga automático não será reativado automaticamente.

# Instantâneos

## Visão geral dos instantâneos

O recurso Snapshot permite que você crie imagens pontuais de volumes de storage array a serem usados para backup ou teste.

### O que são imagens instantâneas?

Uma imagem *snapshot* é uma cópia lógica dos dados de volume, capturados em um determinado ponto no tempo. Como um ponto de restauração, as imagens instantâneas permitem que você role de volta para um conjunto de dados em boas condições. Embora o host possa acessar a imagem instantânea, ele não pode ler ou gravar diretamente nela.

Saiba mais:

- "Como funciona o armazenamento de instantâneos"
- "Terminologia Snapshot"
- "Volumes base, capacidade reservada e grupos de snapshot"
- "Agendamentos de snapshot e grupos de consistência"
- "Volumes Snapshot"

### Como faço para criar snapshots?

Você pode criar manualmente uma imagem de snapshot a partir de um volume base ou grupo de consistência de snapshot. Este procedimento está disponível no **armazenamento › instantâneos**.

Saiba mais:

- "Requisitos e diretrizes para snapshots"
- "Fluxo de trabalho para criar imagens instantâneas e volumes"
- "Crie uma imagem instantânea"
- "Agendar imagens instantâneas"
- "Crie um grupo de consistência de snapshot"
- "Criar um volume instantâneo"

### Como faço para reverter dados de um snapshot?

Um *rollback* é o processo de retornar dados em um volume base para um ponto anterior no tempo. Você pode reverter os dados instantâneos a partir do **armazenamento › instantâneos**.

Saiba mais:

- "Reversão do Snapshot"
- "Inicie uma reversão de imagem instantânea para um volume base"
- "Inicie uma reversão de imagem instantânea para um membro do grupo de consistência"

### Informações relacionadas

Saiba mais sobre tarefas relacionadas a instantâneos:

- "Alterar a capacidade reservada para um volume de snapshot"
- "Alterar a capacidade reservada para um grupo de snapshot"

## Conceitos

### Como funciona o armazenamento de instantâneos

O recurso Snapshots usa tecnologia copy-on-write para armazenar imagens instantâneas e usar a capacidade reservada alocada.

#### Como as imagens instantâneas são usadas

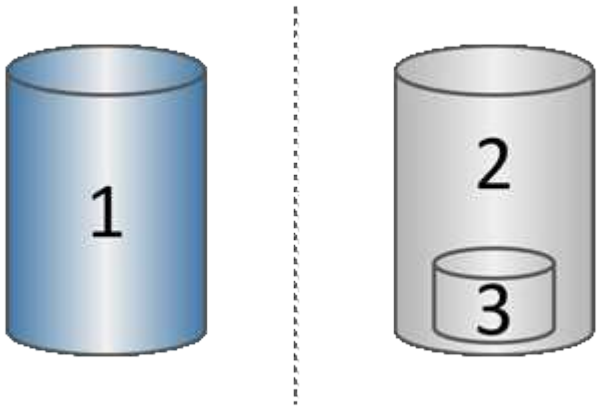
Uma imagem instantânea é uma cópia lógica e somente leitura do conteúdo do volume, capturada em um determinado momento. Você pode usar snapshots para se proteger contra a perda de dados.

As imagens instantâneas também são úteis para ambientes de teste. Ao criar uma cópia virtual de dados, você pode testar os dados usando o snapshot sem alterar o próprio volume. Além disso, os hosts não têm acesso de gravação a imagens instantâneas, portanto, seus snapshots são sempre um recurso de backup seguro.

#### Criação de snapshot

À medida que os instantâneos são criados, o recurso Snapshots armazena os dados da imagem da seguinte forma:

- Quando uma imagem instantânea é criada, ela corresponde exatamente ao volume base. O recurso Snapshots usa tecnologia copy-on-write. Depois que o snapshot é capturado, a primeira gravação em qualquer bloco ou conjunto de blocos no volume base faz com que os dados originais sejam copiados para a capacidade reservada antes de gravar os novos dados no volume base.
- Os instantâneos subsequentes incluem apenas blocos de dados alterados. Antes que os dados sejam sobrescritos no volume base, o recurso Snapshots usa sua tecnologia copy-on-write para salvar as imagens necessárias dos setores afetados na capacidade reservada do snapshot.




1. Volume base (capacidade de disco físico); 2 Snapshots (capacidade de disco lógico); 3. Capacidade reservada (capacidade de disco físico)

- A capacidade reservada armazena blocos de dados originais para partes do volume base que foram alteradas após a captura instantânea e inclui um índice para rastrear alterações. Geralmente, o tamanho da capacidade reservada é de 40% do volume base. (Se você precisar de mais capacidade reservada, poderá aumentar a capacidade reservada.)
- As imagens instantâneas são armazenadas numa ordem específica, com base no seu carimbo de data/hora. Apenas a imagem instantânea mais antiga de um volume base está disponível para eliminação manual.

#### Restauração de instantâneos

Para restaurar dados para um volume base, você pode usar um volume instantâneo ou uma imagem instantânea:

- **Volume instantâneo** — se você precisar recuperar arquivos excluídos, crie um volume instantâneo a partir de uma imagem de snapshot em boas condições e, em seguida, atribua-o ao host.
- **Imagem instantânea** — se você precisar restaurar um volume base para um determinado ponto no tempo, use uma imagem snapshot anterior para reverter os dados para o volume base.

### Terminologia Snapshot

Saiba como os termos do snapshot se aplicam ao storage array.

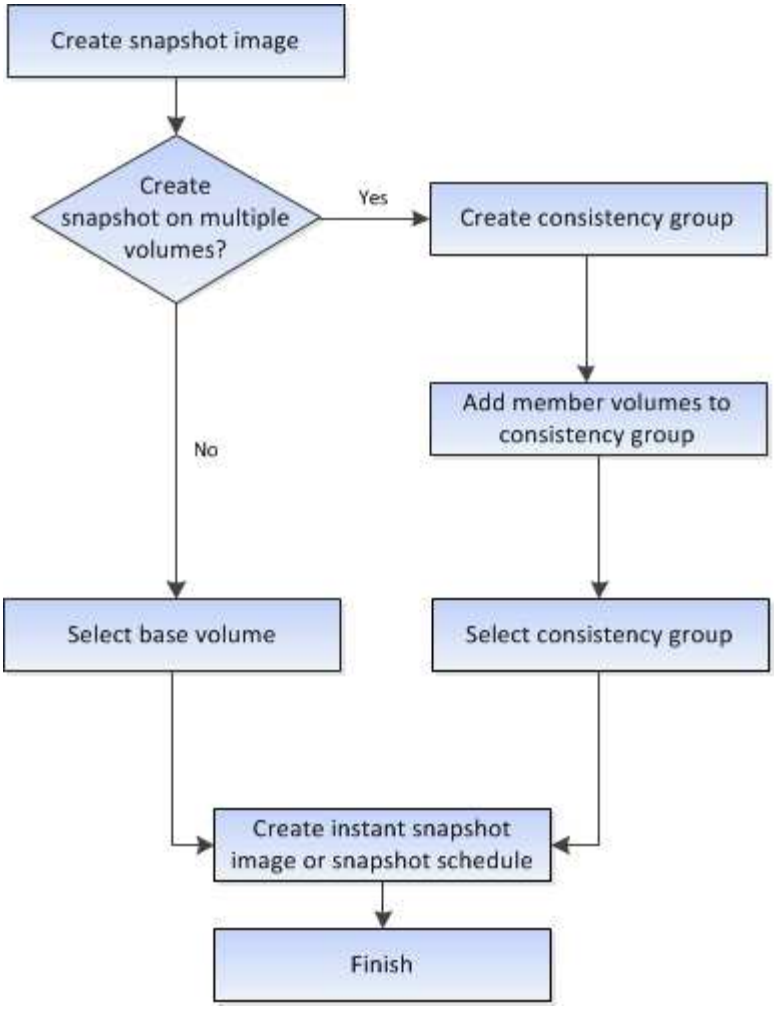
| Prazo | Descrição |
|---|---|
| Recurso de instantâneos | O recurso Snapshots é usado para criar e gerenciar imagens de volumes. |
| Imagem instantânea | Uma imagem instantânea é uma cópia lógica dos dados de volume, capturados em um determinado ponto no tempo. Como um ponto de restauração, as imagens instantâneas permitem que você role de volta para um conjunto de dados em boas condições. Embora o host possa acessar a imagem instantânea, ele não pode ler ou gravar diretamente nela. |
| Volume base | Um volume base é a origem a partir da qual uma imagem instantânea é criada. Pode ser um volume grosso ou fino e é normalmente atribuído a um host. O volume base pode residir em um grupo de volumes ou em um pool de discos. |
| Volume do Snapshot | Um volume instantâneo permite que o host acesse dados na imagem instantânea. O volume instantâneo contém a sua própria capacidade reservada, que guarda quaisquer modificações no volume base sem afetar a imagem instantânea original. |
| Grupo de instantâneos | Um grupo de instantâneos é uma coleção de imagens instantâneas a partir de um único volume base. |
| Volume de capacidade reservada | Um volume de capacidade reservada rastreia quais blocos de dados do volume base são sobrescritos e o conteúdo preservado desses blocos. |
| Agendamento do Snapshot | Um agendamento de instantâneos é um calendário para criar imagens instantâneas automatizadas. Através da programação, você pode controlar a frequência das criações de imagens. |

| Prazo | Descrição |
| --- | --- |
| Grupo de consistência do Snapshot | Um grupo de consistência de snapshot é uma coleção de volumes que são tratados como uma única entidade quando uma imagem instantânea é criada. Cada um desses volumes tem sua própria imagem instantânea, mas todas as imagens são criadas no mesmo momento. |
| Volume do membro do grupo de consistência de snapshot | Cada volume que pertence a um grupo de consistência de instantâneos é referido como um volume de membro. Quando você adiciona um volume a um grupo de consistência de snapshot, o System Manager cria automaticamente um novo grupo de snapshot que corresponde a esse volume de membro. |
| Reverter | Uma reversão é o processo de retornar dados em um volume base para um ponto anterior no tempo. |
| Capacidade reservada | A capacidade reservada é a capacidade alocada física usada para qualquer operação de serviço de cópia e objeto de storage. Não é diretamente legível pelo host. |

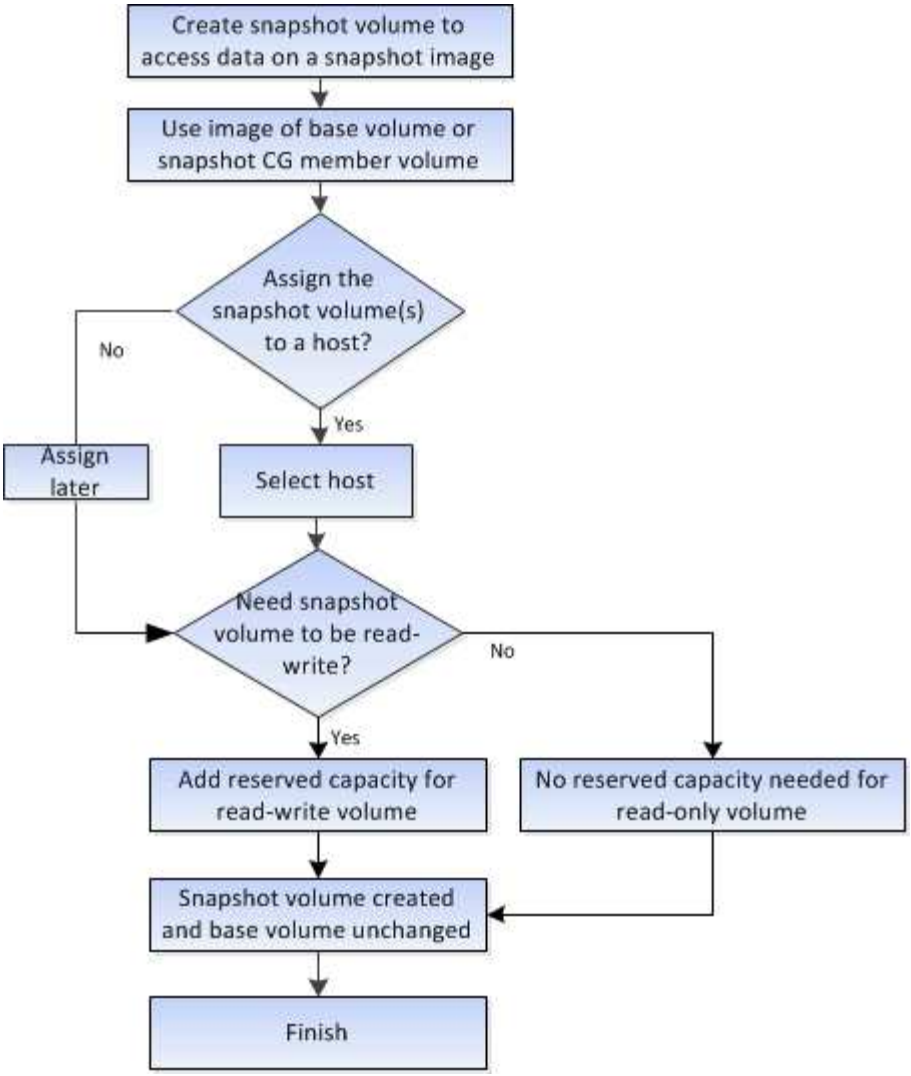
### Fluxo de trabalho para criar imagens instantâneas e volumes instantâneos

No System Manager, pode criar imagens instantâneas e volumes instantâneos seguindo estes passos.

#### Fluxo de trabalho para criar imagens instantâneas




**Fluxo de trabalho para criar volumes instantâneos**




**Requisitos e diretrizes para snapshots**

Ao criar e usar snapshots, revise os requisitos e diretrizes a seguir.

#### Imagens instantâneas e grupos de instantâneos

- Cada imagem instantânea está associada a exatamente um grupo de instantâneos.
- Um grupo de instantâneos é criado na primeira vez que você cria uma imagem de instantâneo agendada ou instantânea para um objeto associado. Isso cria capacidade reservada.

  Pode visualizar grupos de instantâneos a partir da página pools e grupos de volume.

- As imagens instantâneas programadas não ocorrem quando a matriz de armazenamento está offline ou desligada.
- Se eliminar um grupo de instantâneos que tenha uma agenda de instantâneos, a agenda de instantâneos também é eliminada.
- Se você tiver um volume instantâneo que não precisa mais, poderá reutilizá-lo, juntamente com qualquer capacidade reservada associada, em vez de excluí-lo. Isso cria um volume instantâneo diferente do mesmo volume base. Pode associar novamente o volume instantâneo ou o volume instantâneo do grupo de consistência de instantâneos à mesma imagem instantânea ou a uma imagem de instantâneo diferente, desde que a imagem de instantâneo esteja no mesmo volume base.

#### Grupo de consistência do Snapshot

- Um grupo de consistência de snapshot contém um grupo de snapshot para cada volume que é membro do grupo de consistência de snapshot.
- Você pode associar um grupo de consistência de snapshot a apenas uma programação.
- Se você excluir um grupo de consistência de snapshot que tenha uma programação de snapshot, a programação de snapshot também será excluída.
- Não é possível gerenciar individualmente um grupo de snapshot associado a um grupo de consistência de snapshot. Em vez disso, você deve executar as operações de gerenciamento (criar imagem instantânea, excluir imagem instantânea ou grupo instantâneo e reverter imagem instantânea) no nível do grupo de consistência de snapshot.

#### Volume base

- Um volume instantâneo deve ter as mesmas configurações de segurança e garantia de dados que o volume base associado.
- Não é possível criar um volume instantâneo de um volume base com falha.
- Se o volume base residir em um grupo de volumes, os volumes membros de qualquer grupo de consistência de snapshot associado poderão residir em um pool ou grupo de volumes.
- Se um volume base residir em um pool, todos os volumes de membros de qualquer grupo de consistência de snapshot associado deverão residir no mesmo pool que o volume base.

#### Capacidade reservada

- A capacidade reservada está associada a apenas um volume base.
- A utilização de um agendamento pode resultar num grande número de imagens instantâneas. Certifique-se de ter capacidade reservada suficiente para snapshots programados.
- O volume de capacidade reservada para um grupo de consistência de instantâneos deve ter as mesmas configurações de segurança e garantia de dados que seu volume base associado para o volume membro do grupo de consistência de snapshot.

#### Imagens instantâneas pendentes

A criação de imagens instantâneas pode permanecer em um estado pendente nas seguintes condições:

- O volume base que contém esta imagem instantânea é membro de um grupo de espelhos assíncrono.
- O volume base está atualmente em uma operação de sincronização. A criação da imagem instantânea é concluída assim que a operação de sincronização for concluída.

#### Número máximo de imagens instantâneas

- Se um volume for membro de um grupo de consistência de snapshot, o System Manager criará um grupo de snapshot para esse volume de membro. Este grupo de instantâneos conta para o número máximo permitido de grupos de instantâneos por volume base.
- Se tentar criar uma imagem instantânea num grupo de instantâneos ou num grupo de consistência de instantâneos, mas o grupo associado tiver atingido o número máximo de imagens instantâneas, tem duas opções:
  - Ative a exclusão automática para o grupo de snapshot ou grupo de consistência de snapshot.
  - Elimine manualmente uma ou mais imagens de instantâneos do grupo de instantâneos ou do grupo de consistência de instantâneos e repita a operação.

#### Eliminação automática

Se o grupo de instantâneos ou o grupo de consistência de instantâneos estiver ativado para eliminação automática, o System Manager eliminará a imagem de instantâneo mais antiga quando o sistema criar uma nova para o grupo.

#### Operação de reversão

- Você não pode executar as seguintes ações quando uma operação de reversão estiver em andamento:
  - Exclua a imagem instantânea que está sendo usada para a reversão.
  - Crie uma nova imagem instantânea para um volume base que esteja participando de uma operação de reversão.
  - Altere a Política de Repositório completo do grupo de instantâneos associado.
- Não é possível iniciar uma operação de reversão quando qualquer uma dessas operações estiver em andamento:
  - Expansão de capacidade (adição de capacidade a um pool ou grupo de volumes)
  - Expansão de volume (aumentando a capacidade de um volume)
  - Alteração de nível RAID para um grupo de volumes
  - Alteração do tamanho do segmento para um volume
- Não é possível iniciar uma operação de reversão se o volume base estiver participando de uma cópia de volume.
- Não é possível iniciar uma operação de reversão se o volume base for um volume secundário em um espelho remoto.
- Uma operação de reversão falhará se alguma da capacidade usada no volume do repositório instantâneo associado tiver setores ilegíveis.

### Volumes base, capacidade reservada e grupos de snapshot

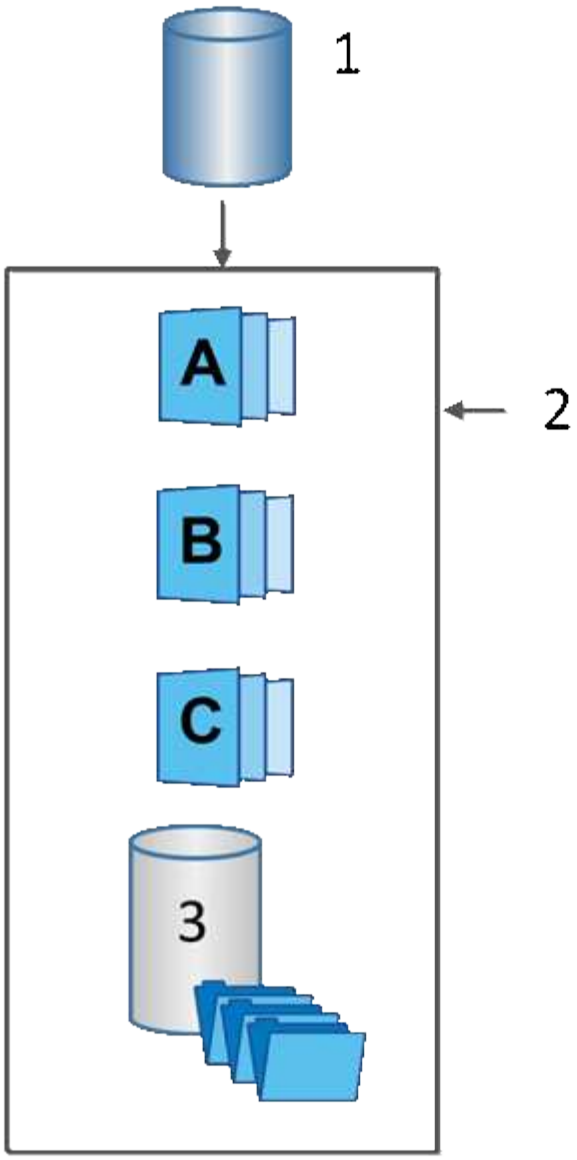
O recurso Snapshots faz uso de volumes base, capacidade reservada e grupos de snapshot.

#### Volumes base

Um *volume base* é o volume usado como a origem de uma imagem instantânea. Um volume base pode ser um volume grosso ou um volume fino e pode residir em um pool ou grupo de volumes.

Para tirar instantâneos do volume base, você pode criar uma imagem instantânea a qualquer momento ou automatizar o processo definindo uma programação regular para instantâneos.

A figura a seguir mostra a relação entre os objetos snapshot e o volume base.




1. Volume base; 2 objetos instantâneos no grupo (imagens e capacidade reservada); 3 capacidade reservada para o grupo instantâneo.

#### Capacidade reservada e grupos de snapshot

O System Manager organiza imagens instantâneas em *grupos de instantâneos*. Quando o System Manager estabelece o grupo de instantâneos, cria automaticamente a capacidade reservada associada _para manter as imagens instantâneas para o grupo e para acompanhar as alterações subsequentes a instantâneos adicionais.

Se o volume base residir em um grupo de volumes, a capacidade reservada poderá ser localizada em um pool ou grupo de volumes. Se o volume base residir em um pool, a capacidade reservada deverá estar localizada no mesmo pool que o volume base.

Os grupos de snapshot não exigem nenhuma ação do usuário, mas você pode ajustar a capacidade reservada em um grupo de snapshot a qualquer momento. Além disso, você pode ser solicitado a criar capacidade reservada quando as seguintes condições forem atendidas:

- Sempre que você tirar um snapshot de um volume base que ainda não tenha um grupo de snapshot, o System Manager cria automaticamente um grupo de snapshot. Esta ação também cria capacidade reservada para o volume base que é utilizado para armazenar imagens instantâneas subsequentes.
- Sempre que você criar uma programação de snapshot para um volume base, o System Manager cria automaticamente um grupo de snapshot.

#### Eliminação automática

Ao trabalhar com instantâneos, use a opção padrão para ativar a exclusão automática. A eliminação automática elimina automaticamente a imagem instantânea mais antiga quando o grupo de instantâneos atinge o limite de 32 imagens do grupo de instantâneos. Se você desativar a exclusão automática, os limites do grupo instantâneo serão eventualmente excedidos e você deverá tomar ações manuais para configurar as configurações do grupo instantâneo e gerenciar a capacidade reservada.

### Agendamentos de snapshot e grupos de consistência de snapshot

Use programações para coleta de imagens instantâneas e use grupos de consistência de snapshot para gerenciar vários volumes base.

Para gerenciar facilmente operações de snapshot de volumes base, você pode usar os seguintes recursos:

- **Agendamento de instantâneos** — Automatize instantâneos para um único volume base.
- **Snapshot consistency group** — Gerencie vários volumes base como uma entidade.

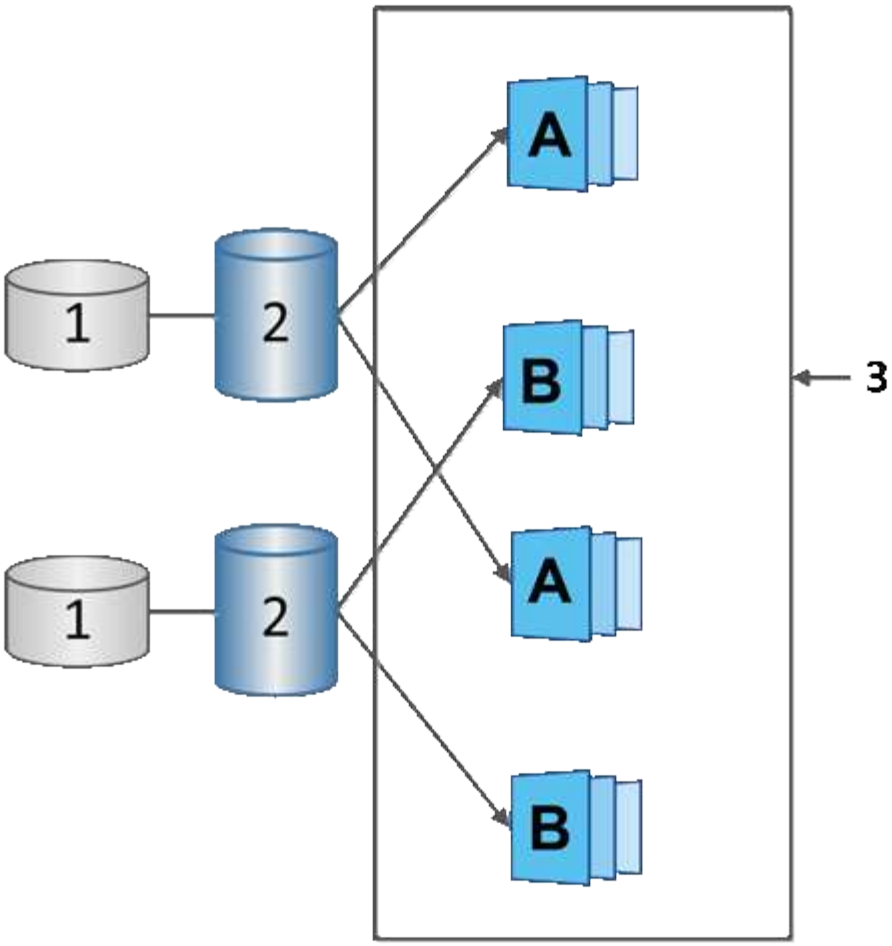
#### Agendamento do Snapshot

Se você quiser tirar snapshots automaticamente para um volume base, você pode criar um agendamento. Por exemplo, você pode definir uma programação que tira imagens instantâneas todos os sábados à meia-noite, no primeiro de cada mês ou em quaisquer datas e horas que você decidir. Depois que o máximo de 32 instantâneos for alcançado para um único agendamento, você poderá suspender snapshots programados, criar mais capacidade reservada ou excluir snapshots. Os instantâneos podem ser excluídos manualmente ou automatizando o processo de exclusão. Depois de eliminar uma imagem instantânea, a capacidade reservada adicional está disponível para reutilização.

#### Grupo de consistência do Snapshot

Você cria um grupo de consistência de instantâneos quando deseja garantir que as imagens instantâneas sejam tiradas em vários volumes ao mesmo tempo. As ações de imagem instantânea são executadas no grupo de consistência de instantâneos como um todo. Por exemplo, você pode agendar snapshots sincronizados de todos os volumes com o mesmo carimbo de data/hora. Os grupos de consistência de snapshot são ideais para aplicativos que abrangem vários volumes, como aplicativos de banco de dados que armazenam Registros em um volume e os arquivos de banco de dados em outro volume.

Os volumes incluídos em um grupo de consistência de snapshot são chamados de volumes de membros. Quando você adiciona um volume a um grupo de consistência, o System Manager cria automaticamente uma nova capacidade reservada que corresponde a esse volume de membro. Pode definir uma agenda para criar automaticamente uma imagem instantânea de cada volume de membro.



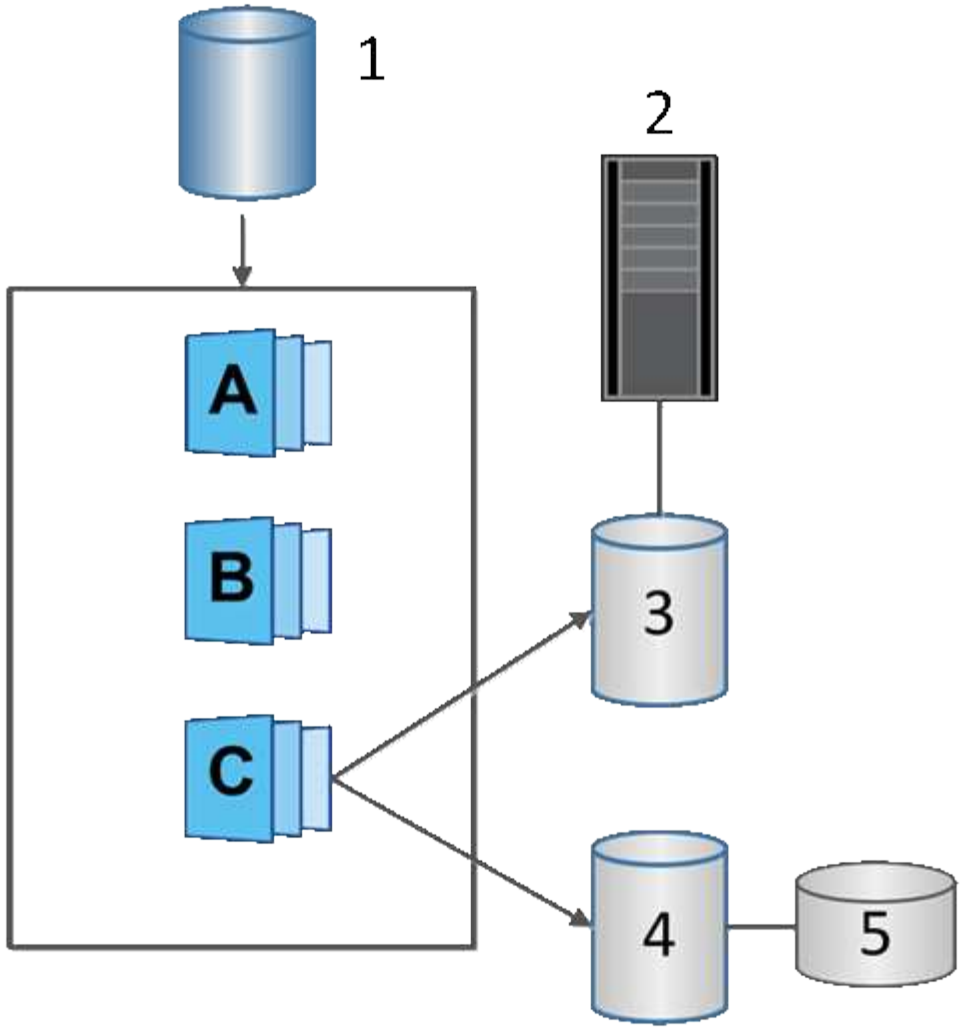

1 capacidade reservada; 2 volume de Membros; 3 imagens de instantâneos de grupo de consistência

**Volumes Snapshot**

Você pode criar um volume de snapshot e atribuí-lo a um host se quiser ler ou gravar dados de snapshot. O volume do Snapshot compartilha as mesmas características que o volume base (nível RAID, características de e/S etc.).

Ao criar um volume instantâneo, você pode designá-lo como *read-only* ou *read-write accessible*.

Quando você cria volumes snapshot somente leitura, não é necessário adicionar capacidade reservada. Ao criar volumes snapshot de leitura e gravação, você deve adicionar capacidade reservada para fornecer acesso de gravação.




1 volume base; 2 Host; 3 volume de instantâneos só de leitura; 4 volume de instantâneos de leitura-escrita; 5 capacidade reservada

**Reversão do Snapshot**

Uma operação de reversão retorna um volume base para um estado anterior, determinado pelo snapshot selecionado.

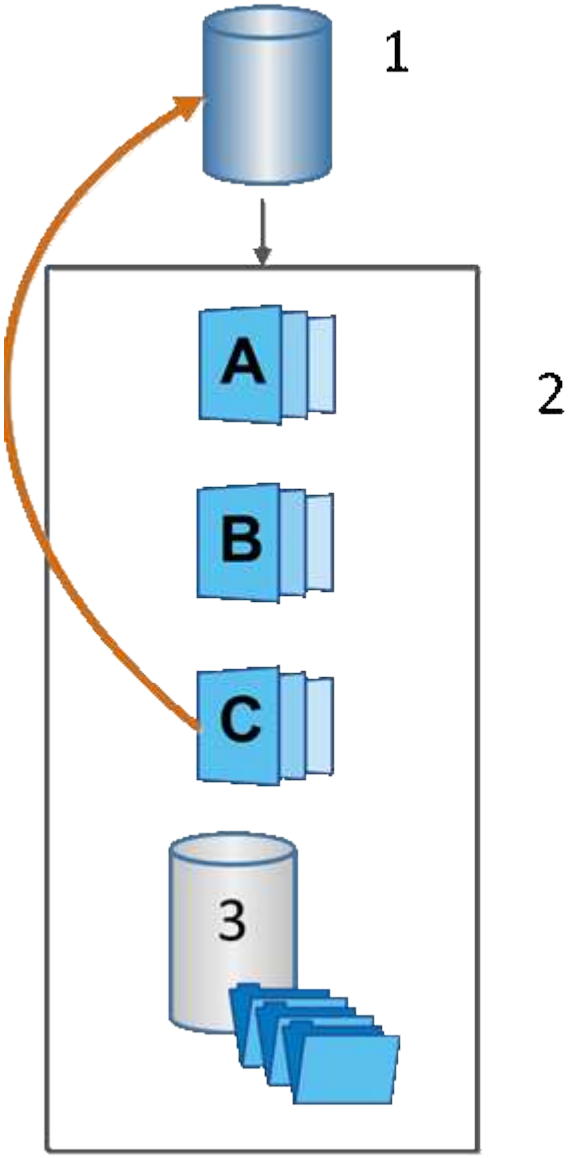
Para a reversão, você pode selecionar uma imagem instantânea de uma das seguintes fontes:

- **Snapshot image rollback**, para uma restauração completa de um volume base.
- **Snapshot consistency group rollback**, que pode ser usado para reverter um ou mais volumes.

Durante a reversão, o recurso Snapshots preserva todas as imagens instantâneas no grupo. Ele também permite que o host acesse o volume base durante esse processo, se necessário para operações de e/S.

Quando uma reversão é iniciada, um processo em segundo plano varre os endereços de bloco lógico (LBAs) para o volume base e, em seguida, encontra dados de cópia na gravação na imagem de snapshot de reversão a ser restaurada. Como o volume base é acessível ao host para leituras e gravações e todos os dados gravados anteriormente estão disponíveis imediatamente, o volume de capacidade reservada deve ser grande o suficiente para conter todas as alterações enquanto a reversão está sendo processada. A

transferência de dados continua como uma operação em segundo plano até que a reversão seja concluída.




1. Volume base; 2 objetos instantâneos em grupo; 3 capacidade reservada para o grupo

## Criar snapshots e objetos snapshot

### Criar imagem instantânea

Você pode criar manualmente uma imagem de snapshot a partir de um volume base ou grupo de consistência de snapshot. Isso também é chamado de *instantâneo instantâneo* ou *imagem instantânea*.

#### Antes de começar

- O volume de base deve ser ideal.
- A unidade deve ser ideal.

- O grupo instantâneo não pode ser designado como "reservido".
- O volume de capacidade reservada deve ter as mesmas definições de Data Assurance (DA) que o volume base associado para o grupo de instantâneos.

**Passos**

1. Execute uma das seguintes ações para criar uma imagem instantânea:
   - Selecione **armazenamento › volumes**. Selecione o objeto (volume base ou grupo de consistência de instantâneos) e, em seguida, selecione **Serviços de cópia › criar instantâneo instantâneo instantâneo**.
   - Selecione **armazenamento › instantâneos**. Selecione o separador **Snapshot Images** (imagens instantâneas) e, em seguida, selecione **Create › Instant snapshot** (criar instantâneo instantâneo).

     A caixa de diálogo criar imagem Instantânea é exibida. Selecione o objeto (volume base ou grupo de consistência de instantâneos) e clique em **Next**. Se uma imagem snapshot anterior foi criada para o grupo de consistência de volume ou snapshot, o sistema cria o instantâneo imediatamente. Caso contrário, se for a primeira vez que uma imagem instantânea for criada para o grupo de consistência de volume ou instantâneo, a caixa de diálogo confirmar criar imagem instantânea será exibida.
2. Clique em **Create** para aceitar a notificação de que a capacidade reservada é necessária e para avançar para a etapa de reserva de capacidade.

   A caixa de diálogo capacidade de reserva é exibida.
3. Use a caixa giratório para ajustar a porcentagem de capacidade e clique em **Next** para aceitar o volume do candidato destacado na tabela.

   A caixa de diálogo Editar configurações é exibida.
4. Selecione as definições da imagem instantânea conforme adequado e confirme que pretende executar a operação.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| **Configurações de imagem instantânea** | Limite de imagem instantânea |
| Mantenha a caixa de verificação selecionada se pretender que as imagens instantâneas sejam eliminadas automaticamente após o limite especificado; utilize a caixa de seleção para alterar o limite. Se desmarcar esta caixa de verificação, a criação de imagens instantâneas pára após 32 imagens. | • Configurações de capacidade reservada* |
| Alerta-me quando… | Use a caixa giratório para ajustar o ponto percentual no qual o sistema envia uma notificação de alerta quando a capacidade reservada para um grupo de instantâneos estiver quase cheia.<br><br>Quando a capacidade reservada para o grupo de instantâneos exceder o limite especificado, use o aviso prévio para aumentar a capacidade reservada ou excluir objetos desnecessários antes que o espaço restante se esgote. |
| Política de capacidade reservada completa | Escolha uma das seguintes políticas:<br><br>• **Limpar imagem de snapshot mais antiga** — o sistema limpa automaticamente a imagem de snapshot mais antiga no grupo de instantâneos, que libera a capacidade reservada da imagem de snapshot para reutilização dentro do grupo.<br>• **Rejeitar gravações no volume base** — quando a capacidade reservada atinge sua porcentagem máxima definida, o sistema rejeita qualquer solicitação de gravação de e/S para o volume base que acionou o acesso à capacidade reservada. |

**Resultados**

- O System Manager (Gestor do sistema) apresenta a nova imagem instantânea na tabela Snapshot Images (imagens instantâneas). A tabela lista a nova imagem por carimbo de data/hora e o volume base associado ou grupo de consistência de instantâneos.
- A criação de instantâneos pode permanecer em um estado pendente devido às seguintes condições:
  - O volume base que contém esta imagem instantânea é membro de um grupo de espelhos assíncrono.

- O volume base está atualmente em uma operação de sincronização. A criação da imagem instantânea é concluída assim que a operação de sincronização for concluída.

### Agendar imagens instantâneas

Você cria uma programação de snapshot para habilitar a recuperação em caso de problema com o volume base e executar backups programados. Snapshots de volumes base ou grupos de consistência de snapshot podem ser criados em uma programação diária, semanal ou mensal, a qualquer hora do dia.

#### Antes de começar

O volume de base deve ser ideal.

#### Sobre esta tarefa

Esta tarefa descreve como criar uma programação de instantâneos para um grupo de consistência de instantâneos existente ou volume base.

> Você também pode criar um agendamento de snapshot ao mesmo tempo em que cria uma imagem de snapshot de um volume base ou grupo de consistência de snapshot.

#### Passos

1. Execute uma das seguintes ações para criar uma programação de instantâneos:
   - Selecione **armazenamento › volumes**.

     Selecione o objeto (grupo de consistência de volume ou snapshot) para esta programação de instantâneos e, em seguida, selecione **Serviços de cópia › criar agendamento de instantâneos**.
   - Selecione **armazenamento › instantâneos**.

     Selecione a guia **horários** e clique em **criar**.
2. Selecione o objeto (grupo de consistência de volume ou snapshot) para essa programação de snapshot e clique em **Avançar**.

   A caixa de diálogo criar agendamento instantâneo é exibida.
3. Execute uma das seguintes ações:
   - **Use um agendamento previamente definido de outro objeto snapshot**.

     Certifique-se de que as opções avançadas são apresentadas. Clique em **Mostrar mais opções**. Clique em **Import Schedule**, selecione o objeto com a programação que deseja importar e clique em **Import**.
   - **Modificar as opções básicas ou avançadas**.

     No canto superior direito da caixa de diálogo, clique em **Mostrar mais opções** para exibir todas as opções e, em seguida, consulte a tabela a seguir.

**Detalhes do campo**

| Campo | Descrição |
| --- | --- |
| **Definições básicas** | Selecione dias |
| Selecione dias individuais da semana para imagens instantâneas. | Hora de início |
| Na lista suspensa, selecione uma nova hora de início para os instantâneos diários (as seleções são fornecidas em incrementos de meia hora). A hora de início é predefinida para meia hora à frente da hora atual. | Fuso horário |
| Na lista suspensa, selecione o fuso horário da matriz. | • Configurações avançadas* |
| Dia / mês | Escolha uma das seguintes opções:<br>• **Daily / Weekly** — Selecione dias individuais para instantâneos de sincronização. Você também pode selecionar a caixa de seleção **Selecionar todos os dias** no canto superior direito, se desejar uma programação diária.<br>• **Mensal / anual** — Selecione meses individuais para instantâneos de sincronização. No campo **no(s) dia(s)**, insira os dias do mês para que as sincronizações ocorram. As inscrições válidas são **1** a **31** e **Last**. Você pode separar vários dias com uma vírgula ou ponto e vírgula. Use um hífen para datas inclusivas. Por exemplo: 1,3,4,10-15,último. Você também pode selecionar a caixa de seleção **Selecionar todos os meses** no canto superior direito, se desejar um agendamento mensal. |
| Hora de início | Na lista suspensa, selecione uma nova hora de início para os instantâneos diários (as seleções são fornecidas em incrementos de meia hora). A hora de início é predefinida para meia hora à frente da hora atual. |
| Fuso horário | Na lista suspensa, selecione o fuso horário da matriz. |

| Campo | Descrição |
| --- | --- |
| Instantâneos por dia/hora entre instantâneos | Selecione o número de imagens instantâneas a criar por dia. Se selecionar mais de um, selecione também a hora entre as imagens instantâneas. Para várias imagens instantâneas, certifique-se de que tem capacidade reservada adequada. |
| Criar imagem instantânea agora? | Selecione esta caixa de verificação para criar uma imagem instantânea, além das imagens automáticas que está a programar. |
| Data de início/fim ou sem data de fim | Introduza a data de início para que as sincronizações comecem. Introduza também uma data de fim ou selecione **sem data de fim**. |

4. Execute uma das seguintes ações:
   - Se o objeto for um grupo de consistência de instantâneos, clique em **criar** para aceitar as configurações e criar a programação.
   - Se o objeto for um volume, clique em **Next** (seguinte) para alocar a capacidade reservada para as imagens instantâneas.

     A tabela de candidatos ao volume exibe apenas os candidatos que suportam a capacidade reservada especificada. A capacidade reservada é a capacidade alocada física usada para qualquer operação de serviço de cópia e objeto de storage. Não é diretamente legível pelo host.
5. Utilize a caixa de rotação para atribuir a capacidade reservada às imagens instantâneas. Execute uma das seguintes ações:
   - **Aceite as configurações padrão.**

     Utilize esta opção recomendada para alocar a capacidade reservada para as imagens instantâneas com as predefinições.
   - **Aloque suas próprias configurações de capacidade reservada para atender às suas necessidades de armazenamento de dados.**

     Se você alterar a configuração de capacidade reservada padrão, clique em **Atualizar candidatos** para atualizar a lista de candidatos para a capacidade reservada especificada.

     Alocar a capacidade reservada usando as seguintes diretrizes:
     - A configuração padrão para capacidade reservada é de 40% da capacidade do volume base. Normalmente, essa capacidade é suficiente.
     - A capacidade necessária varia, dependendo da frequência e do tamanho das gravações de e/S nos volumes e da quantidade e duração da coleção de imagens instantâneas.
6. Clique em **seguinte**.

   A caixa de diálogo Editar configurações é exibida.
7. Edite as configurações para a programação de instantâneos conforme necessário e clique em **Finish**.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| **Limite de imagem instantâneo** | Ativar eliminação automática de imagens instantâneas quando… |
| Mantenha a caixa de verificação selecionada se pretender que as imagens instantâneas sejam eliminadas automaticamente após o limite especificado; utilize a caixa de seleção para alterar o limite. Se desmarcar esta caixa de verificação, a criação de imagens instantâneas pára após 32 imagens. | • Configurações de capacidade reservada* |
| Alerta-me quando… | Use a caixa giratório para ajustar o ponto percentual no qual o sistema envia uma notificação de alerta quando a capacidade reservada para um agendamento estiver quase cheia.<br><br>Quando a capacidade reservada para o agendamento exceder o limite especificado, use o aviso prévio para aumentar a capacidade reservada ou excluir objetos desnecessários antes que o espaço restante se esgote. |
| Política de capacidade reservada completa | Escolha uma das seguintes políticas:<br><br>• **Limpar imagem instantânea mais antiga** — o sistema limpa automaticamente a imagem instantânea mais antiga, que libera a capacidade reservada da imagem instantânea para reutilização dentro do grupo de instantâneos.<br>• **Rejeitar gravações no volume base** — quando a capacidade reservada atinge sua porcentagem máxima definida, o sistema rejeita qualquer solicitação de gravação de e/S para o volume base que acionou o acesso à capacidade reservada. |

**Criar grupo de consistência de snapshot**

## Para garantir que você tenha cópias consistentes, você pode criar um conjunto de vários volumes chamado *snapshot consistency group*.

Este grupo permite-lhe criar imagens instantâneas de todos os volumes ao mesmo tempo para obter consistência. Cada volume que pertence a um grupo de consistência de snapshot é referido como um *volume de membro*. Quando você adiciona um volume a um grupo de consistência de snapshot, o sistema cria

automaticamente um novo grupo de snapshot que corresponde a esse volume de membro.

**Sobre esta tarefa**

A sequência de criação do grupo de consistência de instantâneos permite selecionar volumes de membros para o grupo e alocar capacidade para os volumes de membros.

O processo para criar um grupo de consistência de instantâneos é um procedimento de várias etapas.

#### Etapa 1: Adicionar membros ao grupo de consistência de snapshot

Selecione membros para especificar uma coleção de volumes que compõem o grupo de consistência de snapshot. Todas as ações executadas no grupo de consistência de snapshot se estendem uniformemente para os volumes de membros selecionados.

**Antes de começar**

Os volumes dos membros devem ser ótimos.

**Passos**

1. Selecione **armazenamento › instantâneos**.
2. Clique na guia **Snapshot Consistency Groups** (grupos de consistência de instantâneos).
3. Selecione **criar › Snapshot consistency group**.

   A caixa de diálogo criar grupo de consistência de instantâneo é exibida.

4. Selecione o(s) volume(s) a ser(em) adicionado(s) como volumes membros ao grupo de consistência de instantâneos.
5. Clique em **seguinte** e vá para Etapa 2: Reserva de capacidade para o grupo de consistência de snapshot.

#### Etapa 2: Reserva de capacidade para o grupo de consistência de snapshot

Associe a capacidade reservada ao grupo de consistência de snapshot. O System Manager sugere os volumes e a capacidade com base nas propriedades do grupo de consistência de snapshot. Pode aceitar a configuração de capacidade reservada recomendada ou personalizar o armazenamento alocado.

**Sobre esta tarefa**

Na caixa de diálogo capacidade de reserva, a tabela de candidatos ao volume exibe apenas os candidatos que suportam a capacidade reservada especificada. A capacidade reservada é a capacidade alocada física usada para qualquer operação de serviço de cópia e objeto de storage. Não é diretamente legível pelo host.

**Passos**

1. Use a caixa giratório para alocar a capacidade reservada para o grupo de consistência de snapshot. Execute uma das seguintes ações:
   - **Aceite as configurações padrão**.

     Use esta opção recomendada para alocar a capacidade reservada para cada volume de membro com as configurações padrão.

   - **Aloque suas próprias configurações de capacidade reservada para atender às suas necessidades de armazenamento de dados.**

     Alocar a capacidade reservada usando as diretrizes a seguir.

- A configuração padrão para capacidade reservada é de 40% da capacidade do volume base. Normalmente, essa capacidade é suficiente.
- A capacidade necessária varia, dependendo da frequência e do tamanho das gravações de e/S nos volumes e da quantidade e duração da coleção de imagens instantâneas.

2. **Opcional:** se você alterar a configuração de capacidade reservada padrão, clique em **Atualizar candidatos** para atualizar a lista de candidatos para a capacidade reservada especificada.
3. Clique em **seguinte** e vá para Etapa 3: Edite as configurações para o grupo de consistência de snapshot.

#### Etapa 3: Edite as configurações para o grupo de consistência de snapshot

Aceite ou escolha configurações de exclusão automática e limites de alerta de capacidade reservada para o grupo de consistência de snapshot.

**Sobre esta tarefa**

A sequência de criação do grupo de consistência de instantâneos permite selecionar volumes de membros para o grupo e alocar capacidade para os volumes de membros.

**Passos**

1. Aceite ou altere as configurações padrão para o grupo de consistência de snapshot, conforme apropriado.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| • Configurações do grupo de consistência do instantâneo* | Nome |
| Especifique o nome para o grupo de consistência de snapshot. | Ativar eliminação automática de imagens instantâneas quando… |
| Mantenha a caixa de verificação selecionada se pretender que as imagens instantâneas sejam eliminadas automaticamente após o limite especificado; utilize a caixa de seleção para alterar o limite. Se desmarcar esta caixa de verificação, a criação de imagens instantâneas pára após 32 imagens. | • Configurações de capacidade reservada* |
| Alerta-me quando… | Use a caixa giratório para ajustar o ponto percentual no qual o sistema envia uma notificação de alerta quando a capacidade reservada para um grupo de consistência de snapshot estiver quase cheia.<br><br>Quando a capacidade reservada para o grupo de consistência de snapshot exceder o limite especificado, use o aviso prévio para aumentar a capacidade reservada ou excluir objetos desnecessários antes que o espaço restante se esgote. |
| Política de capacidade reservada completa | Escolha uma das seguintes políticas:<br><br>• **Limpar imagem de snapshot mais antiga** — o sistema limpa automaticamente a imagem de snapshot mais antiga no grupo consistência de snapshot, que libera a capacidade reservada da imagem de snapshot para reutilização dentro do grupo.<br>• **Rejeitar gravações no volume base** — quando a capacidade reservada atinge sua porcentagem máxima definida, o sistema rejeita qualquer solicitação de gravação de e/S para o volume base que acionou o acesso à capacidade reservada. |

2. Depois de ficar satisfeito com a configuração do grupo de consistência de instantâneos, clique em **Finish**.

### Criar volume instantâneo

Você cria um volume de snapshot para fornecer acesso do host a uma imagem de snapshot de um volume ou grupo de consistência de snapshot. Você pode designar o volume do snapshot como somente leitura ou leitura-gravação.

#### Sobre esta tarefa

A sequência de criação de volume instantâneo permite criar um volume instantâneo a partir de uma imagem instantânea e fornece opções para alocar capacidade reservada se o volume for leitura/gravação. Um volume instantâneo pode ser designado como um dos seguintes:

- Um volume instantâneo somente leitura fornece um aplicativo host com acesso de leitura a uma cópia dos dados contidos na imagem instantânea, mas sem a capacidade de modificar a imagem instantânea. Um volume snapshot somente leitura não tem capacidade reservada associada.
- Um volume instantâneo de leitura e gravação fornece ao aplicativo host acesso de gravação a uma cópia dos dados contidos na imagem instantânea. Ele tem sua própria capacidade reservada que é usada para salvar quaisquer modificações subsequentes feitas pelo aplicativo host no volume base sem afetar a imagem de snapshot referenciada.

O processo para criar um volume instantâneo é um procedimento de várias etapas.

##### Etapa 1: Revise os membros para obter um volume instantâneo

Selecione uma imagem instantânea de um volume base ou um grupo de consistência de instantâneos. Se você selecionar uma imagem instantânea do grupo de consistência de instantâneos, os volumes membros do grupo de consistência de instantâneos serão exibidos para revisão.

#### Passos

1. Selecione **armazenamento › instantâneos**.
2. Selecione a guia **volumes instantâneos**.
3. Selecione **criar**.

   A caixa de diálogo criar volume instantâneo é exibida.

4. Selecione a imagem instantânea (volume ou grupo de consistência de instantâneos) que deseja converter em um volume instantâneo e clique em **Avançar**. Use uma entrada de texto no campo **filtro** para restringir a lista.

   Se a seleção foi para uma imagem instantânea de um grupo de consistência de instantâneos, a caixa de diálogo Membros de revisão será exibida.

   Na caixa de diálogo Review Members (Rever membros), reveja a lista de volumes selecionados para conversão em volumes instantâneos e, em seguida, clique em **Next** (seguinte).

5. Vá para Etapa 2: Atribuir volume instantâneo ao host.

##### Etapa 2: Atribuir volume instantâneo ao host

Selecione um host ou cluster de host específico para atribuí-lo ao volume de snapshot. Esta atribuição concede a um host ou cluster de host acesso ao volume de snapshot. Você pode optar por atribuir um host

mais tarde, se necessário.

**Antes de começar**

- Existem hosts ou clusters de host válidos na página hosts.
- Os identificadores de porta do host devem ter sido definidos para o host.
- Antes de criar um volume habilitado PARA DA, verifique se sua conexão de host planejada suporta o recurso Data Assurance (DA). Se qualquer uma das conexões de host nos controladores do storage array não suportar DA, os hosts associados não poderão acessar dados em volumes habilitados PARA DA.

**Sobre esta tarefa**

Ao atribuir volumes, tenha em mente estas diretrizes:

- O sistema operacional de um host pode ter limites específicos sobre quantos volumes o host pode acessar.
- Você pode definir uma atribuição de host para cada volume instantâneo no storage array.
- Os volumes atribuídos são compartilhados entre controladores no storage array.
- O mesmo número de unidade lógica (LUN) não pode ser usado duas vezes por um host ou um cluster de host para acessar um volume de snapshot. Você deve usar um LUN exclusivo.

> A atribuição de um volume a um host falhará se você tentar atribuir um volume a um cluster de host que esteja em conflito com uma atribuição estabelecida para um host no cluster de host.

**Passos**

1. Na caixa de diálogo **Assign to Host**, selecione o host ou cluster de host que você deseja atribuir ao novo volume. Se você quiser criar o volume sem atribuir um host, selecione **Assign later** na lista suspensa.
2. Selecione o modo de acesso. Escolha uma das seguintes opções:
   - **Leitura/gravação** — esta opção fornece ao host acesso de leitura/gravação ao volume instantâneo e requer capacidade reservada.
   - **Somente leitura** — esta opção fornece ao host acesso somente leitura ao volume instantâneo e não requer capacidade reservada.
3. Clique em **seguinte** e siga um destes procedimentos:
   - Se o volume do instantâneo for leitura/gravação, a caixa de diálogo capacidade de revisão será exibida. Vá para Etapa 3: Reserva de capacidade para um volume instantâneo.
   - Se o volume do instantâneo for somente leitura, a caixa de diálogo Editar prioridade será exibida. Vá para Etapa 4: Edite as configurações para um volume instantâneo.

#### Etapa 3: Reserva de capacidade para um volume instantâneo

Associar a capacidade reservada a um volume instantâneo de leitura/gravação. O System Manager sugere os volumes e a capacidade com base nas propriedades do volume base ou do grupo de consistência de snapshot. Pode aceitar a configuração de capacidade reservada recomendada ou personalizar o armazenamento alocado.

**Sobre esta tarefa**

Você pode aumentar ou diminuir a capacidade reservada para o volume de snapshot conforme necessário. Se você descobrir que a capacidade reservada do snapshot é maior do que o necessário, poderá reduzir o tamanho para liberar espaço necessário para outros volumes lógicos.

**Passos**

1. Use a caixa giratório para alocar a capacidade reservada para o volume instantâneo.

   A tabela volume Candidate exibe apenas os candidatos que suportam a capacidade reservada especificada.

   Execute uma das seguintes ações:

   - **Aceite as configurações padrão**.

     Utilize esta opção recomendada para alocar a capacidade reservada para o volume instantâneo com as predefinições.

   - **Aloque suas próprias configurações de capacidade reservada para atender às suas necessidades de armazenamento de dados**.

     Se você alterar a configuração de capacidade reservada padrão, clique em **Atualizar candidatos** para atualizar a lista de candidatos para a capacidade reservada especificada.

     Alocar a capacidade reservada usando as diretrizes a seguir.

     - A configuração padrão para capacidade reservada é de 40% da capacidade do volume base e, geralmente, essa capacidade é suficiente.
     - A capacidade necessária varia, dependendo da frequência e do tamanho das gravações de e/S nos volumes e da quantidade e duração da coleção de imagens instantâneas.

2. **Opcional:** se você estiver criando o volume instantâneo para um grupo de consistência de snapshot, a opção "alterar candidato" aparecerá na tabela candidatos de capacidade reservada. Clique em **Change candidate** para selecionar um candidato de capacidade reservada alternativa.
3. Clique em **seguinte** e vá para Etapa 4: Edite as configurações para um volume instantâneo.

#### Etapa 4: Edite as configurações para um volume instantâneo

Altere as configurações de um volume instantâneo, como nome, armazenamento em cache, limites de alerta de capacidade reservada, etc.

**Sobre esta tarefa**

Você pode adicionar o volume ao cache de disco de estado sólido (SSD) como uma maneira de melhorar o desempenho somente leitura. O cache SSD consiste em um conjunto de unidades SSD que você agrupa logicamente em sua matriz de armazenamento.

**Passos**

1. Aceite ou altere as definições do volume instantâneo, conforme adequado.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| • Configurações de volume instantâneo* | Nome |
| Especifique o nome do volume instantâneo. | Ativar cache SSD |
| Escolha essa opção para habilitar o armazenamento em cache somente leitura em SSDs. | • Configurações de capacidade reservada* |
| Alerta-me quando… | **Aparece apenas para um volume instantâneo de leitura/gravação**.<br><br>Use a caixa giratório para ajustar o ponto percentual no qual o sistema envia uma notificação de alerta quando a capacidade reservada para um grupo de instantâneos estiver quase cheia.<br><br>Quando a capacidade reservada para o grupo de instantâneos exceder o limite especificado, use o aviso prévio para aumentar a capacidade reservada ou excluir objetos desnecessários antes que o espaço restante se esgote. |

2. Reveja a configuração do volume instantâneo. Clique em **voltar** para fazer quaisquer alterações.
3. Quando estiver satisfeito com a configuração do volume do instantâneo, clique em **Finish**.

## Gerenciar programações de snapshot

### Altere as definições de uma programação de instantâneos

Para uma programação de instantâneos, pode alterar os tempos de recolha automática ou a frequência da recolha.

**Sobre esta tarefa**

Você pode importar configurações de um agendamento instantâneo existente ou modificar as configurações conforme necessário.

Como uma programação de instantâneos está associada a um grupo de instantâneos ou a um grupo de consistência de instantâneos, a capacidade reservada pode ser afetada por alterações nas configurações de agendamento.

**Passos**

1. Selecione **armazenamento › instantâneos**.
2. Clique na guia **horários**.

3. Selecione a programação de instantâneos que pretende alterar e, em seguida, clique em **Editar**.

   A caixa de diálogo Editar agendamento instantâneo é exibida.

4. Execute um dos seguintes procedimentos:
   - **Use um agendamento previamente definido de outro objeto snapshot** — clique em **Importar Agendamento**, selecione o objeto com o agendamento que deseja importar e clique em **Importar**.
   - **Editar as configurações de agendamento** — consulte os detalhes do campo abaixo.

     **Detalhes do campo**

| Definição | Descrição |
|---|---|
| Dia / mês | Escolha uma das seguintes opções:<br>• **Daily / Weekly** — Selecione dias individuais para instantâneos de sincronização. Você também pode selecionar a caixa de seleção **Selecionar todos os dias** no canto superior direito, se desejar uma programação diária.<br>• **Mensal / anual** — Selecione meses individuais para instantâneos de sincronização. No campo **no(s) dia(s)**, insira os dias do mês para que as sincronizações ocorram. As inscrições válidas são **1** a **31** e **Last**. Você pode separar vários dias com uma vírgula ou ponto e vírgula. Use um hífen para datas inclusivas. Por exemplo: 1,3,4,10-15,último. Você também pode selecionar a caixa de seleção **Selecionar todos os meses** no canto superior direito, se desejar um agendamento mensal. |
| Hora de início | Na lista suspensa, selecione uma nova hora de início para os instantâneos diários. As seleções são fornecidas em incrementos de meia hora. A hora de início é predefinida para meia hora à frente da hora atual. |
| Fuso horário | Na lista suspensa, selecione o fuso horário da matriz de armazenamento. |
| Instantâneos por dia<br><br>Tempo entre instantâneos | Selecione o número de imagens instantâneas a criar por dia.<br><br>Se selecionar mais de um, selecione também o tempo entre os pontos de restauro. Para vários pontos de restauração, verifique se você tem capacidade reservada adequada. |
| Data de início<br><br>Data de fim<br><br>Sem data de fim | Introduza a data de início para que as sincronizações comecem. Introduza também uma data de fim ou selecione **sem data de fim**. |

5. Clique em **Salvar**.

### Ativar e suspender a programação de instantâneos

Você pode suspender temporariamente a coleção programada de imagens instantâneas quando precisar conservar espaço de armazenamento. Esse método é mais eficiente do que excluir e recriar posteriormente o agendamento de instantâneos.

#### Sobre esta tarefa

O estado da programação de instantâneos permanece suspenso até que você use a opção **Activate** para retomar a atividade de snapshot agendada.

#### Passos

1. Selecione **armazenamento › instantâneos**.
2. Se ainda não for exibido, clique na guia **horários**.

   Os horários estão listados na página.

3. Selecione uma agenda de instantâneos ativa que pretende suspender e, em seguida, clique em **Ativar/suspender**.

   O estado da coluna Estado muda para **suspenso** e o agendamento de instantâneos interrompe a coleta de todas as imagens instantâneas.

4. Para retomar a recolha de imagens instantâneas, selecione a agenda de instantâneos suspensos que pretende retomar e, em seguida, clique em **Ativar/suspender**.

   O status da coluna Estado muda para **Ativo**.

### Eliminar agendamento de instantâneos

Se já não pretender recolher imagens de instantâneos, pode eliminar uma agenda de instantâneos existente.

#### Sobre esta tarefa

Quando elimina uma agenda de instantâneos, as imagens de instantâneos associadas não são eliminadas juntamente com esta. Se você acha que a coleção de imagens instantâneas pode ser retomada em algum momento, você deve suspender o agendamento de instantâneos em vez de excluí-lo.

#### Passos

1. Selecione **armazenamento › instantâneos**.
2. Clique na guia **horários**.
3. Selecione a programação de instantâneos que pretende eliminar e confirme a operação.

#### Resultados

O sistema remove todos os atributos de agendamento do volume base ou do grupo de consistência de snapshot.

## Gerir imagens instantâneas

### Ver definições de imagem instantânea

Você pode exibir as propriedades, o status, a capacidade reservada e os objetos associados atribuídos a cada imagem instantânea.

#### Sobre esta tarefa

Os objetos associados a uma imagem instantânea incluem o volume base ou o grupo de consistência de instantâneos para o qual esta imagem instantânea é um ponto de restauração, o grupo de instantâneos associado e quaisquer volumes de instantâneos criados a partir da imagem instantânea. Utilize as definições de instantâneos para determinar se pretende copiar ou converter a imagem instantânea.

#### Passos

1. Selecione **armazenamento › instantâneos**.
2. Clique no separador **Snapshot Images** (imagens instantâneas).
3. Selecione a imagem instantânea que você deseja exibir e clique em **Exibir configurações**.

   É apresentada a caixa de diálogo Definições de imagem instantânea.

4. Ver as definições da imagem instantânea.

### Iniciar reversão de imagem instantânea para um volume base

Você pode executar uma operação de reversão para alterar o conteúdo de um volume base para corresponder ao conteúdo que é salvo em uma imagem instantânea.

A operação de reversão não altera o conteúdo das imagens instantâneas associadas ao volume base.

#### Antes de começar

- A capacidade reservada suficiente está disponível para iniciar uma operação de reversão.
- A imagem instantânea selecionada é ideal e o volume selecionado é ideal.
- O volume selecionado não tem uma operação de reversão já em andamento.

#### Sobre esta tarefa

A sequência de início de reversão permite que você comece a reversão em uma imagem instantânea de um volume base, ao mesmo tempo em que fornece opções para adicionar capacidade de armazenamento. Não é possível iniciar mais de uma operação de reversão para um volume base de cada vez.

> O host pode acessar imediatamente o novo volume base revertido, mas o volume base existente não permite o acesso de leitura e gravação do host após o início da reversão. Você pode criar um snapshot do volume base antes de iniciar o rollback para preservar o volume base pré-rollback para recuperação.

#### Passos

1. Selecione **armazenamento › instantâneos**.
2. Selecione o separador **Snapshot Images** (imagens instantâneas).
3. Selecione a imagem de instantâneo e, em seguida, selecione **Reverter › Start**.

   A caixa de diálogo confirmar início de reversão é exibida.

4. **Opcional:** Selecione a opção para **aumentar a capacidade**, se necessário.

   A caixa de diálogo aumentar capacidade reservada é exibida.

   a. Utilize a caixa de rotação para ajustar a percentagem de capacidade.

      Se a capacidade livre não existir no pool ou grupo de volumes que contém o objeto de armazenamento selecionado e o storage de armazenamento tiver capacidade não atribuída, você poderá adicionar capacidade. Você pode criar um novo pool ou grupo de volumes e tentar novamente essa operação usando a nova capacidade livre nesse pool ou grupo de volumes.

   b. Clique em **aumentar**.

5. Confirme se deseja executar esta operação e clique em **Rollback**.

**Resultados**

O System Manager executa as seguintes ações:

- Restaura o volume com o conteúdo guardado na imagem instantânea selecionada.
- Torna os volumes revertidos imediatamente disponíveis para acesso ao host. Não é necessário esperar que a operação de reversão seja concluída.

**Depois de terminar**

Selecione **Home › View Operations in Progress** (Ver operações em curso) para ver o progresso da operação de reversão.

Se a operação de reversão não for bem-sucedida, a operação será interrompida. Você pode retomar a operação em pausa e, se ainda não tiver êxito, siga o procedimento Recovery Guru para corrigir o problema ou entre em Contato com o suporte técnico.

### Iniciar reversão de imagem instantânea para volumes de membros do grupo de consistência de instantâneos

Você pode executar uma operação de reversão para alterar o conteúdo dos volumes de membros do grupo de consistência de instantâneos para corresponder ao conteúdo que é salvo em uma imagem instantânea.

A operação de reversão não altera o conteúdo das imagens instantâneas associadas ao grupo de consistência de instantâneos.

**Antes de começar**

- A capacidade reservada suficiente está disponível para iniciar uma operação de reversão.
- A imagem instantânea selecionada é ideal e o volume selecionado é ideal.
- O volume selecionado não tem uma operação de reversão já em andamento.

**Sobre esta tarefa**

A sequência de início de reversão permite que você comece a reversão em uma imagem instantânea de um grupo de consistência de snapshot, ao mesmo tempo em que fornece opções para adicionar capacidade de armazenamento. Você não pode iniciar mais de uma operação de reversão para um grupo de consistência de snapshot de cada vez.

O host tem acesso imediato aos novos volumes revertidos, mas os volumes de membros existentes não permitem mais o acesso de leitura e gravação do host após o início da reversão. Você pode criar uma imagem instantânea dos volumes membros antes de iniciar o rollback para preservar os volumes base pré-rollback para fins de recuperação.

O processo para iniciar a reversão de uma imagem instantânea de um grupo de consistência de instantâneos é um procedimento de várias etapas.

#### Passo 1: Selecione membros

Você deve selecionar os volumes de membros a serem revertidos.

**Passos**

1. Selecione **armazenamento › instantâneos**.
2. Selecione o separador **Snapshot Images** (imagens instantâneas).
3. Selecione a imagem instantânea do grupo de consistência de instantâneos e, em seguida, selecione **Repor › Iniciar**.

   A caixa de diálogo Start Rollback (Iniciar reversão) é exibida.

4. Selecione o volume ou volumes do membro.
5. Clique em **seguinte** e siga um destes procedimentos:
   - Se algum dos volumes de membros selecionados estiver associado a mais de um objeto de capacidade reservada que armazena imagens instantâneas, a caixa de diálogo capacidade de revisão é exibida. Vá para Passo 2: Rever a capacidade.
   - Se nenhum dos volumes de membros selecionados estiver associado a mais de um objeto de capacidade reservada que armazena imagens instantâneas, a caixa de diálogo Editar prioridade será exibida. Vá para Passo 3: Editar prioridade.

#### Passo 2: Rever a capacidade

Se você selecionou volumes de membros associados a mais de um objeto de capacidade reservada, como um grupo de snapshot e um volume de capacidade reservada, poderá analisar e aumentar a capacidade reservada para o(s) volume(s) revertido(s).

**Passos**

1. Ao lado de qualquer volume de membro com capacidade reservada muito baixa (ou zero), clique no link **aumentar capacidade** na coluna **Editar**.

   A caixa de diálogo aumentar capacidade reservada é exibida.

2. Use a caixa giratório para ajustar a porcentagem de capacidade e clique em **aumentar**.

   Se a capacidade livre não existir no pool ou grupo de volumes que contém o objeto de armazenamento selecionado e o storage de armazenamento tiver capacidade não atribuída, você poderá adicionar capacidade. Você pode criar um novo pool ou grupo de volumes e tentar novamente essa operação usando a nova capacidade livre nesse pool ou grupo de volumes.

3. Clique em **seguinte** e vá para Passo 3: Editar prioridade.

   A caixa de diálogo Editar prioridade é exibida.

#### Passo 3: Editar prioridade

Você pode editar a prioridade da operação de reversão, se necessário.

**Sobre esta tarefa**

A prioridade de reversão determina quantos recursos do sistema são dedicados à operação de reversão à custa do desempenho do sistema.

**Passos**

1. Use o controle deslizante para ajustar a prioridade de reversão conforme necessário.
2. Confirme se deseja executar esta operação e clique em **Finish**.

**Resultados**

O System Manager executa as seguintes ações:

- Restaura os volumes dos membros do grupo de consistência de instantâneos com o conteúdo guardado na imagem de instantâneo selecionada.
- Torna os volumes revertidos imediatamente disponíveis para acesso ao host. Não é necessário esperar que a operação de reversão seja concluída.

**Depois de terminar**

Selecione **Home › View Operations in Progress** (Ver operações em curso) para ver o progresso da operação de reversão.

Se a operação de reversão não for bem-sucedida, a operação será interrompida. Você pode retomar a operação em pausa e, se ainda não tiver êxito, siga o procedimento Recovery Guru para corrigir o problema ou entre em Contato com o suporte técnico.

### Retomar a reversão da imagem instantânea

Se ocorrer um erro durante uma operação de reversão de imagem instantânea, a operação é pausada automaticamente. Você pode retomar uma operação de reversão que está em um estado de pausa.

**Passos**

1. Selecione **armazenamento › instantâneos**.
2. Clique no separador **Snapshot Images** (imagens instantâneas).
3. Realce a reversão pausada e, em seguida, selecione **Reverter › Resume**.

   A operação é retomada.

**Resultados**

O System Manager executa as seguintes ações:

- Se a operação de reversão for retomada com êxito, você poderá visualizar o andamento da operação de reversão na janela operações em andamento.
- Se a operação de reversão não for bem-sucedida, a operação será interrompida novamente. Você pode seguir o procedimento Recovery Guru para corrigir o problema ou entrar em Contato com o suporte técnico.

### Cancelar reversão de imagem instantânea

Você pode cancelar uma reversão ativa em andamento (cópia ativa de dados), uma reversão pendente (em uma fila pendente aguardando recursos para iniciar) ou uma reversão que tenha sido pausada devido a um erro.

#### Sobre esta tarefa

Quando você cancela uma operação de reversão em andamento, o volume base reverte para um estado inutilizável e aparece como falhou. Portanto, considere cancelar uma operação de reversão somente quando existirem opções de recuperação para restaurar o conteúdo do volume base.

> Se o grupo de instantâneos no qual a imagem instantânea reside tiver uma ou mais imagens instantâneas que foram eliminadas automaticamente, a imagem instantânea usada para a operação de reversão pode não estar disponível para futuros rollbacks.

#### Passos

1. Selecione **armazenamento › instantâneos**.
2. Clique no separador **Snapshot Images** (imagens instantâneas).
3. Selecione a reversão ativa ou pausada e, em seguida, selecione **Repor › Cancelar**.

   A caixa de diálogo confirmar Cancelar reversão é exibida.

4. Clique em **Yes** para confirmar.

#### Resultados

O System Manager pára a operação de reversão. O volume base é utilizável, mas pode ter dados inconsistentes ou não intactos.

#### Depois de terminar

Depois de cancelar uma operação de reversão, você deve executar uma das seguintes ações:

- Reinicializar o conteúdo do volume base.
- Execute uma nova operação de reversão para restaurar o volume base usando a mesma imagem de snapshot usada na operação Cancelar reversão ou uma imagem de snapshot diferente para executar a nova operação de reversão.

### Eliminar imagem instantânea

Elimina imagens de instantâneos para limpar a imagem de instantâneos mais antiga de um grupo de instantâneos ou de um grupo de consistência de instantâneos.

#### Sobre esta tarefa

Você pode excluir uma única imagem de snapshot ou excluir imagens de snapshot de grupos de consistência de snapshot que tenham o mesmo carimbo de data/hora de criação. Também pode eliminar imagens instantâneas de um grupo de instantâneos.

Não é possível excluir uma imagem instantânea se ela não for a imagem de snapshot mais antiga para o volume base associado ou grupo de consistência de snapshot.

#### Passos

1. Selecione **armazenamento › instantâneos**.
2. Clique no separador **Snapshot Images** (imagens instantâneas).
3. Selecione a imagem instantânea que pretende eliminar e confirme que pretende executar a operação.

   Se tiver selecionado uma imagem instantânea de um grupo de consistência de instantâneos, selecione cada volume de membro que pretende eliminar e confirme que pretende executar a operação.

4. Clique em **Excluir**.

**Resultados**

O System Manager executa as seguintes ações:

- Elimina a imagem instantânea da matriz de armazenamento.
- Libera a capacidade reservada para reutilização no grupo de snapshot ou no grupo de consistência de snapshot.
- Desativa todos os volumes instantâneos associados que existem para a imagem de instantâneo eliminada.
- A partir de uma exclusão de grupo de consistência de snapshot, move qualquer volume de membro associado à imagem de snapshot excluída para um estado parado.

## Gerenciar grupos de consistência de snapshot

### Adicionar volume de membro a um grupo de consistência de snapshot

Você pode adicionar um novo volume de membro a um grupo de consistência de snapshot existente. Quando você adiciona um novo volume de membro, você também deve reservar capacidade para o volume de membro.

**Antes de começar**

- O volume do membro deve ser ótimo.
- O grupo de consistência de snapshot deve ter menos do que o número máximo de volumes permitidos (conforme definido pela configuração).
- Cada volume de capacidade reservada deve ter as mesmas configurações de garantia de dados (DA) e segurança que o volume associado.

**Sobre esta tarefa**

É possível adicionar volumes padrão ou volumes finos ao grupo de consistência de snapshot. O volume base pode residir em um pool ou grupo de volumes.

**Passos**

1. Selecione **armazenamento › instantâneos**.
2. Selecione a guia **grupos de consistência de instantâneos**.

   A tabela é exibida e exibe todos os grupos de consistência de snapshot associados ao storage array.

3. Selecione o grupo de consistência de instantâneos que deseja modificar e clique em **Adicionar membros**.

   A caixa de diálogo Adicionar membros é exibida.

4. Selecione o(s) volume(s) de membro que pretende adicionar e clique em **seguinte**.

   É apresentado o passo de reserva da capacidade. A tabela volume Candidate exibe apenas os candidatos que suportam a capacidade reservada especificada.

5. Use a caixa giratório para alocar a capacidade reservada para o volume do membro. Execute uma das seguintes ações:
   - **Aceite as configurações padrão.**

     Use esta opção recomendada para alocar a capacidade reservada para o volume do membro com as configurações padrão.

   - **Aloque suas próprias configurações de capacidade reservada para atender às suas necessidades de armazenamento de dados.**

     Se você alterar a configuração de capacidade reservada padrão, clique em **Atualizar candidatos** para atualizar a lista de candidatos para a capacidade reservada especificada.

     Alocar a capacidade reservada usando as diretrizes a seguir.

     - A configuração padrão para capacidade reservada é de 40% da capacidade do volume base e, geralmente, essa capacidade é suficiente.
     - A capacidade necessária varia, dependendo da frequência e do tamanho das gravações de e/S nos volumes e da quantidade e duração da coleção de imagens instantâneas.
6. Clique em **Finish** para adicionar os volumes de membros.

#### Remover um volume de membro de um grupo de consistência de snapshot

## Você pode remover um volume de membro de um grupo de consistência de snapshot existente.

#### Sobre esta tarefa

Quando você remove um volume de membro de um grupo de consistência de snapshot, o System Manager exclui automaticamente os objetos de snapshot associados a esse volume de membro.

#### Passos

1. Selecione **armazenamento › instantâneos**.
2. Clique na guia **Snapshot Consistency Groups** (grupos de consistência de instantâneos).
3. Expanda o grupo de consistência de snapshot que você deseja modificar selecionando o sinal de mais ao lado dele.
4. Selecione o volume do membro que deseja remover e clique em **Remover**.
5. Confirme se deseja executar a operação e clique em **Remover**.

#### Resultados

O System Manager executa as seguintes ações:

- Elimina todas as imagens instantâneas e volumes instantâneos associados ao volume membro.
- Exclui o grupo instantâneo associado ao volume do membro.
- O volume do membro não é alterado ou eliminado de outra forma.

### Altere as configurações de um grupo de consistência de snapshot

Altere as definições de um grupo de consistência de instantâneos quando pretender alterar o seu nome, as definições de eliminação automática ou o número máximo de imagens instantâneas permitidas.

**Passos**

1. Selecione **armazenamento › instantâneos**.
2. Clique na guia **Snapshot Consistency Groups** (grupos de consistência de instantâneos).
3. Selecione o grupo de consistência de instantâneos que você deseja editar e clique em **Exibir/Editar configurações**.

   A caixa de diálogo Definição do grupo de consistência de instantâneo é exibida.

4. Altere as configurações do grupo de consistência de instantâneos conforme apropriado.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| • Configurações do grupo de consistência do instantâneo* | Nome |
| Você pode alterar o nome do grupo de consistência de snapshot. | Eliminação automática |
| Mantenha a caixa de verificação selecionada se pretender que as imagens instantâneas sejam eliminadas automaticamente após o limite especificado; utilize a caixa de seleção para alterar o limite. Se desmarcar esta caixa de verificação, a criação de imagens instantâneas pára após 32 imagens. | Limite de imagem instantânea |
| Pode alterar o número máximo de imagens instantâneas permitidas para um grupo de instantâneos. | Agendamento do Snapshot |
| Este campo indica se uma programação está associada ao grupo de consistência de instantâneos. | **Objetos associados** |
| Volumes dos membros | É possível exibir a quantidade de volumes de membros associados ao grupo de consistência de snapshot. |

5. Clique em **Salvar**.

### Eliminar grupo de consistência de instantâneos

Você pode excluir grupos de consistência de snapshot que não são mais necessários.

**Antes de começar**

Confirme se as imagens de todos os volumes de membros não são mais necessárias para fins de backup ou teste.

**Sobre esta tarefa**

Esta operação elimina todas as imagens instantâneas ou programações associadas ao grupo de consistência de instantâneos.

**Passos**

1. Selecione **armazenamento › instantâneos**.
2. Selecione a guia **grupos de consistência de instantâneos**.
3. Selecione o grupo de consistência de instantâneos que deseja excluir e, em seguida, selecione **tarefas incomuns › Excluir**.

   A caixa de diálogo Confirm Delete Snapshot consistency Group (confirmar Grupo de consistência de instantâneos)

4. Confirme se deseja executar esta operação e clique em **Excluir**.

**Resultados**

O System Manager executa as seguintes ações:

- Elimina todas as imagens instantâneas e volumes instantâneos existentes do grupo de consistência de instantâneos.
- Elimina todas as imagens de instantâneos associadas existentes para cada volume de membro no grupo de consistência de instantâneos.
- Exclui todos os volumes de snapshot associados que existem para cada volume de membro no grupo de consistência de snapshot.
- Exclui toda a capacidade reservada associada para cada volume de membro no grupo de consistência de instantâneos (se selecionado).

## Gerenciar volumes de snapshot

### Converta o volume instantâneo para o modo de leitura-gravação

Você pode converter um volume de snapshot somente leitura ou um volume de snapshot de grupo de consistência de snapshot para o modo leitura-gravação, se necessário.

Um volume de snapshot que é convertido para leitura-gravação acessível contém sua própria capacidade reservada. Essa capacidade é usada para salvar quaisquer modificações subsequentes feitas pelo aplicativo host no volume base sem afetar a imagem de snapshot referenciada.

**Passos**

1. Selecione **armazenamento › instantâneos**.
2. Selecione a guia **volumes instantâneos**.

   A tabela volumes de Snapshot é exibida e exibe todos os volumes de snapshot associados ao storage array.

3. Selecione o volume instantâneo somente leitura que deseja converter e clique em **Converter para**

**ler/escrever**.

A caixa de diálogo Converter para ler/escrever é exibida com a etapa **reserva de capacidade** ativada. A tabela volume Candidate exibe apenas os candidatos que suportam a capacidade reservada especificada.

4. Para alocar a capacidade reservada para o volume de snapshot de leitura e gravação, execute uma das seguintes ações:
   - **Accept the default settings** — Use esta opção recomendada para alocar a capacidade reservada para o volume instantâneo com as configurações padrão.
   - **Aloque suas próprias configurações de capacidade reservada para atender às suas necessidades de armazenamento de dados** — aloque a capacidade reservada usando as seguintes diretrizes.
     - A configuração padrão para capacidade reservada é de 40% da capacidade do volume base e, geralmente, essa capacidade é suficiente.
     - A capacidade necessária varia, dependendo da frequência e do tamanho das gravações de e/S no volume.
5. Selecione **seguinte** para rever ou editar as definições.

   A caixa de diálogo Editar configurações é exibida.

6. Aceite ou especifique as configurações do volume instantâneo conforme apropriado e selecione **Finish** para converter o volume instantâneo.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| • Configurações de capacidade reservada* | Alerta-me quando… |

### Alterar as definições de volume de um volume instantâneo

Você pode alterar as configurações de um volume instantâneo ou volume instantâneo do grupo de consistência de snapshot para renomeá-lo, ativar ou desativar o cache SSD ou alterar a atribuição do host, cluster de host ou número de unidade lógica (LUN).

**Passos**

1. Selecione **armazenamento › instantâneos**.
2. Clique na guia **volumes instantâneos**.
3. Selecione o volume instantâneo que deseja alterar e clique em **Exibir/Editar configurações**.

   A caixa de diálogo Configurações de volume instantâneo é exibida.

4. Veja ou edite as definições do volume instantâneo, conforme apropriado.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| **Volume instantâneo** | Nome |
| Pode alterar o nome do volume instantâneo. | Atribuído a |
| Você pode alterar a atribuição de cluster de host ou host para o volume de snapshot. | LUN |
| Pode alterar a atribuição LUN para o volume instantâneo. | Cache SSD |
| Você pode ativar/desativar o armazenamento em cache somente leitura em discos de estado sólido (SSDs). | **Objetos associados** |
| Imagem instantânea | Pode visualizar as imagens instantâneas associadas ao volume instantâneo. Uma imagem instantânea é uma cópia lógica dos dados de volume, capturados em um determinado ponto no tempo. Como um ponto de restauração, as imagens instantâneas permitem que você role de volta para um conjunto de dados em boas condições. Embora o host possa acessar a imagem instantânea, ele não pode ler ou gravar diretamente nela. |
| Volume base | É possível exibir o volume base associado ao volume instantâneo. Um volume base é a origem a partir da qual uma imagem instantânea é criada. Pode ser um volume grosso ou fino e é normalmente atribuído a um host. O volume base pode residir em um grupo de volumes ou em um pool de discos. |
| Grupo de instantâneos | Você pode exibir o grupo de snapshot associado ao volume de snapshot. Um grupo de instantâneos é uma coleção de imagens instantâneas a partir de um único volume base. |

### Copiar volume instantâneo

Você pode executar um processo de volume de cópia em um volume instantâneo ou em um volume instantâneo de grupo de consistência de snapshot.

**Sobre esta tarefa**

Você pode copiar um volume instantâneo para o volume de destino, conforme executado em uma operação normal de volume de cópia. No entanto, os volumes instantâneos não podem permanecer online durante o processo de volume de cópia.

**Passos**

1. Selecione **armazenamento › instantâneos**.
2. Selecione a guia **volumes instantâneos**.

   A tabela volumes de Snapshot é exibida e exibe todos os volumes de snapshot associados ao storage array.

3. Selecione o volume instantâneo que pretende copiar e, em seguida, selecione **volume de cópia**.

   A caixa de diálogo volume de cópia é exibida, solicitando que você selecione um destino.

4. Selecione o volume de destino a ser utilizado como destino da cópia e, em seguida, clique em **Finish**.

### Recriar o volume instantâneo

Você pode criar novamente um volume instantâneo ou um volume instantâneo do grupo de consistência de snapshot que você desativou anteriormente. A recriação de um volume instantâneo demora menos tempo do que a criação de um novo.

**Antes de começar**

- O volume instantâneo deve estar no estado ideal ou Desativado.
- Todos os volumes instantâneos de membros devem estar em um estado Desativado antes de poder recriar o volume instantâneo do grupo de consistência de instantâneos.

**Sobre esta tarefa**

Não é possível recriar um volume de instantâneo individual de membro; você pode recriar apenas o volume de instantâneo geral do grupo de consistência de instantâneo.

> Se o volume instantâneo do volume do instantâneo ou do grupo de consistência do instantâneo fizer parte de uma relação de cópia online, não poderá efetuar a opção recriar no volume.

**Passos**

1. Selecione **armazenamento › instantâneos**.
2. Selecione a guia **volumes instantâneos**.

   A tabela volumes de Snapshot é exibida e exibe todos os volumes de snapshot associados ao storage array.

3. Selecione o volume instantâneo que pretende recriar e, em seguida, selecione **tarefas incomuns › recriar**.

   A caixa de diálogo recriar volume instantâneo é exibida.

4. Selecione uma das seguintes opções:
   - **Uma imagem instantânea existente criada a partir do volume <name>**

     Selecione esta opção para indicar uma imagem instantânea existente a partir da qual pretende recriar

o volume instantâneo.

- **Uma nova imagem instantânea do volume <name>**

  Selecione esta opção para criar uma nova imagem instantânea a partir da qual recriar o volume instantâneo.

5. Clique em **recriar**.

**Resultados**

O System Manager executa as seguintes ações:

- Exclui todos `write` os dados em qualquer volume de repositório instantâneo associado.
- Os parâmetros do volume instantâneo do volume do instantâneo do grupo de consistência do instantâneo permanecem os mesmos que os parâmetros de volume anteriormente desativados.
- Retém os nomes originais do volume instantâneo ou do volume instantâneo do grupo de consistência de instantâneos.

### Desativar volume instantâneo

Você pode desabilitar um volume instantâneo ou um volume instantâneo em um grupo de consistência de snapshot quando não precisar mais dele ou desejar parar temporariamente de usá-lo.

**Sobre esta tarefa**

Utilize a opção Desativar se uma destas condições se aplicar:

- Você terminou com o volume instantâneo ou o volume instantâneo do grupo de consistência de snapshot por enquanto.
- Você pretende recriar o volume instantâneo ou o volume instantâneo do grupo de consistência de instantâneo (que é designado como leitura-gravação) posteriormente e deseja manter a capacidade reservada associada para que você não precise criá-lo novamente.
- Você deseja aumentar a performance do storage array interrompendo a atividade de gravação em um volume de snapshot de leitura e gravação.

Se o volume instantâneo do grupo de consistência de snapshot for designado como leitura-gravação, essa opção também permitirá que você interrompa qualquer atividade de gravação adicional no volume de capacidade reservada associado. Se decidir recriar o volume instantâneo ou o volume instantâneo do grupo de consistência de instantâneos, terá de escolher uma imagem instantânea a partir do mesmo volume base.

Se o volume instantâneo do volume do instantâneo ou do grupo de consistência do instantâneo fizer parte de uma relação de cópia online, não poderá efetuar a opção Desativar no volume.

**Passos**

1. Selecione **armazenamento › instantâneos**.
2. Selecione a guia **volumes instantâneos**.

   O System Manager exibe todos os volumes instantâneos associados ao storage array.

3. Selecione o volume instantâneo que pretende desativar e, em seguida, selecione **tarefas incomuns › Desativar**.

4. Confirme se deseja executar a operação e clique em **Desativar**.

**Resultados**

- O volume do Snapshot permanece associado ao volume base.
- O volume do instantâneo mantém seu nome mundial (WWN).
- Se a leitura-gravação for lida, o volume do Snapshot manterá sua capacidade reservada associada.
- O volume de snapshot retém todas as atribuições e acessos do host. No entanto, as solicitações de leitura e gravação falham.
- O volume instantâneo perde a sua associação com a sua imagem instantânea.

### Eliminar volume instantâneo

Você pode excluir um volume instantâneo ou um volume instantâneo de grupo de consistência de snapshot que não seja mais necessário para fins de teste de aplicativos de backup ou software.

Você também pode especificar se deseja excluir o volume de capacidade reservada de snapshot associado a um volume instantâneo `read-write` ou reter o volume de capacidade reservada de snapshot como um volume não atribuído.

**Sobre esta tarefa**

A exclusão de um volume base exclui automaticamente qualquer volume instantâneo associado ou volume instantâneo de grupo de consistência. Não é possível excluir um volume instantâneo que esteja em uma cópia de volume com o status **em andamento**.

**Passos**

1. Selecione **armazenamento › instantâneos**.
2. Selecione a guia **volumes instantâneos**.

   O System Manager exibe todos os volumes instantâneos associados ao storage array.

3. Selecione o volume instantâneo que pretende eliminar e, em seguida, selecione **tarefas pouco comuns › Eliminar**.
4. Confirme se deseja executar a operação e clique em **Excluir**.

**Resultados**

O System Manager executa as seguintes ações:

- Exclui todos os volumes de snapshot de membros (para um volume de snapshot de um grupo de consistência de snapshot).
- Remove todas as atribuições de host associadas.

## FAQs

### Por que não vejo todos os meus volumes, hosts ou clusters de host?

Os volumes instantâneos com um volume base habilitado PARA DA não são elegíveis para serem atribuídos a um host que não seja capaz de Data Assurance (DA). Você deve desativar DA no volume base antes que um volume instantâneo possa ser atribuído

a um host que não seja capaz de DA.

Considere as seguintes diretrizes para o host ao qual você está atribuindo o volume de snapshot:

- Um host não é capaz de DA se ele estiver conetado ao storage array por meio de uma interface de e/S que não seja capaz de DA.
- Um cluster de host não é capaz de DA se tiver pelo menos um membro de host que não seja capaz de DA.

> Não é possível desativar DA em um volume associado a snapshots (grupos de consistência, grupos de snapshot, imagens de snapshot e volumes de snapshot), cópias de volume e espelhos. Todos os objetos snapshot e capacidade reservada associados devem ser excluídos antes que DA possa ser desabilitada no volume base.

**O que é uma imagem instantânea?**

Uma imagem instantânea é uma cópia lógica do conteúdo do volume, capturada em um determinado ponto no tempo. As imagens instantâneas usam espaço de armazenamento mínimo.

Os dados de imagem instantânea são armazenados da seguinte forma:

- Quando uma imagem instantânea é criada, ela corresponde exatamente ao volume base. Depois que o snapshot é capturado, quando a primeira solicitação de gravação ocorre para qualquer bloco ou conjunto de blocos no volume base, os dados originais são copiados para a capacidade reservada do snapshot antes que os novos dados sejam gravados no volume base.
- Os instantâneos subsequentes incluem apenas blocos de dados que foram alterados desde que a primeira imagem instantânea foi criada. Cada operação de cópia em gravação subsequente salva os dados originais que estão prestes a ser sobrescritos no volume base para a capacidade reservada do snapshot antes que os novos dados sejam gravados no volume base.

**Por que usar imagens instantâneas?**

Você pode usar snapshots para proteger e permitir a recuperação de perda acidental ou maliciosa ou corrupção de dados.

Selecione um volume base ou um grupo de volumes base, chamado de grupo de consistência de instantâneos e, em seguida, capture imagens de instantâneos de uma ou mais das seguintes formas:

- Você pode criar uma imagem instantânea de um único volume base ou de um grupo de consistência de snapshot que consiste em vários volumes base.
- Você pode tirar snapshots manualmente ou criar uma programação para um volume base ou grupo de consistência de snapshot para capturar automaticamente imagens instantâneas periódicas.
- Você pode criar um volume instantâneo acessível pelo host de uma imagem instantânea.
- Você pode executar uma operação de reversão para restaurar uma imagem instantânea.

O sistema retém várias imagens instantâneas como pontos de restauração que você pode usar para reverter para conjuntos de dados em boas condições em pontos específicos no tempo. A capacidade de reverter fornece proteção contra exclusão acidental de dados e corrupção de dados.

#### Que tipos de volumes podem ser usados para instantâneos?

Volumes padrão e volumes finos são os únicos tipos de volumes que podem ser usados para armazenar imagens instantâneas. Não é possível utilizar volumes não standard. O volume base pode residir em um pool ou grupo de volumes.

#### Por que eu criaria um grupo de consistência de snapshot?

Você cria um grupo de consistência de instantâneos quando deseja garantir que as imagens instantâneas sejam tiradas em vários volumes ao mesmo tempo.

Por exemplo, um banco de dados composto por vários volumes que precisam permanecer consistentes para fins de recuperação exigiria que um grupo de consistência de snapshot coletasse snapshots coordenados de todos os volumes e os usasse para restaurar todo o banco de dados.

Os volumes incluídos em um grupo de consistência de snapshot são chamados *volumes de membros*.

Você pode executar as seguintes operações de snapshot em um grupo de consistência de snapshot:

- Crie uma imagem instantânea de um grupo de consistência de instantâneos para obter imagens simultâneas dos volumes de membros.
- Crie uma programação para que o grupo de consistência de instantâneos capture automaticamente imagens simultâneas periódicas dos volumes de membros.
- Crie um volume instantâneo acessível ao host de uma imagem de grupo de consistência de snapshot.
- Execute uma operação de reversão para um grupo de consistência de snapshot.

#### O que é um volume snapshot e quando ele precisa de capacidade reservada?

Um volume instantâneo permite que o host acesse dados na imagem instantânea. O volume instantâneo contém a sua própria capacidade reservada, que guarda quaisquer modificações no volume base sem afetar a imagem instantânea original. As imagens instantâneas não são acessíveis para leitura ou gravação para os hosts. Se você quiser ler ou gravar dados de snapshot, crie um volume de snapshot e atribua-o a um host.

Você pode criar dois tipos de volumes de snapshot. O tipo de volume instantâneo determina se ele usa a capacidade reservada.

- **Somente leitura** — Um volume instantâneo criado como somente leitura fornece um aplicativo host com acesso de leitura a uma cópia dos dados contidos na imagem instantânea. Um volume snapshot somente leitura não usa a capacidade reservada.
- **Read-write** — Um volume instantâneo que é criado como read-write permite que você faça alterações no volume instantâneo sem afetar a imagem de snapshot referenciada. Um volume instantâneo de leitura e gravação usa a capacidade reservada para armazenar essas alterações. Você pode converter um volume instantâneo somente leitura para leitura e gravação a qualquer momento.

#### O que é um grupo de instantâneos?

Um grupo de instantâneos é uma coleção de imagens instantâneas pontuais de um único volume base associado.

O System Manager organiza imagens instantâneas em *grupos de instantâneos*. Os grupos de snapshot não exigem nenhuma ação do usuário, mas você pode ajustar a capacidade reservada em um grupo de snapshot a qualquer momento. Além disso, você pode ser solicitado a criar capacidade reservada quando as seguintes condições forem atendidas:

- Sempre que você tirar um snapshot de um volume base que ainda não tenha um grupo de snapshot, o System Manager cria automaticamente um grupo de snapshot. Isso cria capacidade reservada para o volume base que é usado para armazenar imagens instantâneas subsequentes.
- Sempre que você criar uma programação de snapshot para um volume base, o System Manager cria automaticamente um grupo de snapshot.

**Por que eu desabilitaria um volume de snapshot?**

Desativa um volume instantâneo quando pretende atribuir um volume instantâneo diferente à imagem instantânea. Pode reservar o volume instantâneo desativado para utilização posterior.

Se você não precisar mais do volume instantâneo ou do volume instantâneo do grupo de consistência e não pretender recriá-lo posteriormente, exclua o volume em vez de desativá-lo.

**Qual é o estado Desativado?**

Um volume instantâneo no estado Disabled (Desativado) não está atualmente atribuído a uma imagem instantânea. Para ativar o volume instantâneo, tem de utilizar a operação de recriação para atribuir uma nova imagem instantânea ao volume instantâneo desativado.

As caraterísticas do volume instantâneo são definidas pela imagem instantânea atribuída a ele. A atividade de leitura e gravação é suspensa em um volume instantâneo no status Desativado.

**Por que eu suspenderia uma programação de instantâneos?**

Quando um agendamento é suspenso, as criações de imagem instantânea programadas não ocorrem. Você pode pausar uma programação de snapshot para economizar espaço de armazenamento e, em seguida, retomar os snapshots programados posteriormente.

Se você não precisar da programação de instantâneos, você deve excluir a programação em vez de suspendê-la.

# Espelhamento

## Visão geral

**Visão geral do espelhamento assíncrono**

O recurso espelhamento assíncrono fornece um mecanismo baseado em firmware em nível de controlador para replicação de dados entre um storage array local e um storage array remoto.

#### O que é espelhamento assíncrono?

*Espelhamento assíncrono* captura o estado do volume primário em um determinado momento no tempo e copia apenas os dados que foram alterados desde a última captura de imagem. O site principal pode ser atualizado imediatamente e o site secundário pode ser atualizado como a largura de banda permite. As informações são armazenadas em cache e enviadas posteriormente, à medida que os recursos de rede ficam disponíveis.

O espelhamento assíncrono é criado por volume, mas gerenciado em um nível de grupo, permitindo que você associe um volume espelhado remoto distinto a qualquer volume primário em um determinado storage array. Esse tipo de espelhamento é ideal para satisfazer a demanda por operações ininterruptas e, em geral, é muito mais eficiente em rede para processos periódicos.

Saiba mais:

- "Como o espelhamento assíncrono funciona"
- "Terminologia de espelhamento assíncrono"
- "Estado do espelho assíncrono"
- "Propriedade do volume"
- "Mudança de papel de um grupo de consistência de espelho"

#### Como faço para configurar o espelhamento assíncrono?

Você deve usar a interface do Unified Manager para executar a configuração de espelhamento inicial entre os arrays. Uma vez configurado, você pode gerenciar pares espelhados e grupos de consistência no System Manager.

Saiba mais:

- "Requisitos para uso do espelhamento assíncrono"
- "Fluxo de trabalho para espelhar um volume de forma assíncrona"
- "Criar par espelhado assíncrono (no Unified Manager)"

#### Informações relacionadas

Saiba mais sobre conceitos relacionados ao espelhamento assíncrono:

- "O que você precisa saber antes de criar um grupo de consistência de espelho"
- "O que você precisa saber antes de criar um par espelhado"
- "Como o espelhamento assíncrono difere do espelhamento síncrono"

### Visão geral do espelhamento síncrono

O recurso de espelhamento síncrono oferece replicação de dados on-line em tempo real entre storage arrays em uma distância remota.

Este recurso não está disponível no sistema de armazenamento EF600 ou EF300.

#### O que é espelhamento síncrono?

O *espelhamento síncrono* replica volumes de dados em tempo real para garantir disponibilidade contínua. Os controladores de storage array gerenciam a operação de espelhamento, que é transparente para máquinas host e aplicações de software.

Esse tipo de espelhamento é ideal para fins de continuidade dos negócios, como recuperação de desastres.

Saiba mais:

- "Como o espelhamento síncrono funciona"
- "Terminologia de espelhamento síncrono"
- "Status do espelhamento síncrono"
- "Propriedade do volume"
- "Mudança de função entre volumes em um par espelhado"

#### Como faço para configurar o espelhamento síncrono?

Você deve usar a interface do Unified Manager para executar a configuração de espelhamento inicial entre os arrays. Uma vez configurado, você pode gerenciar pares espelhados no System Manager.

Saiba mais:

- "Requisitos para o uso do espelhamento síncrono"
- "Fluxo de trabalho para espelhar um volume de forma síncrona"
- "Criar par espelhado síncrono (no Unified Manager)"

#### Informações relacionadas

Saiba mais sobre conceitos relacionados ao espelhamento síncrono:

- "O que você precisa saber antes de criar um par espelhado"
- "Como o espelhamento assíncrono difere do espelhamento síncrono"

## Conceitos assíncronos

### Como o espelhamento assíncrono funciona

O espelhamento assíncrono copia volumes de dados sob demanda ou de acordo com o cronograma, o que minimiza ou evita o tempo de inatividade que pode resultar de corrupção ou perda de dados.

O espelhamento assíncrono captura o estado do volume primário em um determinado momento no tempo e copia apenas os dados que foram alterados desde a última captura de imagem. O site principal pode ser atualizado imediatamente e o site secundário pode ser atualizado como a largura de banda permite. As informações são armazenadas em cache e enviadas posteriormente, à medida que os recursos de rede ficam disponíveis.

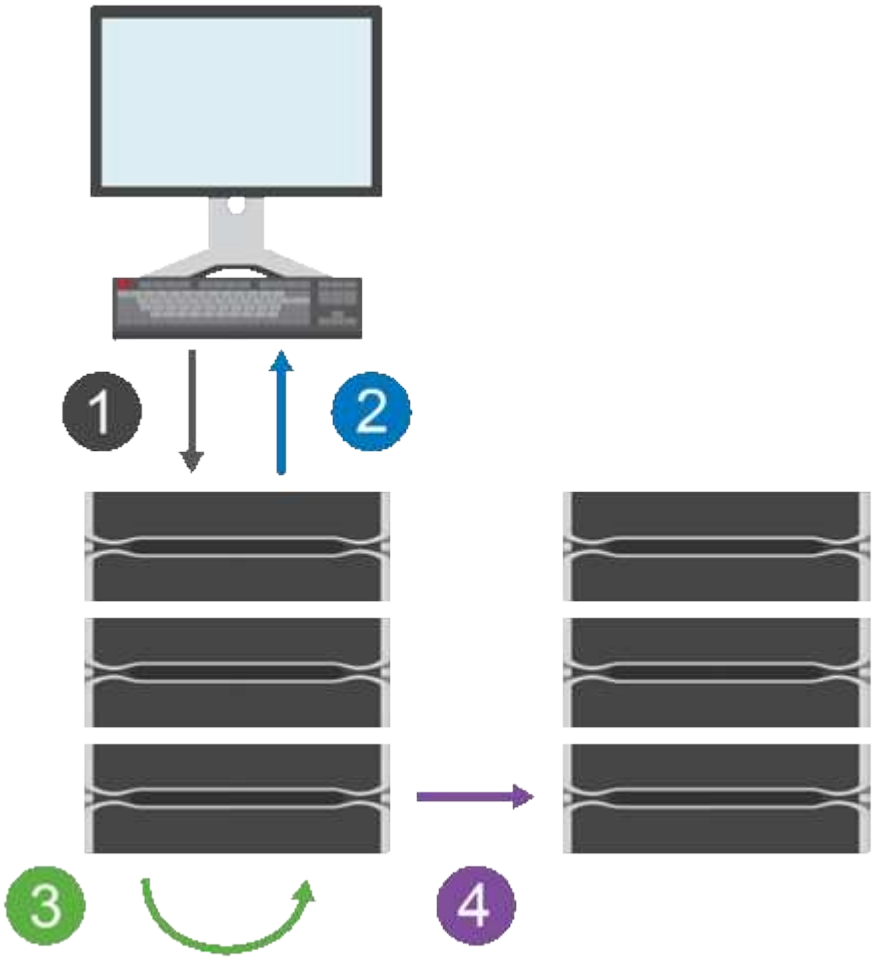
Esse tipo de espelhamento é ideal para atender a demanda por operações ininterruptas e, em geral, é muito mais eficiente em rede para processos periódicos, como backup e arquivamento. Os motivos para usar o espelhamento assíncrono incluem o seguinte:

- Consolidação remota de backup.
- Proteja-se contra desastres locais ou em áreas amplas.
- Desenvolvimento e teste de aplicativos em uma imagem pontual de dados ao vivo.

#### Sessão de espelhamento assíncrono

O espelhamento assíncrono captura o estado do volume primário em um determinado momento no tempo e copia apenas os dados que foram alterados desde a última captura de imagem. O espelhamento assíncrono permite que o site primário seja atualizado imediatamente e o site secundário seja atualizado conforme a largura de banda o permita. As informações são armazenadas em cache e enviadas posteriormente, à medida que os recursos de rede ficam disponíveis.

Há quatro etapas principais em uma sessão de espelhamento assíncrono ativo.




1. Uma operação de gravação ocorre primeiro no storage array do volume primário.
2. O status da operação é retornado ao host.
3. Todas as alterações no volume primário são registadas e monitorizadas.
4. Todas as alterações são enviadas para a matriz de armazenamento do volume secundário como um processo em segundo plano.

Estes passos são repetidos de acordo com os intervalos de sincronização definidos ou os passos podem ser repetidos manualmente se não forem definidos intervalos.

O espelhamento assíncrono transfere dados para o local remoto apenas em intervalos definidos, para que a e/S local não seja afetada quase tanto por conexões de rede lentas. Como essa transferência não está vinculada à e/S local, ela não afeta o desempenho do aplicativo. Portanto, o espelhamento assíncrono pode usar conexões mais lentas, como iSCSI, e executar em distâncias maiores entre os sistemas de armazenamento local e remoto.

Os storage arrays devem ter uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)

#### Grupos de consistência espelhada e pares espelhados

Você cria um grupo de consistência de espelho para estabelecer a relação de espelhamento entre o storage array local e o storage array remoto. A relação de espelhamento assíncrono consiste em um par espelhado: Um volume primário em um storage array e um volume secundário em outro storage array.

O storage array que contém o volume primário geralmente está localizado no local principal e serve os hosts ativos. O storage array que contém o volume secundário geralmente fica em um local secundário e contém uma réplica dos dados. O volume secundário normalmente contém uma cópia de backup dos dados e é usado para recuperação de desastres.

#### Definições de sincronização

Ao criar um par espelhado, você também define a prioridade de sincronização e a política de ressincronização que o par espelhado usa para concluir a operação de ressincronização após uma interrupção de comunicação.

Ao criar um grupo de consistência de espelho, você também define a prioridade de sincronização e a política de ressincronização para todos os pares espelhados dentro do grupo. Os pares espelhados usam a política de prioridade de sincronização e ressincronização para concluir a operação de ressincronização após uma interrupção de comunicação.

Os volumes primário e secundário em um par espelhado podem ficar não sincronizados quando o storage array do volume primário não consegue gravar dados no volume secundário. Esta condição pode ser causada pelos seguintes problemas:

- Problemas de rede entre os storages de armazenamento local e remoto.
- Um volume secundário com falha.
- Sincronização sendo suspensa manualmente no par espelhado.
- Conflito de função do grupo de espelhos.

É possível sincronizar dados no storage de armazenamento remoto manualmente ou automaticamente.

#### Capacidade reservada e espelhamento assíncrono

A capacidade reservada é usada para acompanhar as diferenças entre o volume primário e secundário quando a sincronização não está ocorrendo. Ele também mantém o controle das estatísticas de sincronização para cada par espelhado.

Cada volume em um par espelhado requer sua própria capacidade reservada.

#### Configuração e gerenciamento

Para ativar e configurar o espelhamento entre dois arrays, você deve usar a interface do Unified Manager. Quando o espelhamento estiver ativado, você poderá gerenciar pares espelhados e configurações de

sincronização no System Manager.

### Terminologia de espelhamento assíncrono

Saiba como os termos do espelhamento assíncrono se aplicam ao storage array.

| Prazo | Descrição |
| --- | --- |
| Storage array local | O storage array local é o storage array em que você está agindo.<br><br>Quando você vê **Primary** na coluna de função local, indica que o storage array contém o volume que detém a função primária na relação de espelhamento. Quando você vê **secundário** na coluna função local, indica que a matriz de armazenamento contém o volume que detém a função secundária na relação de espelhamento. |
| Grupo de consistência do espelho | Um grupo de consistência de espelho é um recipiente para um ou mais pares espelhados. Para operações de espelhamento assíncrono, você precisa criar um grupo de consistência de espelhamento. |
| Par espelhado | Um par espelhado é composto por dois volumes, um volume primário e um volume secundário.<br><br>No espelhamento assíncrono, um par espelhado sempre pertence a um grupo de consistência de espelho. As operações de gravação são executadas primeiro no volume primário e, em seguida, replicadas no volume secundário. Cada par espelhado em um grupo de consistência de espelho compartilha as mesmas configurações de sincronização. |
| Volume primário | O volume primário de um par espelhado é o volume de origem a ser espelhado. |
| Storage array remoto | O storage array remoto geralmente é designado como local secundário, que geralmente contém uma réplica dos dados em uma configuração de espelhamento. |
| Capacidade reservada | A capacidade reservada é a capacidade alocada física usada para qualquer operação de serviço de cópia e objeto de storage. Não é diretamente legível pelo host. |
| Mudança de função | A mudança de função está atribuindo a função primária ao volume secundário e vice-versa. |
| Volume secundário | O volume secundário de um par espelhado geralmente está localizado em um local secundário e contém uma réplica dos dados. |

| Prazo | Descrição |
| --- | --- |
| Sincronização | A sincronização ocorre na sincronização inicial entre o storage array local e o storage array remoto. A sincronização também ocorre quando os volumes primário e secundário ficam não sincronizados após uma interrupção da comunicação. Quando o link de comunicação está funcionando novamente, todos os dados não replicados são sincronizados com o storage array do volume secundário. |

#### Fluxo de trabalho para espelhar um volume de forma assíncrona

Você configura o espelhamento assíncrono usando o fluxo de trabalho a seguir.

1. Execute a configuração inicial no Unified Manager:
   a. Selecione a matriz de armazenamento local como a origem para a transferência de dados.
   b. Crie ou selecione um grupo de consistência de espelho existente, que é um contentor para o volume primário no array local e o volume secundário no array remoto. Os volumes primário e secundário são referidos como o "par espelhado". Se você estiver criando o grupo de consistência de espelho pela primeira vez, especifique se deseja executar sincronizações manuais ou agendadas.
   c. Selecione um volume primário no storage array local e, em seguida, determine sua capacidade reservada. A capacidade reservada é a capacidade física alocada a ser usada para a operação de cópia.
   d. Selecione um storage array remoto como o destino da transferência, um volume secundário e, em seguida, determine sua capacidade reservada.
   e. Inicie a transferência de dados inicial do volume primário para o volume secundário. Dependendo do tamanho do volume, esta transferência inicial pode demorar várias horas.
2. Verifique o progresso da sincronização inicial:
   a. No Unified Manager, inicie o System Manager para o array local.
   b. No System Manager, visualize o status da operação de espelhamento. Quando o espelhamento estiver concluído, o status do par espelhado é "ótimo".
3. **Opcional:** você pode reagendar ou realizar manualmente transferências de dados subsequentes no System Manager. Somente blocos novos e alterados são transferidos do volume primário para o volume secundário.

> Como a replicação assíncrona é periódica, o sistema pode consolidar os blocos alterados e conservar a largura de banda da rede. Há impacto mínimo na taxa de transferência de gravação e na latência de gravação.

#### Requisitos para uso do espelhamento assíncrono

Se você planeja usar o espelhamento assíncrono, tenha em mente os seguintes requisitos.

##### Unified Manager

Para ativar e configurar o espelhamento entre dois arrays, você deve usar a interface do Unified Manager. O Unified Manager é instalado em um sistema host juntamente com o Web Services Proxy.

- O serviço Web Services Proxy deve estar em execução.
- O Unified Manager deve estar em execução em seu host local por meio de uma conexão HTTPS.
- O Unified Manager deve mostrar certificados SSL válidos para a matriz de armazenamento. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando o Unified Manager e navegando para o **certificado › Gerenciamento de certificados**.

#### Storage arrays

- Você precisa ter dois storage arrays.
- Cada storage array deve ter duas controladoras.
- Os dois storage arrays devem ser descobertos no Unified Manager.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conetado à rede.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)
- Você deve saber a senha para os storages de armazenamento local e remoto.
- Você precisa ter capacidade livre suficiente no storage array remoto para criar um volume secundário igual ou maior que o volume principal que deseja espelhar.
- Seus storage arrays locais e remotos são conectados por meio de uma malha Fibre Channel ou de uma interface iSCSI.

#### Conexões suportadas

O espelhamento assíncrono pode usar conexões FC ou iSCSI ou ambas para comunicação entre sistemas de storage locais e remotos. No momento da criação de um grupo de consistência de espelho, o administrador pode selecionar FC ou iSCSI para esse grupo se ambos estiverem conetados ao storage array remoto. Não há failover de um tipo de canal para o outro.

O espelhamento assíncrono usa as portas de e/S do host do storage array para transmitir dados espelhados do lado principal para o lado secundário.

- **Espelhamento por uma interface Fibre Channel (FC)**

  Cada controladora do storage array dedica sua porta de host FC de maior número às operações de espelhamento.

  Se o controlador tiver portas FC de base e portas FC da placa de interface do host (HIC), a porta numerada mais alta estará em um HIC. Qualquer host conetado à porta dedicada é desconetado e nenhuma solicitação de login do host é aceita. As solicitações de e/S nessa porta são aceitas somente de controladores que participam de operações de espelhamento.

  As portas de espelhamento dedicadas devem ser conectadas a um ambiente de malha FC que suporte as interfaces do serviço de diretório e serviço de nomes. Em particular, FC-AL e ponto a ponto não são compatíveis como opções de conectividade entre as controladoras que estão participando de relacionamentos espelhados.

- **Espelhamento através de uma interface iSCSI**

  Ao contrário do FC, o iSCSI não requer uma porta dedicada. Quando o espelhamento assíncrono é usado em ambientes iSCSI, não é necessário dedicar nenhuma das portas iSCSI de front-end do storage array para uso com espelhamento assíncrono. Essas portas são compartilhadas para tráfego de espelhamento

assíncrono e conexões de e/S de host para array.

O controlador mantém uma lista de sistemas de armazenamento remoto com os quais o iniciador iSCSI tenta estabelecer uma sessão. A primeira porta que estabelece com êxito uma conexão iSCSI é usada para toda a comunicação subsequente com esse storage de armazenamento remoto. Se a comunicação falhar, uma nova sessão é tentada usando todas as portas disponíveis.

As portas iSCSI são configuradas no nível da matriz, porta a porta. A comunicação entre controladores para mensagens de configuração e transferência de dados usa as configurações globais, incluindo configurações para:

- VLAN: Os sistemas locais e remotos devem ter a mesma configuração de VLAN para se comunicar
- Porta de escuta iSCSI
- Jumbo Frames
- Prioridade Ethernet

> A comunicação do intercontrolador iSCSI deve usar uma porta de conexão de host e não a porta Ethernet de gerenciamento.

O espelhamento assíncrono usa as portas de e/S do host do storage array para transmitir dados espelhados do lado principal para o lado secundário. Como o espelhamento assíncrono é destinado a redes de maior latência e de menor custo, as conexões iSCSI (e, portanto, baseadas em TCP/IP) são uma boa opção para isso. Quando o espelhamento assíncrono é usado em ambientes iSCSI, não é necessário dedicar nenhuma das portas iSCSI de front-end do array para uso com espelhamento assíncrono; essas portas são compartilhadas para tráfego de espelhamento assíncrono e conexões de e/S de host para array

#### Candidatos a volume espelhado

- O nível RAID, os parâmetros de armazenamento em cache e o tamanho do segmento podem ser diferentes nos volumes primário e secundário de um par espelhado assíncrono.

> Para controladores EF600 e EF300, os volumes primário e secundário de um par espelhado assíncrono devem corresponder ao mesmo protocolo, nível da bandeja, tamanho do segmento, tipo de segurança e nível RAID. Pares espelhados assíncronos não elegíveis não aparecerão na lista de volumes disponíveis.

- O volume secundário deve ser pelo menos tão grande quanto o volume primário.
- Um volume pode participar de apenas um relacionamento de espelho.
- Os candidatos em volume devem compartilhar os mesmos recursos de Segurança de dados.
  - Se o volume primário for compatível com FIPS, o volume secundário deve ser capaz de FIPS.
  - Se o volume principal for compatível com FDE, o volume secundário tem de ser capaz de FDE.
  - Se o volume principal não estiver usando o Drive Security, o volume secundário não deve estar usando o Drive Security.
- Os volumes primário e secundário devem compartilhar o mesmo tipo de unidade. A combinação de unidades NVMe e SAS entre volumes primário e secundário não é compatível.

#### Capacidade reservada

- Um volume de capacidade reservada é necessário para um volume primário e para um volume secundário em um par espelhado para Registrar informações de gravação para recuperar de reinicializações do controlador e outras interrupções temporárias.
- Como o volume principal e o volume secundário em um par espelhado exigem capacidade reservada adicional, você precisa garantir que tenha capacidade livre disponível em ambos os storage arrays na relação espelhada.
- O volume de capacidade reservada deve compartilhar o mesmo tipo de unidade que seus volumes de espelhamento associados.
  - Se o volume de capacidade reservada for criado em unidades NVMe, os volumes espelhados também precisarão ser criados nas unidades NVMe.
  - Se o volume de capacidade reservada for criado em unidades SAS, seus volumes espelhados também deverão ser criados em unidades SAS.

#### Recurso de segurança da unidade

- Se você estiver usando unidades com capacidade de segurança, o volume primário e o volume secundário devem ter configurações de segurança compatíveis. Esta restrição não é imposta; portanto, você deve verificá-la por conta própria.
- Se você estiver usando unidades com capacidade segura, o volume primário e o volume secundário deverão usar o mesmo tipo de unidade. Esta restrição não é imposta; portanto, você deve verificá-la por conta própria.
- Se estiver a utilizar o Data Assurance (DA), o volume primário e o volume secundário têm de ter as mesmas definições DE DA.

### Estado do espelho assíncrono

O status do espelho define o estado dos grupos de consistência do espelho e pares de volume espelhado.

#### Estado para grupos de consistência de espelhos

| Estado | Descrição |
|---|---|
| Sincronização (sincronização inicial) | O progresso da sincronização inicial de dados que foi concluída entre os pares de volume espelhado.<br><br>Durante uma sincronização inicial, os volumes podem fazer a transição para os seguintes estados: Degraded/Failed/Optimal/Unknown. |
| Sincronização (sincronização de intervalo) | O progresso da sincronização periódica de dados que foi concluída entre os pares de volume espelhado. |
| Sistema suspenso | Sincronização de dados suspensa por sistema de storage em todos os pares espelhados no nível do grupo de consistência de espelhos.<br><br>Pelo menos um par espelhado no grupo de consistência do espelho está em um estado parado ou com falha. |

| Estado | Descrição |
| --- | --- |
| Usuário suspenso | Sincronização de dados suspensa pelo usuário em todos os pares espelhados no nível do grupo de consistência espelhada.<br><br>Esse estado ajuda a reduzir qualquer impacto no desempenho do aplicativo host que possa ocorrer enquanto quaisquer dados alterados no storage array local são copiados para o storage array remoto. |
| Em pausa | O processo de sincronização de dados parou temporariamente devido a um erro ao acessar o storage de armazenamento remoto. |
| Órfão | Existe um volume de par espelhado órfão quando um volume de membro em um grupo de espelho de consistência foi removido de um lado do grupo de espelho de consistência (o lado primário ou o lado secundário), mas não do outro lado.<br><br>Volumes de pares espelhados órfãos são detetados quando a comunicação entre arrays é restaurada e os dois lados da configuração do espelho reconciliam parâmetros de espelho.<br><br>Você pode remover um par espelhado para corrigir um estado de par espelhado órfão. |
| Mudança de função pendente/em andamento | Uma mudança de função entre os grupos de consistência de espelho está pendente ou em andamento.<br><br>A mudança de reversão de função (para uma função primária ou secundária) afeta todos os pares espelhados assíncronos dentro do grupo de consistência de espelho selecionado.<br><br>Você pode cancelar uma alteração de função pendente, mas não uma mudança de função em andamento. |
| Conflito de funções | Ocorreu um conflito de função entre grupos de consistência de espelho devido a um problema de comunicação entre o storage array local e o storage array remoto durante uma operação de alteração de função.<br><br>Quando o problema de comunicação foi resolvido, ocorre um conflito de função. Use o Recovery Guru para recuperar desse erro.<br><br>Uma promoção forçada não é permitida ao resolver um conflito de função. |

#### Status para pares espelhados

O status de um par espelhado indica se os dados no volume primário e no volume secundário estão sincronizados.

| Estado | Descrição |
| --- | --- |
| Sincronização | O progresso da sincronização de dados inicial ou periódica que foi concluída entre os pares espelhados.<br><br>Existem dois tipos de sincronização: Sincronização inicial e sincronização periódica. O progresso inicial da sincronização também é exibido na caixa de diálogo operações de execução longa. |
| Ideal | Os volumes no par espelhado são sincronizados, o que indica que a conexão entre os storages de armazenamento está operacional e cada volume está na condição de trabalho desejada. |
| Incompleto | O par espelhado assíncrono está incompleto no storage array remoto porque a sequência de criação de par espelhado foi iniciada em um storage array que não é compatível com o System Manager e o par espelhado não foi concluído no secundário.<br><br>O processo de criação de par espelhado é concluído quando um volume é adicionado ao grupo de consistência espelhada no storage array remoto. Esse volume se torna o volume secundário no par espelhado assíncrono.<br><br>O par espelhado é concluído automaticamente se o storage array remoto for gerenciado pelo System Manager. |
| Falha | A operação de espelhamento assíncrono não consegue operar normalmente devido a uma falha nos volumes primários, volumes secundários ou na capacidade reservada espelhada. |
| Órfão | Existe um volume de par espelhado órfão quando um volume de membro em um grupo de espelho de consistência foi removido de um lado do grupo de espelho de consistência (o lado primário ou o lado secundário), mas não do outro lado.<br><br>Volumes de pares espelhados órfãos são detetados quando a comunicação é restaurada entre os dois arrays de armazenamento e os dois lados da configuração do espelho reconciliar parâmetros de espelho.<br><br>Você pode remover um par espelhado para corrigir um estado de par espelhado órfão. |
| Parado | O par espelhado está em um estado parado porque o grupo de consistência espelhada está em um estado suspenso pelo sistema. |

**Propriedade do volume**

## Você pode alterar o proprietário do controlador preferido em um par espelhado.

Se o volume primário do par espelhado for de propriedade da controladora A, o volume secundário também será de propriedade da controladora A do storage array remoto. Alterar o proprietário do volume primário mudará automaticamente o proprietário do volume secundário para garantir que ambos os volumes sejam propriedade do mesmo controlador. As alterações de propriedade atuais no lado primário propagam-se automaticamente para as alterações de propriedade atuais correspondentes no lado secundário.

Por exemplo, um volume primário é de propriedade da controladora A e, em seguida, você altera o proprietário da controladora para a controladora B. nesse caso, a próxima gravação remota altera o proprietário do volume secundário da controladora A para B. como as alterações de propriedade da controladora no lado secundário são controladas pelo lado primário, elas não exigem nenhuma intervenção especial do administrador de storage.

#### O controlador é reiniciado

Uma reinicialização do controlador causa uma alteração de propriedade de volume no lado primário do proprietário do controlador preferido para o controlador alternativo no storage de armazenamento.

Às vezes, uma gravação remota é interrompida por uma reinicialização do controlador ou por um ciclo de energia do storage antes de poder ser gravada no volume secundário. O controlador não precisa executar uma sincronização completa do par espelhado, neste caso.

Quando uma gravação remota foi interrompida durante uma reinicialização do controlador, o novo proprietário do controlador no lado principal lê as informações armazenadas em um arquivo de log no volume de capacidade reservada do proprietário do controlador preferido. Em seguida, o novo proprietário da controladora copia os blocos de dados afetados do volume primário para o volume secundário, eliminando a necessidade de uma sincronização completa dos volumes espelhados.

### Mudança de papel de um grupo de consistência de espelho

Você pode alterar a função entre pares espelhados em um grupo de consistência de espelho. Você pode fazer isso rebaixando o grupo de consistência de espelho primário para a função secundária ou promovendo o grupo de consistência de espelho secundário para a função principal.

Reveja as seguintes informações sobre a operação de mudança de função:

- A mudança de função afeta todos os pares espelhados dentro do grupo de consistência de espelho selecionado.
- Quando um grupo de consistência de espelho é rebaixado para a função secundária, todos os pares espelhados dentro desse grupo de consistência de espelho também são rebaixados para a função secundária e vice-versa.
- Quando o grupo de consistência de espelho primário é rebaixado para a função secundária, os hosts que foram atribuídos aos volumes de membro dentro desse grupo não têm mais acesso de gravação a eles.
- Quando um grupo de consistência de espelho é promovido para a função principal, todos os hosts que estiverem acessando os volumes de membros dentro desse grupo agora poderão escrever para eles.
- Se a matriz de armazenamento local não conseguir se comunicar com a matriz de armazenamento remoto, você pode forçar a alteração de função na matriz de armazenamento local.

#### Forçar mudança de função

Você pode forçar uma mudança de função entre grupos de consistência de espelho quando um problema de comunicação entre o storage array local e o storage array remoto estiver impedindo a promoção dos volumes de membro dentro do grupo de consistência de espelho secundário ou a rebaixamento dos volumes de membro dentro do grupo de consistência de espelho primário.

Você pode forçar o grupo de consistência de espelho no lado secundário a fazer a transição para a função principal. Em seguida, o host de recuperação pode acessar os volumes de membros recém-promovidos dentro desse grupo de consistência espelhada, e as operações de negócios podem continuar.

#### Quando é permitida uma promoção forçada e não é permitida?

A promoção forçada de um grupo de consistência de espelho só é permitida se todos os volumes de membros do grupo de consistência de espelho tiverem sido sincronizados e tiverem pontos de recuperação consistentes.

A promoção forçada de um grupo de consistência de espelhos não é permitida nas seguintes condições:

- Qualquer um dos volumes de membros de um grupo de consistência de espelho está no processo de uma sincronização inicial.
- Qualquer um dos volumes membros de um grupo de consistência de espelho não tem uma imagem pontual do ponto de recuperação (por exemplo, devido a um erro de capacidade reservada total).
- O grupo de consistência de espelho não contém volumes de membros.
- O grupo de consistência espelhada está nos estados Falha, mudança de função pendente ou mudança de função em andamento ou se algum dos volumes associados ou volumes de capacidade reservada falhar.

#### Conflito de função do grupo de espelhos

Quando um problema de comunicação entre as matrizes de armazenamento local e remoto foi resolvido, ocorre uma condição de conflito de função de Grupo de espelhos. Use o Recovery Guru para recuperar desse erro. Uma promoção forçada não é permitida ao resolver um conflito de dupla função.

Para evitar a condição de conflito de função do Grupo de espelhos e as etapas subsequentes de recuperação, aguarde até que a conexão entre os arrays de armazenamento esteja operacional para forçar a mudança de função.

#### Mudança de função no estado em andamento

Se dois storage arrays em uma configuração de espelhamento forem desconetados e o lado primário de um grupo de consistência de espelho for forçado a uma função secundária, e o lado secundário de um grupo de consistência de espelho for promovido a uma função primária, então, quando a comunicação for restaurada, os grupos de consistência de espelho em ambos os storage arrays serão colocados no estado de mudança de função em andamento.

O sistema concluirá o processo de mudança de função transferindo os logs de mudança, sincronizando novamente, definindo o estado do grupo de consistência do espelho de volta para um estado operacional normal e continuando com sincronizações periódicas.

## Conceitos de sincronização

### Como o espelhamento síncrono funciona

O espelhamento síncrono replica volumes de dados em tempo real para garantir disponibilidade contínua.

O espelhamento síncrono não está disponível no storage array EF600 ou EF300.

O espelhamento síncrono alcança um objetivo de ponto de recuperação (RPO) sem perda de dados ao dispor uma cópia dos dados importantes se um desastre ocorrer em um dos dois storage arrays. A cópia é idêntica aos dados de produção a cada momento, porque cada vez que uma gravação é feita no volume primário, uma gravação é feita no volume secundário. O host não recebe uma confirmação de que a gravação foi bem-sucedida até que o volume secundário seja atualizado com êxito com as alterações feitas no volume primário.

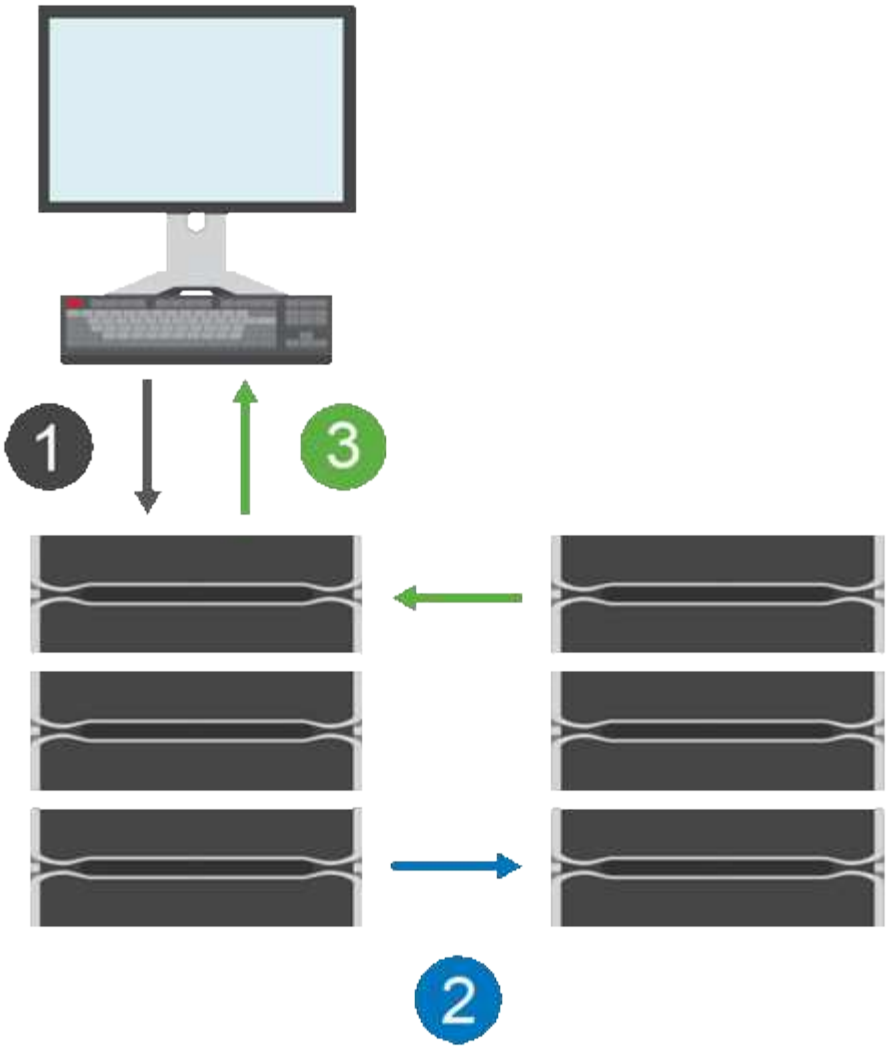
Esse tipo de espelhamento é ideal para fins de continuidade dos negócios, como recuperação de desastres.

#### Relação de espelhamento síncrono

Uma relação de espelhamento síncrono consiste em um volume primário e um volume secundário em storage arrays separados. O storage array que contém o volume primário geralmente está localizado no local principal e serve os hosts ativos. O storage array que contém o volume secundário geralmente fica em um local secundário e contém uma réplica dos dados. O volume secundário será usado se o storage array do volume primário não estiver disponível devido, por exemplo, a uma interrupção completa de energia, um incêndio ou uma falha de hardware no local primário.

#### Sessão de espelhamento síncrono

O processo de configuração de espelhamento síncrono envolve a configuração de volumes em pares. Depois de criar um par espelhado, que consiste em um volume primário em um storage array e um volume secundário em outro storage array, é possível iniciar o espelhamento síncrono. Os passos no espelhamento síncrono são apresentados abaixo.




1. Uma escrita vem do host.
2. A gravação é comprometida com o volume primário, propagada para o sistema remoto e, em seguida, comprometida com o volume secundário.
3. O storage array do volume primário envia uma mensagem de conclusão de e/S para o sistema host *após* ambas as operações de gravação foram concluídas com sucesso.

A capacidade reservada é usada para Registrar informações sobre a solicitação de gravação recebida de um host.

Quando o proprietário atual do controlador do volume primário recebe uma solicitação de gravação de um host, o controlador primeiro Registra informações sobre a gravação na capacidade reservada do volume primário. Em seguida, ele grava os dados no volume primário. Em seguida, o controlador inicia uma operação de gravação remota para copiar os blocos de dados afetados para o volume secundário no storage array remoto.

Como o aplicativo host deve esperar que a gravação ocorra no storage array local e na rede no storage array remoto, uma conexão muito rápida entre o storage array local e o storage array remoto é necessária para manter o relacionamento espelhado sem reduzir excessivamente o desempenho de e/S local.

#### Recuperação de desastres

O espelhamento síncrono mantém uma cópia dos dados que está fisicamente distante do local onde os dados residem. Se um desastre ocorrer no local principal, como uma interrupção de energia ou uma inundação, os dados podem ser acessados rapidamente a partir do local secundário.

O volume secundário não está disponível para hospedar aplicações enquanto a operação de espelhamento síncrono está em andamento. Portanto, em caso de desastre no storage array local, você pode fazer failover para o storage array remoto. Para fazer failover, promova o volume secundário para o papel principal. Em seguida, o host de recuperação pode acessar o volume recém-promovido e as operações de negócios podem continuar.

#### Definições de sincronização

Ao criar um par espelhado, você também define a prioridade de sincronização e a política de ressincronização que o par espelhado usa para concluir a operação de ressincronização após uma interrupção de comunicação.

Se o link de comunicação entre os dois storages parar de funcionar, os hosts continuarão recebendo confirmações do storage array local, impedindo a perda de acesso. Quando o link de comunicação está funcionando novamente, qualquer dado não replicado pode ser ressinced automaticamente ou manualmente para o storage array remoto.

Se os dados são ressincronizados automaticamente depende da política de ressincronização do par espelhado. Uma política de ressincronização automática permite que o par espelhado ressincronize automaticamente quando o link estiver funcionando novamente. Uma política de ressincronização manual requer que você retome manualmente a sincronização após um problema de comunicação. A ressincronização manual é a política recomendada.

Você pode editar as configurações de sincronização para um par espelhado somente na matriz de armazenamento que contém o volume primário.

#### Dados não sincronizados

Os volumes primário e secundário ficam não sincronizados quando o storage array do volume primário não consegue gravar dados no volume secundário. Isso pode ser causado pelos seguintes problemas:

- Problemas de rede entre os storages de armazenamento local e remoto
- Um volume secundário com falha
- Sincronização sendo suspensa manualmente no par espelhado

#### Par espelhado órfão

Existe um volume de par espelhado órfão quando um volume de membro foi removido de um lado (do lado primário ou secundário), mas não do outro lado.

Volumes de pares espelhados órfãos são detetados quando a comunicação entre arrays é restaurada e os dois lados da configuração do espelho reconciliam parâmetros de espelho.

Você pode remover um par espelhado para corrigir um estado de par espelhado órfão.

#### Configuração e gerenciamento

Para ativar e configurar o espelhamento entre dois arrays, você deve usar a interface do Unified Manager. Quando o espelhamento estiver ativado, você poderá gerenciar pares espelhados e configurações de sincronização no System Manager.

### Terminologia de espelhamento síncrono

Saiba como os termos do espelhamento síncrono se aplicam ao storage array.

| Prazo | Descrição |
|---|---|
| Storage array local | O storage array local é o storage array em que você está agindo.<br><br>Quando você vê **Primary** na coluna de função local, indica que o storage array contém o volume que detém a função primária na relação de espelhamento. Quando você vê **secundário** na coluna função local, indica que a matriz de armazenamento contém o volume que detém a função secundária na relação de espelhamento. |
| Par espelhado | Um par espelhado é composto por dois volumes, um volume primário e um volume secundário. |
| Volume primário | O volume primário de um par espelhado é o volume de origem a ser espelhado. |
| Objetivo do ponto de restauração (RPO) | O objetivo do ponto de recuperação (RPO) representa um objetivo que indica a diferença considerada aceitável entre o volume primário e o volume secundário em um par espelhado. Um RPO de zero indica que nenhuma diferença entre o volume primário e o volume secundário pode ser tolerada. Um RPO maior que zero indica que o volume secundário está menos corrente ou fica aquém do volume primário. |
| Storage array remoto | O storage array remoto geralmente é designado como local secundário, que geralmente contém uma réplica dos dados em uma configuração de espelhamento. |
| Capacidade reservada | A capacidade reservada é a capacidade alocada física usada para qualquer operação de serviço de cópia e objeto de storage. Não é diretamente legível pelo host. |

| Prazo | Descrição |
| --- | --- |
| Mudança de função | A mudança de função está atribuindo a função primária ao volume secundário e vice-versa. |
| Volume secundário | O volume secundário de um par espelhado geralmente está localizado em um local secundário e contém uma réplica dos dados. |
| Sincronização | A sincronização ocorre na sincronização inicial entre o storage array local e o storage array remoto. A sincronização também ocorre quando os volumes primário e secundário ficam não sincronizados após uma interrupção da comunicação. Quando o link de comunicação está funcionando novamente, todos os dados não replicados são sincronizados com o storage array do volume secundário. |

#### Fluxo de trabalho para espelhar um volume de forma síncrona

Você configura o espelhamento síncrono usando o fluxo de trabalho a seguir.

Este recurso não está disponível no sistema de armazenamento EF600 ou EF300.

1. Execute a configuração inicial no Unified Manager:
   a. Selecione uma matriz de armazenamento local como a origem para a transferência de dados.
   b. Selecione um volume primário no storage array local.
   c. Selecione uma matriz de armazenamento remota como destino para a transferência de dados e, em seguida, selecione um volume secundário.
   d. Selecione as prioridades de sincronização e ressincronização.
   e. Inicie a transferência de dados inicial do volume primário para o volume secundário. Dependendo do tamanho do volume, esta transferência inicial pode demorar várias horas.
2. Verifique o progresso da sincronização inicial:
   a. No Unified Manager, inicie o System Manager para o array local.
   b. No System Manager, visualize o status da operação de espelhamento. Quando o espelhamento estiver concluído, o status do par espelhado é "ótimo". Os dois arrays tentam permanecer sincronizados através de operações normais. Somente blocos novos e alterados são transferidos do volume primário para o volume secundário.
3. **Opcional:** você pode alterar as configurações de sincronização no System Manager.

Como a replicação síncrona é contínua, o link de replicação entre os dois locais precisa fornecer recursos de largura de banda suficientes.

#### Requisitos para o uso do espelhamento síncrono

Se você planeja usar o espelhamento síncrono, tenha em mente os seguintes requisitos.

#### Unified Manager

Para ativar e configurar o espelhamento entre dois arrays, você deve usar a interface do Unified Manager. O Unified Manager é instalado em um sistema host juntamente com o Web Services Proxy.

- O serviço Web Services Proxy deve estar em execução.
- O Unified Manager deve estar em execução em seu host local por meio de uma conexão HTTPS.
- O Unified Manager deve mostrar certificados SSL válidos para a matriz de armazenamento. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando o Unified Manager e navegando para o **certificado › Gerenciamento de certificados**.

#### Storage arrays

O espelhamento síncrono não está disponível no storage array EF300 ou EF600.

- Você precisa ter dois storage arrays.
- Cada storage array deve ter duas controladoras.
- Os dois storage arrays devem ser descobertos no Unified Manager.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conetado à rede.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)
- Você deve saber a senha para os storages de armazenamento local e remoto.
- Você precisa ter capacidade livre suficiente no storage array remoto para criar um volume secundário igual ou maior que o volume principal que deseja espelhar.
- Seus storage arrays locais e remotos são conectados por meio de uma malha Fibre Channel.

#### Conexões suportadas

A comunicação para espelhamento síncrono é compatível apenas com controladoras com portas de host Fibre Channel (FC).

O espelhamento síncrono usa a porta de host com número mais alto em cada controlador, no storage array local e no storage array remoto. A porta de host 4 do adaptador de barramento do host do controlador (HBA) é normalmente reservada para transmissão de dados espelhados.

#### Candidatos a volume espelhado

- O nível RAID, os parâmetros de armazenamento em cache e o tamanho do segmento podem ser diferentes nos volumes primário e secundário de um par espelhado síncrono.
- Os volumes primário e secundário em um par espelhado síncrono devem ser volumes padrão. Não podem ser volumes finos ou volumes instantâneos.
- O volume secundário deve ser pelo menos tão grande quanto o volume primário.
- Somente o volume principal pode ter snapshots associados a ele e/ou ser o volume de origem ou destino em uma operação de cópia de volume.
- Um volume pode participar de apenas um relacionamento de espelho.
- Há limites para o número de volumes suportados em um determinado storage array. Certifique-se de que o número de volumes configurados na matriz de armazenamento seja inferior ao limite suportado. Quando

o espelhamento síncrono está ativo, os dois volumes de capacidade reservada criados contam para o limite de volume.

#### Capacidade reservada

- A capacidade reservada é necessária para um volume primário e para um volume secundário para registar informações de gravação para recuperar de reinicializações do controlador e outras interrupções temporárias.
- Os volumes de capacidade reservada são criados automaticamente quando o espelhamento síncrono é ativado. Como o volume principal e o volume secundário em um par espelhado exigem capacidade reservada, você precisa garantir que tenha capacidade livre suficiente disponível em ambos os storage arrays que participam do relacionamento de espelhamento síncrono.

#### Recurso de segurança da unidade

- Se você estiver usando unidades com capacidade de segurança, o volume primário e o volume secundário devem ter configurações de segurança compatíveis. Esta restrição não é imposta; portanto, você deve verificá-la por conta própria.
- Se você estiver usando unidades com capacidade segura, o volume primário e o volume secundário deverão usar o mesmo tipo de unidade. Esta restrição não é imposta; portanto, você deve verificá-la por conta própria.
  - Se o volume principal utilizar unidades de encriptação total de disco (FDE), o volume secundário deverá utilizar unidades FDE.
  - Se o volume primário usar unidades validadas FIPS (Federal Information Processing Standards 140-2), o volume secundário deverá usar unidades validadas FIPS 140-2-2.
- Se estiver a utilizar o Data Assurance (DA), o volume primário e o volume secundário têm de ter as mesmas definições DE DA.

### Status do espelhamento síncrono

O status de um par espelhado síncrono indica se os dados no volume primário e no volume secundário estão sincronizados. Um status de espelho é independente do status do componente dos volumes no par espelhado.

Este recurso não está disponível no sistema de armazenamento EF600 ou EF300.

Pares espelhados síncronos podem ter um dos seguintes status:

- **Ótimo**

  Indica que os volumes no par espelhado estão sincronizados, o que significa que a conexão de malha entre os storages de armazenamento está operacional e cada volume está na condição de trabalho desejada.

- **Sincronização**

  Mostra o progresso da sincronização de dados entre os pares espelhados. Este estado também será apresentado durante a sincronização inicial.

  Após uma interrupção do link de comunicação, apenas os blocos de dados que foram alterados no volume primário durante a interrupção do link são copiados para o volume secundário.

- **Não sincronizado**

  Indica que a matriz de armazenamento do volume primário não consegue gravar dados de entrada na matriz remota. O host local pode continuar a gravar no volume principal, mas não ocorrem gravações remotas. Condições diferentes podem impedir que o storage array do volume primário grave dados recebidos no volume secundário, como:

  - O volume secundário não está acessível.
  - A matriz de armazenamento remoto não está acessível.
  - A conexão de malha entre os storage arrays não está acessível.
  - O volume secundário não pode ser atualizado com um novo World Wide Identifier (WWID).

- * Suspenso*

  Indica que a operação de espelhamento síncrono foi suspensa pelo usuário. Quando um par espelhado é suspenso, nenhuma tentativa é feita para entrar em Contato com o volume secundário. Todas as gravações no volume primário são persistentemente registradas nos volumes de capacidade reservada espelhada.

- **Falhou**

  Indica que a operação de espelhamento síncrono não pode operar normalmente devido a uma falha no volume primário, no volume secundário ou na capacidade reservada do espelho.

**Propriedade do volume**

Você pode alterar o proprietário do controlador preferido em um par espelhado.

Esse recurso não está disponível para espelhamento síncrono no sistema de storage EF600 ou EF300.

Se o volume primário do par espelhado for de propriedade da controladora A, o volume secundário também será de propriedade da controladora A do storage array remoto. Alterar o proprietário do volume primário mudará automaticamente o proprietário do volume secundário para garantir que ambos os volumes sejam propriedade do mesmo controlador. As alterações de propriedade atuais no lado primário propagam-se automaticamente para as alterações de propriedade atuais correspondentes no lado secundário.

Por exemplo, um volume primário é de propriedade da controladora A e, em seguida, você altera o proprietário da controladora para a controladora B. nesse caso, a próxima gravação remota altera o proprietário do volume secundário da controladora A para B. como as alterações de propriedade da controladora no lado secundário são controladas pelo lado primário, elas não exigem nenhuma intervenção especial do administrador de storage.

#### O controlador é reiniciado

Uma reinicialização do controlador causa uma alteração de propriedade de volume no lado primário do proprietário do controlador preferido para o controlador alternativo no storage de armazenamento.

Às vezes, uma gravação remota é interrompida por uma reinicialização do controlador ou por um ciclo de energia do storage antes de poder ser gravada no volume secundário. O controlador não precisa executar uma sincronização completa do par espelhado, neste caso.

Quando uma gravação remota foi interrompida durante uma reinicialização do controlador, o novo proprietário

do controlador no lado principal lê as informações armazenadas em um arquivo de log no volume de capacidade reservada do proprietário do controlador preferido. Em seguida, o novo proprietário da controladora copia os blocos de dados afetados do volume primário para o volume secundário, eliminando a necessidade de uma sincronização completa dos volumes espelhados.

### Mudança de função entre volumes em um par espelhado

Você pode alterar a função entre volumes em um par espelhado. Você pode fazer isso rebaixando o volume primário para a função secundária ou promovendo o volume secundário para a função principal.

> O espelhamento síncrono não está disponível no sistema de storage EF600 ou EF300.

Reveja as seguintes informações sobre a operação de mudança de função:

- Quando um volume primário é rebaixado para a função secundária, o volume secundário nesse par espelhado é promovido para a função primária e vice-versa.
- Quando o volume primário é rebaixado para a função secundária, os hosts que foram atribuídos a esse volume não têm mais acesso de gravação a ele.
- Quando o volume secundário é promovido à função principal, todos os hosts que estiverem acessando esse volume agora poderão gravar nele.
- Se a matriz de armazenamento local não conseguir se comunicar com a matriz de armazenamento remoto, você pode forçar a alteração de função na matriz de armazenamento local.

#### Forçar mudança de função

Você pode forçar uma mudança de função entre volumes em um par espelhado quando um problema de comunicação entre o storage array local e o storage array remoto estiver impedindo a promoção do volume secundário ou a rebaixamento do volume primário.

Você pode forçar o volume no lado secundário a fazer a transição para a função principal. Em seguida, o host de recuperação pode acessar o volume recém-promovido e as operações de negócios podem continuar.

> Quando a matriz de armazenamento remoto for recuperada e quaisquer problemas de comunicação tiverem sido resolvidos, ocorre uma condição de conflito de espelhamento síncrono - volume primário. As etapas de recuperação incluem ressincronizar os volumes. Use o Recovery Guru para recuperar desse erro.

#### Quando é permitida uma promoção forçada e não é permitida?

A promoção forçada de um volume em um par espelhado não é permitida nas seguintes condições:

- Qualquer um dos volumes em um par espelhado está no processo de uma sincronização inicial.
- O par espelhado está nos estados Falha, mudança de função pendente ou mudança de função em andamento ou se algum dos volumes de capacidade reservada associados estiver com falha.

#### Mudança de função no estado em andamento

Se dois storage arrays em uma configuração de espelhamento forem desconetados e o volume primário de um par espelhado for forçado a ser rebaixado para uma função secundária, e o volume secundário de um par espelhado for forçado a uma função primária, então, quando a comunicação for restaurada, os volumes em

ambos os storage arrays serão colocados no estado de mudança de função em andamento.

O sistema concluirá o processo de mudança de função transferindo os logs de mudança, sincronizando novamente, definindo o estado do par espelhado de volta para um estado operacional normal e continuando com as sincronizações.

## Gerenciar grupos assíncronos de consistência de espelho

### Teste a comunicação para grupos de consistência de espelhos

Você pode testar o link de comunicação para diagnosticar possíveis problemas de comunicação entre o storage de armazenamento local e o storage de armazenamento remoto associado a um grupo de consistência de espelho.

#### Antes de começar

O grupo de consistência de espelho que você deseja testar deve existir nos storages locais e remotos.

#### Sobre esta tarefa

Você pode executar quatro testes diferentes:

- **Conetividade** — verifica se os dois controladores têm um caminho de comunicação. O teste de conetividade envia uma mensagem inter-array entre os arrays de armazenamento e, em seguida, valida que o grupo de consistência de espelho correspondente na matriz de armazenamento remoto existe. Ele também valida que os volumes membros do grupo de consistência de espelho na matriz de armazenamento remoto correspondem aos volumes membros do grupo de consistência de espelho na matriz de armazenamento local.
- **Latência** — envia um comando SCSI Test Unit para cada volume espelhado na matriz de armazenamento remoto associada ao grupo de consistência de espelho para testar a latência mínima, média e máxima.
- **Bandwidth** — envia duas mensagens entre arrays para o storage de armazenamento remoto para testar a largura de banda mínima, média e máxima, bem como a velocidade de link negociada da porta na matriz que executa o teste.
- **Port Connections** — mostra a porta que está sendo usada para espelhamento no storage de armazenamento local e a porta que está recebendo os dados espelhados no storage de armazenamento remoto.

#### Passos

1. Selecione **armazenamento › Espelhamento assíncrono**.
2. Selecione a guia **Mirror Consistency Groups** e, em seguida, selecione o grupo Mirror Consistency que deseja testar.
3. Selecione **Test Communication**.

   É apresentada a caixa de diálogo Test Communication (testar comunicação).

4. Selecione um ou mais testes de comunicação a serem executados entre os storages de armazenamento local e remoto associados ao grupo de consistência de espelho selecionado e clique em **Teste**.
5. Reveja as informações apresentadas na janela de resultados.

| Estado do teste de comunicação | Descrição |
| --- | --- |
| Normal sem erros | O grupo de consistência do espelho está a comunicar corretamente. |
| Estado aprovado (mas não normal) | Verifique possíveis problemas de rede ou conexão e tente novamente o teste. |
| Estado com falha | É indicado o motivo da falha. Consulte o Recovery Guru para corrigir o problema. |
| Erro de ligação da porta | O motivo pode ser que a matriz de armazenamento local não esteja conetada ou que a matriz de armazenamento remoto não possa ser contatada. Consulte o Recovery Guru para corrigir o problema. |

**Resultados**

Após a conclusão do teste de comunicação, esta caixa de diálogo mostra um estado normal, um estado aprovado ou um estado de falha.

Se o teste de comunicação retornar um status de falha, o teste continuará sendo executado depois que você fechar esta caixa de diálogo até que a comunicação entre os grupos de consistência de espelho seja restaurada.

### Suspender ou retomar a sincronização para o grupo de consistência do espelho

Você pode suspender ou retomar a sincronização de dados em todos os pares espelhados dentro de um grupo de consistência de espelho, o que é mais eficiente do que suspender ou retomar a sincronização em pares espelhados individuais.

**Sobre esta tarefa**

Suspender e retomar a sincronização em grupos ajuda a reduzir qualquer impactos no desempenho do aplicativo host, que pode ocorrer enquanto quaisquer dados alterados no storage array local são copiados para o storage array remoto.

O estado do grupo de consistência do espelho e seus pares espelhados permanecem suspensos até que você use a opção Retomar para retomar a atividade de sincronização.

**Passos**

1. Selecione **armazenamento › Espelhamento assíncrono**.
2. Selecione a guia **Espelhar grupos de consistência**.

   A tabela Grupo de consistência espelhada é exibida e exibe todos os grupos de consistência de espelho associados ao storage array.

3. Selecione o grupo de consistência de espelho que deseja suspender ou retomar e selecione **mais › suspender** ou **mais › Retomar**.

   O sistema apresenta uma confirmação.

4. Selecione **Sim** para confirmar.

**Resultados**

O System Manager executa as seguintes ações:

- Suspende ou retoma a transferência de dados entre todos os pares espelhados em um grupo de consistência de espelho sem remover a relação de espelhamento.
- Regista todos os dados que foram gravados no lado primário do grupo de consistência do espelho enquanto o grupo de espelhos está suspenso e grava os dados automaticamente no lado secundário do grupo de consistência do espelho quando o grupo de espelhos é retomado. Não é necessária uma sincronização completa.
- Para grupos de consistência de espelho *suspenso*, exibe **suspenso pelo usuário** na tabela grupos de consistência de espelho.
- Para um grupo de consistência de espelho *retomado*, os dados gravados nos volumes primários enquanto o grupo de consistência de espelho foi suspenso são gravados nos volumes secundários imediatamente. A sincronização periódica é retomada se tiver sido definido um intervalo de sincronização automática.

### Altere as configurações de sincronização para um grupo de consistência de espelho

Você pode alterar as configurações de sincronização e os limites de aviso que o grupo de consistência de espelho no storage array local usa quando os dados são sincronizados inicialmente ou quando os dados são sincronizados novamente durante operações de espelhamento assíncrono.

**Sobre esta tarefa**

Alterar as configurações de sincronização afeta as operações de sincronização de todos os pares espelhados dentro do grupo de consistência de espelho.

**Passos**

1. Selecione **armazenamento › Espelhamento assíncrono**.
2. Selecione a guia **Espelhar grupos de consistência**.

   A tabela Grupo de consistência espelhada é exibida e exibe todos os grupos de consistência de espelho associados ao storage array.

3. Selecione o grupo de consistência de espelho que você deseja editar e, em seguida, selecione **mais › Editar configurações**.

   O sistema exibe a caixa de diálogo Editar configurações.

4. Edite as configurações de sincronização e alerta conforme apropriado e clique em **Salvar**.

**Detalhes do campo**

| Campo | Descrição |
| --- | --- |
| Sincronizar os pares espelhados… | Especifique se deseja sincronizar os pares espelhados na matriz de armazenamento remoto manualmente ou automaticamente.<br>• **Manualmente** – Selecione essa opção para sincronizar manualmente os pares espelhados no storage de armazenamento remoto.<br>• **Automaticamente, a cada** – Selecione esta opção para sincronizar automaticamente os pares espelhados na matriz de armazenamento remoto especificando o intervalo de tempo desde o início da atualização anterior até o início da próxima atualização. O intervalo padrão é de 10 minutos. |
| Alerta-me… | Se você definir o método de sincronização para ocorrer automaticamente, defina os seguintes alertas:<br>• **Sincronização** – defina o período de tempo após o qual o System Manager envia um alerta de que a sincronização não foi concluída.<br>• **Ponto de recuperação remota** – defina um limite de tempo após o qual o System Manager envia um alerta indicando que os dados do ponto de recuperação na matriz de armazenamento remoto são mais antigos do que o limite de tempo definido. Defina o limite de tempo a partir do final da atualização anterior.<br>• **Limite de capacidade reservada** – defina um valor de capacidade reservada no qual o System Manager envia um alerta de que você está se aproximando do limite de capacidade reservada. Defina o limite por porcentagem da capacidade restante. |

**Resultados**

O System Manager altera as configurações de sincronização para cada par espelhado no grupo de consistência espelhada.

### Sincronize novamente o grupo de consistência de espelhos manualmente

Você pode iniciar manualmente a re-sincronização para todos os pares espelhados dentro de um grupo de consistência de espelho.

**Passos**

1. Selecione **armazenamento › Espelhamento assíncrono**.
2. Selecione a guia **Espelhar grupos de consistência**.

   A tabela Mirror Consistency Group (Grupo de consistência de espelho) é exibida e exibe todos os grupos de consistência de espelho associados ao storage array.

3. Selecione o grupo de consistência de espelho que deseja sincronizar novamente e, em seguida, selecione **mais › manualmente ressincronizar**.

O sistema apresenta uma confirmação.

4. Selecione **Sim** para confirmar.

**Resultados**

O sistema executa as seguintes ações:

- Inicia a re-sincronização de dados em todos os pares espelhados dentro do grupo de consistência de espelho selecionado.
- Atualiza os dados modificados do storage array local para o storage array remoto.

### Exibir a quantidade de dados não sincronizados entre grupos de consistência de espelho

Você pode exibir a quantidade de dados não sincronizados entre os grupos de consistência de espelho no storage array local e no storage array remoto. Embora o grupo de consistência de espelho esteja em um status não sincronizado, nenhuma atividade de espelhamento ocorre.

**Sobre esta tarefa**

Você pode executar essa tarefa quando o grupo de consistência de espelho selecionado contiver pares espelhados e quando a sincronização não estiver em andamento.

**Passos**

1. Selecione **armazenamento › Espelhamento assíncrono**.
2. Selecione a guia **Espelhar grupos de consistência**.

   A tabela Mirror Consistency Group (Grupo de consistência de espelho) é exibida e exibe todos os grupos de consistência de espelho associados ao storage array.

3. Clique em **mais › Ver quantidade de dados não sincronizados**.

   Se houver dados não sincronizados, os valores da tabela refletem isso. A coluna quantidade de dados lista a quantidade de dados não sincronizados no MIB.

### Atualize o endereço IP remoto

Pode atualizar o endereço IP iSCSI da sua matriz de armazenamento remota para restabelecer a ligação com a matriz de armazenamento local.

**Antes de começar**

Tanto o storage array local quanto o storage array remoto devem ser configurados para espelhamento assíncrono usando uma conexão iSCSI.

**Passos**

1. Selecione **armazenamento › Espelhamento assíncrono**.
2. Selecione a guia **Espelhar grupos de consistência**.

   A tabela Grupo de consistência de espelho exibe todos os grupos de consistência de espelho associados ao storage array.

3. Selecione o grupo de consistência espelhada que deseja atualizar e, em seguida, selecione **mais › Atualizar endereço IP remoto**.

   O sistema exibe a caixa de diálogo Atualizar endereço IP remoto.

4. Selecione **Atualizar** para atualizar o endereço IP iSCSI da matriz de armazenamento remoto.

**Resultados**

O sistema redefine o endereço IP da matriz de armazenamento remoto para restabelecer a conexão com a matriz de armazenamento local.

### Altere a função do grupo de consistência do espelho para primário ou secundário

Você pode alterar a função entre grupos de consistência de espelho para fins administrativos ou em caso de desastre no storage array local.

**Sobre esta tarefa**

Os grupos de consistência de espelho criados no storage array local mantêm a função principal. Os grupos de consistência de espelho criados no storage array remoto mantêm a função secundária. Você pode rebaixar o grupo de consistência de espelho local para uma função secundária ou promover o grupo de consistência de espelho remoto para uma função primária.

**Passos**

1. Selecione **armazenamento › Espelhamento assíncrono**.
2. Selecione a guia **Espelhar grupos de consistência**.

   A tabela Mirror Consistency Group (Grupo de consistência de espelho) é exibida e exibe todos os grupos de consistência de espelho associados ao storage array.

3. Selecione o grupo de consistência de espelho para o qual você deseja alterar a função e selecione menu:mais[alterar função para **>**.

   O sistema apresenta uma confirmação.

4. Confirme que você deseja alterar a função do grupo de consistência espelhada e clique em **alterar função**.

   > O sistema exibe a caixa de diálogo não é possível contactar a matriz de armazenamento quando uma alteração de função é solicitada, mas a matriz de armazenamento remoto não pode ser contatada. Clique em **Sim** para forçar a mudança de função.

**Resultados**

O System Manager executa as seguintes ações:

- A tabela Grupo de consistência de espelho exibe o status "pendente" ou "em andamento" ao lado do grupo de consistência de espelho que está passando pela alteração de função. Você pode cancelar uma operação de alteração de função pendente clicando no link **Cancelar** localizado na célula da tabela.
- Se o grupo de consistência de espelho associado puder ser contatado, as funções entre os grupos de consistência de espelho serão alteradas. O System Manager promove o grupo de consistência de espelhos secundários para uma função primária ou rebaixa o grupo de consistência de espelhos primários para uma função secundária (dependendo da sua seleção). A mudança de função afeta todos os pares

espelhados dentro do grupo de consistência de espelho selecionado.

### Eliminar grupo de consistência de espelho

Você pode excluir grupos de consistência de espelho que não são mais necessários no storage de armazenamento local e no storage de armazenamento remoto.

#### Antes de começar

Todos os pares espelhados devem ser removidos do grupo de consistência de espelho.

#### Passos

1. Selecione **armazenamento › Espelhamento assíncrono**.
2. Selecione a guia **Espelhar grupos de consistência**.

   A tabela Mirror Consistency Group (Grupo de consistência de espelho) é exibida e exibe todos os grupos de consistência de espelho associados ao storage array.

3. Selecione o grupo de consistência de espelho que você deseja excluir e, em seguida, selecione **tarefas incomuns › Excluir**.

   O sistema apresenta uma confirmação.

4. Selecione **Yes** para excluir o grupo de consistência espelhada.

#### Resultados

O System Manager executa as seguintes ações:

- Exclui primeiro o grupo de consistência de espelho na matriz de armazenamento local e, em seguida, exclui o grupo de consistência de espelho na matriz de armazenamento remoto.
- Remove o grupo de consistência de espelho da tabela Grupo de consistência de espelho.

#### Depois de terminar

Ocasionalmente, pode haver instâncias em que o grupo de consistência de espelho é excluído com sucesso da matriz de armazenamento local, mas um erro de comunicação impede que o grupo de consistência de espelho seja excluído da matriz de armazenamento remoto. Nesse caso, você deve acessar a matriz de armazenamento remoto para excluir o grupo de consistência de espelho correspondente.

## Gerenciar pares espelhados assíncronos

### Remova a relação assíncrona do espelho

Você remove um par espelhado para remover a relação de espelhamento do volume primário no storage array local e o volume secundário no storage array remoto.

#### Sobre esta tarefa

Revise as seguintes informações sobre pares espelhados órfãos:

- Um par espelhado órfão existe quando um volume de membro em um grupo de espelhos de consistência foi removido de um lado (do lado do storage array local ou do lado do storage array remoto), mas não do outro lado.
- Pares espelhados órfãos são detetados quando a comunicação inter-array é restaurada e os dois lados da

configuração do espelho reconcitam os parâmetros do espelho.

- Você pode remover um par espelhado para corrigir um estado de par espelhado órfão.

**Passos**

1. Selecione **armazenamento › Espelhamento assíncrono**.
2. Selecione a guia **Mirrored Pair** (par espelhado).

   A tabela pares espelhados é exibida e exibe todos os pares espelhados associados ao storage array.

3. Selecione o par espelhado que deseja remover e clique em **Remover**.
4. Confirme se deseja remover o par espelhado e clique em **Remover**.

**Resultados**

O System Manager executa as seguintes ações:

- Remove a relação de espelhamento do grupo de consistência de espelho no storage de armazenamento local e no storage de armazenamento remoto e exclui a capacidade reservada.
- Retorna o volume primário e o volume secundário para volumes não espelhados acessíveis ao host.
- Atualiza a telha de espelhamento assíncrono com a remoção do par espelhado assíncrono.

### Aumentar a capacidade reservada

Você pode aumentar a capacidade reservada, que é a capacidade alocada fisicamente usada para qualquer operação de serviço de cópia em um objeto de armazenamento.

Para operações de snapshot, geralmente é de 40% do volume base; para operações de espelhamento assíncrono, geralmente é de 20% do volume base. Normalmente, você aumenta a capacidade reservada quando recebe um aviso de que a capacidade reservada do objeto de armazenamento está ficando cheia.

**Antes de começar**

- O volume no pool ou grupo de volumes deve ter um status ideal e não deve estar em nenhum estado de modificação.
- A capacidade livre deve existir no pool ou grupo de volumes que você deseja usar para aumentar a capacidade.

  Se não houver capacidade livre em nenhum pool ou grupo de volumes, você poderá adicionar capacidade não atribuída na forma de unidades não utilizadas a um pool ou grupo de volumes.

**Sobre esta tarefa**

Você pode aumentar a capacidade reservada somente em incrementos de 8 GiB para os seguintes objetos de armazenamento:

- Grupo de instantâneos
- Volume do Snapshot
- Volume do membro do grupo de consistência
- Volume do par espelhado

Use uma porcentagem alta se você acredita que o volume primário sofrerá muitas mudanças ou se a vida útil de uma operação de serviço de cópia específica será muito longa.

Não é possível aumentar a capacidade reservada para um volume instantâneo que seja somente leitura. Somente os volumes snapshot que são leitura-gravação exigem capacidade reservada.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione a guia **capacidade reservada**.
3. Selecione o objeto de armazenamento para o qual deseja aumentar a capacidade reservada e clique em **aumentar a capacidade**.

   A caixa de diálogo aumentar capacidade reservada é exibida.

4. Utilize a caixa de rotação para ajustar a percentagem de capacidade.

   Se a capacidade livre não existir no pool ou no grupo de volumes que contém o objeto de armazenamento selecionado e o array de armazenamento tiver capacidade não atribuída, você poderá criar um novo pool ou grupo de volumes. Em seguida, você pode tentar novamente essa operação usando a nova capacidade livre nesse pool ou grupo de volume.

5. Clique em **aumentar**.

**Resultados**

O System Manager executa as seguintes ações:

- Aumenta a capacidade reservada para o objeto de armazenamento.
- Exibe a capacidade reservada recém-adicionada.

### Altere as configurações de capacidade reservada para um volume de par espelhado

Você pode alterar as configurações de um volume de par espelhado para ajustar o ponto percentual no qual o System Manager envia uma notificação de alerta quando a capacidade reservada para um volume de par espelhado estiver quase cheia.

**Passos**

1. Selecione **armazenamento › pools & grupos de volume**.
2. Selecione a guia **capacidade reservada**.
3. Selecione o volume do par espelhado que você deseja editar e clique em **Exibir/Editar configurações**.

   A caixa de diálogo Configurações de capacidade reservada do volume do par espelhado é exibida.

4. Altere as configurações de capacidade reservada para o volume do par espelhado, conforme apropriado.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| Alerta-me quando… | Use a caixa giratório para ajustar o ponto percentual no qual o System Manager envia uma notificação de alerta quando a capacidade reservada para um par espelhado estiver quase cheia.<br><br>Quando a capacidade reservada para o par espelhado excede o limite especificado, o System Manager envia um alerta, permitindo que você aumente a capacidade reservada.<br><br>Alterar a configuração Alerta para um par espelhado altera a configuração Alerta para todos os pares espelhados que pertencem ao mesmo grupo de consistência de espelho. |

5. Clique em **Salvar** para aplicar suas alterações.

### Par espelhado completo para volumes primários criados no sistema legado

Se você criou um volume primário em um storage array herdado que não pode ser gerenciado pelo System Manager, poderá criar o volume secundário nesse array com o System Manager.

**Sobre esta tarefa**

É possível executar o espelhamento assíncrono entre arrays legados que usam uma interface diferente e arrays mais recentes que podem ser gerenciados pelo System Manager.

- Se você estiver espelhando entre dois storage arrays que usam o System Manager, poderá ignorar essa tarefa porque já concluiu o par espelhado na sequência de criação de par espelhado.
- Execute esta tarefa na matriz de armazenamento remoto.

**Passos**

1. Selecione **armazenamento › Espelhamento assíncrono**.
2. Selecione a guia **Mirrored Pair** (par espelhado).

   A tabela pares espelhados é exibida e exibe todos os pares espelhados associados ao storage array.

3. Localize o volume do par espelhado com um status de incompleto e clique no link **Complete Mirrored pair** exibido na coluna Mirrored pair.
4. Escolha se deseja concluir a sequência de criação de par espelhado automaticamente ou manualmente selecionando um dos seguintes botões de opção:
   - **Automático** — Crie um novo volume secundário.

     Aceite as configurações padrão do lado remoto do par espelhado selecionando um pool ou grupo de volume existente onde você deseja criar o volume secundário. Utilize esta opção recomendada para alocar a capacidade reservada para o volume secundário com as predefinições.

   - **Manual** — Selecione um volume existente.

Defina seus próprios parâmetros para o volume secundário.

i. Clique em **Next** para selecionar o volume secundário.

ii. Selecione um volume existente que você deseja usar como volume secundário e clique em **Next** para alocar a capacidade reservada.

iii. Alocar a capacidade reservada. Execute um dos seguintes procedimentos:

- Aceite as predefinições.

  A configuração padrão para capacidade reservada é de 20% da capacidade do volume base e, geralmente, essa capacidade é suficiente.

- Aloque suas próprias configurações de capacidade reservada para atender às necessidades de storage de dados relacionadas ao espelhamento assíncrono.

  A capacidade necessária varia, dependendo da frequência e do tamanho das gravações de e/S no volume principal e por quanto tempo você precisa manter a capacidade. Em geral, escolha uma capacidade maior para a capacidade reservada se uma ou ambas as condições existirem:

  - Você pretende manter o par espelhado por um longo período de tempo.
  - Uma grande porcentagem de blocos de dados mudará no volume primário devido à intensa atividade de e/S. Use dados históricos de desempenho ou outros utilitários do sistema operacional para ajudá-lo a determinar a atividade típica de e/S para o volume principal.

5. Selecione **Complete**.

**Resultados**

O System Manager executa as seguintes ações:

- Cria o volume secundário no storage array remoto e aloca a capacidade reservada para o lado remoto do par espelhado.
- Inicia a sincronização inicial entre a matriz de armazenamento local e a matriz de armazenamento remoto.
- Se o volume espelhado for um volume fino, apenas os blocos alocados serão transferidos para o volume secundário durante a sincronização inicial. Essa transferência reduz a quantidade de dados que devem ser transferidos para concluir a sincronização inicial.
- Cria a capacidade reservada para o par espelhado no storage array local e no storage array remoto.

## Gerenciar pares espelhados de sincronização

### Teste a comunicação para espelhamento síncrono

Você pode testar a comunicação entre um storage array local e um storage array remoto para diagnosticar possíveis problemas de comunicação de um par espelhado que esteja participando do espelhamento síncrono.

**Sobre esta tarefa**

Dois testes diferentes são executados:

- **Comunicação** — verifica se os dois storages de armazenamento têm um caminho de comunicação. O teste de comunicação valida que a matriz de armazenamento local pode comunicar com a matriz de

armazenamento remoto e que o volume secundário associado ao par espelhado existe na matriz de armazenamento remoto.

- **Latência** — envia um comando SCSI test unit para o volume secundário na matriz de armazenamento remoto associada ao par espelhado para testar a latência mínima, média e máxima.

**Passos**

1. Selecione **armazenamento › Espelhamento síncrono**.
2. Selecione o par espelhado que deseja testar e, em seguida, selecione **Test Communication**.
3. Reveja as informações apresentadas na janela resultados e, se necessário, siga a ação corretiva indicada.

> Se o teste de comunicação falhar, o teste continuará a ser executado depois de fechar esta caixa de diálogo até que a comunicação entre o par espelhado seja restaurada.

### Suspender e retomar a sincronização para um par espelhado

Você pode usar a opção suspender e a opção continuar para controlar quando sincronizar os dados no volume primário e no volume secundário em um par espelhado.

**Sobre esta tarefa**

Se um par espelhado for suspenso manualmente, o par espelhado não será sincronizado até que seja retomado manualmente.

**Passos**

1. Selecione **armazenamento › Espelhamento síncrono**.
2. Selecione o par espelhado que pretende suspender ou retomar e, em seguida, selecione **mais › suspender** ou **mais › continuar**.

   O sistema apresenta uma confirmação.
3. Selecione **Sim** para confirmar.

**Resultados**

O System Manager executa as seguintes ações:

- Suspende ou retoma a transferência de dados entre o par espelhado sem remover a relação de espelhamento.
- Para um par espelhado *suspenso*:
  - Exibe **suspenso** na tabela par espelhado.
  - Registra todos os dados que foram gravados no volume primário do par espelhado enquanto a sincronização é suspensa.
- Para um par espelhado *retomado*, grava os dados automaticamente no volume secundário do par espelhado quando a sincronização é retomada. Não é necessária uma sincronização completa.

### Alterar função entre volumes em um par espelhado

Você pode realizar uma reversão de função entre os dois volumes em um par espelhado que estão participando do espelhamento síncrono. Essa tarefa pode ser necessária para fins administrativos ou em caso de desastre no storage array local.

### Sobre esta tarefa

Você pode rebaixar o volume primário para a função secundária ou promover o volume secundário para a função principal. Todos os hosts que estiverem acessando o volume primário têm acesso de leitura/gravação ao volume. Quando o volume primário se torna um volume secundário, apenas as gravações remotas iniciadas pelo controlador principal são gravadas no volume.

### Passos

1. Selecione **armazenamento › Espelhamento síncrono**.
2. Selecione o par espelhado que contém os volumes para os quais você deseja alterar a função e, em seguida, selecione **mais › alterar função**.

   O sistema apresenta uma confirmação.

3. Confirme se deseja alterar a função dos volumes e selecione **alterar função**.

> Se a matriz de armazenamento local não puder se comunicar com a matriz de armazenamento remota, o sistema exibirá a caixa de diálogo não pode entrar em Contato com a matriz de armazenamento quando uma alteração de função for solicitada, mas a matriz de armazenamento remota não pode ser contatada. Clique em **Sim** para forçar a mudança de função.

### Resultados

O System Manager executa a seguinte ação:

- Se o volume associado no par espelhado puder ser contatado, as funções entre os volumes serão alteradas. O System Manager promove o volume secundário no par espelhado para a função principal ou rebaixa o volume primário no par espelhado para a função secundária (dependendo da sua seleção).

## Altere as configurações de sincronização para um par espelhado

Você pode alterar a prioridade de sincronização e a política de ressincronização que o par espelhado usa para concluir a operação de ressincronização após uma interrupção de comunicação.

### Sobre esta tarefa

Você pode editar as configurações de sincronização para um par espelhado somente na matriz de armazenamento que contém o volume primário.

### Passos

1. Selecione **armazenamento › Espelhamento síncrono**.
2. Selecione o par espelhado que pretende editar e, em seguida, selecione **mais › Editar definições**.

   O sistema exibe a caixa de diálogo Exibir/Editar configurações.

3. Use a barra deslizante para editar a prioridade de sincronização.

   A prioridade de sincronização determina quanto dos recursos do sistema são usados para concluir a operação de ressincronização após uma interrupção de comunicação em comparação com as solicitações de e/S de serviço.

**Mais sobre as taxas de sincronização**

Existem cinco taxas de prioridade de sincronização:

- Mais baixo
- Baixo
- Média
- Alta
- Mais alto

Se a prioridade de sincronização estiver definida para a taxa mais baixa, a atividade de e/S será priorizada e a operação de ressincronização demorará mais tempo. Se a prioridade de sincronização estiver definida para a taxa mais alta, a operação de ressincronização será priorizada, mas a atividade de e/S para o storage array pode ser afetada.

4. Edite a política de ressincronização conforme apropriado.

   Você pode ressincronizar os pares espelhados no storage array remoto manualmente ou automaticamente.

   - **Manual** (a opção recomendada) — Selecione essa opção para exigir que a sincronização seja reiniciada manualmente após a comunicação ser restaurada para um par espelhado. Essa opção oferece a melhor oportunidade para recuperar dados.
   - **Automático** — Selecione esta opção para iniciar a ressincronização automaticamente após a comunicação ser restaurada para um par espelhado.
5. Selecione **Guardar**.

### Remova a relação do espelho síncrono

Você remove um par espelhado para remover a relação de espelhamento do volume primário no storage array local e o volume secundário no storage array remoto.

**Sobre esta tarefa**

Você também pode remover um par espelhado para corrigir um estado de par espelhado órfão. Revise as seguintes informações sobre pares espelhados órfãos:

- Existe um par espelhado órfão quando um volume de membro foi removido de um lado (local/remoto), mas não do outro lado.
- Pares espelhados órfãos são detetados quando a comunicação entre arrays é restaurada.

**Passos**

1. Selecione **armazenamento › Espelhamento síncrono**.
2. Selecione o par espelhado que pretende remover e, em seguida, selecione o **tarefas incomuns › Remover**.

   A caixa de diálogo Remover relação de espelho é exibida.
3. Confirme se deseja remover o par espelhado e clique em **Remover**.

**Resultados**

O System Manager executa as seguintes ações:

- Remove a relação de espelhamento do par espelhado na matriz de armazenamento local e na matriz de armazenamento remoto.
- Retorna o volume primário e o volume secundário para volumes não espelhados acessíveis ao host.
- Atualiza o mosaico Espelhamento síncrono com a remoção do par espelhado síncrono.

## Desativar o espelhamento

### Desativar o espelhamento assíncrono

Você pode desativar o espelhamento assíncrono nos storage arrays locais e remotos para restabelecer o uso normal de portas dedicadas nos storage arrays.

**Antes de começar**

- Você deve ter excluído todas as relações de espelho. Verifique se todos os grupos de consistência de espelho e pares espelhados foram excluídos dos storages locais e remotos.
- O storage array local e o storage array remoto devem ser conectados por meio de uma malha Fibre Channel ou de uma interface iSCSI.

**Sobre esta tarefa**

Quando você desativa o espelhamento assíncrono, nenhuma atividade espelhada pode ocorrer nos storage arrays locais e remotos.

**Passos**

1. Selecione **armazenamento › Espelhamento assíncrono**.
2. Selecione **tarefas incomuns › Desativar**.

   O sistema apresenta uma confirmação.

3. Selecione **Sim** para confirmar.

**Resultados**

- Os canais de host HBA da controladora que foram dedicados à comunicação assíncrona de espelhamento agora podem aceitar solicitações de leitura e gravação do host.
- Nenhum dos volumes desse storage array pode participar de relacionamentos espelhados como volumes primários ou volumes secundários.

### Desativar o espelhamento síncrono

Você pode desativar o recurso de espelhamento síncrono em um storage array para restabelecer o uso normal da porta host 4 do adaptador de barramento do host (HBA), que foi reservada para transmissão de dados espelhados.

**Antes de começar**

Você deve ter excluído todas as relações espelhadas síncronas. Verifique se todos os pares espelhados foram excluídos do storage array.

**Passos**

1. Selecione **armazenamento › Espelhamento síncrono**.
2. Selecione **tarefas incomuns › Desativar**.

   O sistema apresenta uma confirmação.

3. Selecione **Sim** para confirmar.

**Resultados**

- A porta de host HBA 4 da controladora, dedicada à comunicação de espelhamento síncrono, agora pode aceitar solicitações de leitura e gravação do host.
- Os volumes de capacidade reservada no storage array são excluídos.

## FAQs assíncronas

**Como o espelhamento assíncrono difere do espelhamento síncrono?**

O recurso de espelhamento assíncrono difere do recurso de espelhamento síncrono de uma maneira essencial: Captura o estado do volume de origem em um determinado ponto no tempo e copia apenas os dados que foram alterados desde a última captura de imagem.

Com o espelhamento síncrono, o estado do volume primário não é capturado em algum momento do tempo, mas sim reflete todas as alterações que foram feitas no volume primário para o volume secundário. O volume secundário é idêntico ao volume primário a cada momento porque, com este tipo de espelho, cada vez que uma gravação é feita no volume primário, uma gravação é feita no volume secundário. O host não recebe uma confirmação de que a gravação foi bem-sucedida até que o volume secundário seja atualizado com êxito com as alterações feitas no volume primário.

Com o espelhamento assíncrono, o storage array remoto não é totalmente sincronizado com o storage array local. Portanto, se o aplicativo precisar fazer a transição para o storage array remoto devido à perda do storage array local, algumas transações poderão ser perdidas.

Comparação entre os recursos de espelhamento:

| Espelhamento assíncrono | Espelhamento síncrono |
| --- | --- |
| **Método de replicação**<br><br>• **Contínuo**<br><br>O espelhamento é executado automaticamente continuamente, copiando dados de cada gravação do host. | • **Ponto no tempo**<br><br>O espelhamento é feito sob demanda ou automaticamente de acordo com uma programação definida pelo usuário. Os horários podem ser definidos na granularidade de minutos. O tempo mínimo entre sincronizações é de 10 minutos.<br><br>**Capacidade reservada** |

| Espelhamento assíncrono | Espelhamento síncrono |
| --- | --- |
| • **Múltiplo**<br><br>Um volume de capacidade reservada é necessário para cada par espelhado. | • **Single**<br><br>É necessário um único volume de capacidade reservada para todos os volumes espelhados. |
| **Comunicação** | • **ISCSI e Fibre Channel**<br><br>Suporta interfaces iSCSI e Fibre Channel entre storage arrays. |
| • **Fibre Channel**<br><br>Suporta apenas interfaces Fibre Channel entre storage arrays. | **Distância** |
| • **Ilimitado**<br><br>Suporte para distâncias praticamente ilimitadas entre a matriz de armazenamento local e a matriz de armazenamento remoto, com a distância normalmente limitada apenas pelos recursos da rede e da tecnologia de extensão de canal. | • **Restrito**<br><br>Normalmente, deve estar a cerca de 10 km (6,2 milhas) do storage array local para atender aos requisitos de latência e desempenho do aplicativo. |

**Por que não consigo acessar meu recurso de espelhamento escolhido?**

## O espelhamento é configurado na interface do Unified Manager.

O espelhamento síncrono não está disponível no storage array EF600 ou EF300.

Para ativar e configurar o espelhamento entre dois arrays, verifique o seguinte:

- O serviço Web Services Proxy deve estar em execução. (O Unified Manager é instalado em um sistema host juntamente com o Web Services Proxy.)
- O Unified Manager deve estar em execução em seu host local por meio de uma conexão HTTPS.
- Os dois storage arrays que você deseja usar para espelhamento devem ser descobertos no Unified Manager.
- O Unified Manager deve ter certificados SSL válidos para as matrizes de armazenamento. Você pode aceitar um certificado autoassinado ou instalar certificados assinados pela CA do Unified Manager.

Para obter instruções de configuração, consulte o seguinte:

- "Criar par espelhado assíncrono (no Unified Manager)"
- "Criar par espelhado síncrono (no Unified Manager)"

**O que eu preciso saber antes de criar um grupo de consistência de espelho?**

## Siga estas diretrizes antes de criar um grupo de consistência espelhada.

O espelhamento síncrono não está disponível no sistema de storage EF600 ou EF300.

Você cria um grupo de consistência no Unified Manager no assistente criar pares espelhados.

Atender aos seguintes requisitos do Unified Manager:

- O serviço Web Services Proxy deve estar em execução.
- O Unified Manager deve estar em execução em seu host local por meio de uma conexão HTTPS.
- O Unified Manager deve mostrar certificados SSL válidos para a matriz de armazenamento. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando o Unified Manager e navegando para o **certificado › Gerenciamento de certificados**.

Certifique-se também de atender aos seguintes requisitos para matrizes de armazenamento:

- Os dois storage arrays devem ser descobertos no Unified Manager.
- Cada storage array deve ter duas controladoras.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conetado à rede.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)
- Você deve saber a senha para os storages de armazenamento local e remoto.
- Seus storage arrays locais e remotos são conectados por meio de uma malha Fibre Channel ou de uma interface iSCSI.

**Espelhamento assíncrono - o que preciso saber antes de criar um par espelhado?**

## Você configura pares espelhados na interface do Unified Manager e gerencia os pares no System Manager.

Antes de criar um par espelhado, siga estas diretrizes.

- Você precisa ter dois storage arrays.
- Cada storage array deve ter duas controladoras.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conetado à rede.
- Seus storage arrays locais e remotos são conectados por meio de uma malha Fibre Channel ou de uma interface iSCSI.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)
- Você deve saber a senha para os storages de armazenamento local e remoto.
- Você precisa ter capacidade livre suficiente no storage array remoto para criar um volume secundário igual ou maior que o volume principal que deseja espelhar.
- Você instalou o Web Services Proxy e o Unified Manager. Os pares espelhados são configurados na

interface do Unified Manager.

- Os dois storage arrays são descobertos no Unified Manager.
- Seu storage array deve conter pelo menos um grupo de consistência de espelho. Você cria um grupo de consistência no Unified Manager no assistente criar pares espelhados.

**O que eu preciso saber antes de aumentar minha capacidade reservada em um volume de par espelhado?**

Normalmente, você deve aumentar a capacidade reservada quando receber um aviso de que a capacidade reservada para um par espelhado está ficando cheia. Você pode aumentar a capacidade reservada apenas em incrementos de 8 GiB.

Para operações de espelhamento assíncrono, a capacidade reservada costuma ser de 20% do volume base. Escolha uma capacidade maior para a capacidade reservada se uma ou ambas as condições existirem:

- Você pretende manter o par espelhado por um longo período de tempo.
- Uma grande porcentagem de blocos de dados mudará no volume primário devido à intensa atividade de e/S. Use dados históricos de desempenho ou outros utilitários do sistema operacional para ajudá-lo a determinar a atividade típica de e/S para o volume principal.

Você pode aumentar a capacidade reservada para um par espelhado executando uma destas ações:

- Ajuste a porcentagem de capacidade para um volume de par espelhado selecionando **armazenamento › pools and volumes groups** e clicando na guia **capacidade reservada**.
- Crie um novo volume usando a capacidade gratuita disponível em um pool ou grupo de volumes.

  Se não houver capacidade livre em nenhum pool ou grupo de volumes, você poderá adicionar capacidade não configurada na forma de unidades não utilizadas a um pool ou grupo de volumes.

**Por que não posso aumentar a capacidade reservada com o meu valor solicitado?**

Você pode aumentar a capacidade reservada apenas em incrementos de 4 GiB.

Reveja as seguintes diretrizes:

- Você precisa ter capacidade livre suficiente no pool ou no grupo de volumes para que possa ser expandido, se necessário.

  Se não houver capacidade livre em nenhum pool ou grupo de volumes, você poderá adicionar capacidade não atribuída na forma de unidades não utilizadas a um pool ou grupo de volumes.

- O volume no pool ou grupo de volumes deve ter um status ideal e não deve estar em nenhum estado de modificação.
- A capacidade livre deve existir no pool ou grupo de volumes que você deseja usar para aumentar a capacidade.

Para operações de espelhamento assíncrono, a capacidade reservada é de 20% do volume base. Use uma porcentagem maior se você acredita que o volume base sofrerá muitas mudanças ou se a expetativa de vida estimada da operação de serviço de cópia de um objeto de armazenamento será muito longa.

**Por que eu alteraria essa porcentagem?**

A capacidade reservada geralmente é de 40% do volume base para operações de snapshot e 20% do volume base para operações de espelhamento assíncrono.

Normalmente, essa capacidade é suficiente. A capacidade necessária varia, dependendo da frequência e tamanho das gravações de e/S no volume base e quanto tempo você pretende usar a operação de serviço de cópia do objeto de armazenamento.

Em geral, escolha uma porcentagem maior para a capacidade reservada se uma ou ambas as condições existirem:

- Se a vida útil de uma operação de serviço de cópia de um objeto de armazenamento específico será muito longa.
- Se uma grande porcentagem de blocos de dados mudar no volume base devido à intensa atividade de e/S. Use dados históricos de desempenho ou outros utilitários do sistema operacional para ajudá-lo a determinar a atividade típica de e/S para o volume base.

**Por que vejo mais de um candidato à capacidade reservada?**

Se houver mais de um volume em um pool ou grupo de volumes que atenda ao valor percentual de capacidade selecionado para o objeto de armazenamento, você verá vários candidatos.

Você pode atualizar a lista de candidatos recomendados alterando a porcentagem de espaço físico da unidade que deseja reservar no volume base para operações de serviço de cópia. Os melhores candidatos são exibidos com base na sua seleção.

**Por que vejo valores não disponíveis exibidos na tabela?**

A tabela lista valores não disponíveis quando os dados localizados na matriz de armazenamento remoto não estão disponíveis para serem exibidos.

Para exibir os dados do storage array remoto, inicie o System Manager do Unified Manager.

**Por que não vejo todos os meus pools e grupos de volume?**

Quando você cria um volume secundário para o par espelhado assíncrono, o sistema exibe uma lista de todos os pools qualificados e grupos de volumes para esse par espelhado assíncrono. Qualquer pool ou grupo de volume que não seja elegível para ser usado não é exibido nessa lista.

Pools ou grupos de volumes podem não ser elegíveis por qualquer um dos seguintes motivos.

- Os recursos de segurança de um pool ou grupo de volumes não correspondem.
- Um pool ou grupo de volume está em um estado não ideal.
- A capacidade de um pool ou grupo de volume é muito pequena.

**Espelhamento assíncrono - por que não vejo todos os meus volumes?**

Ao selecionar um volume primário para um par espelhado, uma lista mostra todos os

volumes elegíveis.

Quaisquer volumes que não sejam elegíveis para serem usados não são exibidos nessa lista. Os volumes não podem ser elegíveis por qualquer um dos seguintes motivos:

- O volume não é ideal.
- O volume já está participando de uma relação de espelhamento.
- Para volumes finos, a expansão automática deve estar ativada.

> Para controladores EF600 e EF300, os volumes primário e secundário de um par espelhado assíncrono devem corresponder ao mesmo protocolo, nível da bandeja, tamanho do segmento, tipo de segurança e nível RAID. Pares espelhados assíncronos não elegíveis não aparecerão na lista de volumes disponíveis.

**Espelhamento assíncrono - por que não vejo todos os volumes no storage array remoto?**

## Quando você está selecionando um volume secundário no storage array remoto, uma lista mostra todos os volumes elegíveis para esse par espelhado.

Quaisquer volumes que não sejam elegíveis para serem usados, não serão exibidos nessa lista. Os volumes podem não ser elegíveis por qualquer um dos seguintes motivos:

- O volume não é ideal.
- O volume já está participando de uma relação de espelhamento.
- Os atributos de volume fino entre o volume primário e o volume secundário não correspondem.
- Se estiver a utilizar o Data Assurance (DA), o volume primário e o volume secundário têm de ter as mesmas definições DE DA.
  - Se o volume primário for DA ativado, o volume secundário tem de ser DA ativado.
  - Se o volume primário não estiver ativado DA, o volume secundário não deve ser ativado DA.

**Por que eu atualizaria o endereço IP da minha matriz de armazenamento remoto?**

## Você atualiza o endereço IP da matriz de armazenamento remoto quando o endereço IP de uma porta iSCSI muda e a matriz de armazenamento local não consegue se comunicar com a matriz de armazenamento remoto.

Ao estabelecer uma relação de espelhamento assíncrono com uma conexão iSCSI, os storage arrays locais e remotos armazenam um Registro do endereço IP do storage array remoto na configuração de espelhamento assíncrono. Se o endereço IP de uma porta iSCSI mudar, o storage de armazenamento remoto que está tentando usar essa porta encontra um erro de comunicação.

A matriz de armazenamento com o endereço IP alterado envia uma mensagem para cada matriz de armazenamento remoto associada aos grupos de consistência de espelho configurados para espelhar uma conexão iSCSI. As matrizes de armazenamento que recebem esta mensagem atualizam automaticamente o endereço IP de destino remoto.

Se a matriz de armazenamento com o endereço IP alterado não puder enviar sua mensagem entre arrays para um storage remoto, o sistema enviará um alerta sobre o problema de conetividade. Use a opção Atualizar endereço IP remoto para restabelecer a conexão com a matriz de armazenamento local.

## FAQs de sincronização

### Como o espelhamento assíncrono difere do espelhamento síncrono?

O recurso de espelhamento assíncrono difere do recurso de espelhamento síncrono de uma maneira essencial: Captura o estado do volume de origem em um determinado ponto no tempo e copia apenas os dados que foram alterados desde a última captura de imagem.

Com o espelhamento síncrono, o estado do volume primário não é capturado em algum momento do tempo, mas sim reflete todas as alterações que foram feitas no volume primário para o volume secundário. O volume secundário é idêntico ao volume primário a cada momento porque, com este tipo de espelho, cada vez que uma gravação é feita no volume primário, uma gravação é feita no volume secundário. O host não recebe uma confirmação de que a gravação foi bem-sucedida até que o volume secundário seja atualizado com êxito com as alterações feitas no volume primário.

Com o espelhamento assíncrono, o storage array remoto não é totalmente sincronizado com o storage array local. Portanto, se o aplicativo precisar fazer a transição para o storage array remoto devido à perda do storage array local, algumas transações poderão ser perdidas.

Comparação entre os recursos de espelhamento:

| Espelhamento assíncrono | Espelhamento síncrono |
| --- | --- |
| **Método de replicação** | • **Ponto no tempo**<br><br>O espelhamento é feito sob demanda ou automaticamente de acordo com uma programação definida pelo usuário. Os horários podem ser definidos na granularidade de minutos. O tempo mínimo entre sincronizações é de 10 minutos. |
| • **Contínuo**<br><br>O espelhamento é executado automaticamente continuamente, copiando dados de cada gravação do host. | **Capacidade reservada** |
| • **Múltiplo**<br><br>Um volume de capacidade reservada é necessário para cada par espelhado. | • **Single**<br><br>É necessário um único volume de capacidade reservada para todos os volumes espelhados. |
| **Comunicação** | • **ISCSI e Fibre Channel**<br><br>Suporta interfaces iSCSI e Fibre Channel entre storage arrays. |

| Espelhamento assíncrono | Espelhamento síncrono |
| --- | --- |
| • **Fibre Channel**<br><br>Suporta apenas interfaces Fibre Channel entre storage arrays. | **Distância** |
| • **Ilimitado**<br><br>Suporte para distâncias praticamente ilimitadas entre a matriz de armazenamento local e a matriz de armazenamento remoto, com a distância normalmente limitada apenas pelos recursos da rede e da tecnologia de extensão de canal. | • **Restrito**<br><br>Normalmente, deve estar a cerca de 10 km (6,2 milhas) do storage array local para atender aos requisitos de latência e desempenho do aplicativo. |

**Espelhamento síncrono - por que não vejo todos os meus volumes?**

Ao selecionar um volume primário para um par espelhado, uma lista mostra todos os volumes elegíveis.

Quaisquer volumes que não sejam elegíveis para serem usados não são exibidos nessa lista. Os volumes podem não ser elegíveis por qualquer um dos seguintes motivos:

- O volume é um volume não padrão, como um volume instantâneo ou um volume fino.
- O volume não é ideal.
- O volume já está participando de uma relação de espelhamento.

**Espelhamento síncrono - por que não vejo todos os volumes no storage array remoto?**

Quando você está selecionando um volume secundário no storage array remoto, uma lista mostra todos os volumes elegíveis para esse par espelhado.

Quaisquer volumes que não sejam elegíveis para serem usados, não serão exibidos nessa lista. Os volumes podem não ser elegíveis por qualquer um dos seguintes motivos:

- O volume é um volume não padrão, como um volume instantâneo ou um volume fino.
- O volume não é ideal.
- O volume já está participando de uma relação de espelhamento.
- Se estiver a utilizar o Data Assurance (DA), o volume primário e o volume secundário têm de ter as mesmas definições DE DA.
  - Se o volume primário for DA ativado, o volume secundário tem de ser DA ativado.
  - Se o volume primário não estiver ativado DA, o volume secundário não deve ser ativado DA.

**Espelhamento síncrono - o que eu preciso saber antes de criar um par espelhado?**

Você configura pares espelhados na interface do Unified Manager e gerencia os pares no System Manager.

Antes de criar um par espelhado, siga estas diretrizes:

- Você precisa ter dois storage arrays.
- Cada storage array deve ter duas controladoras.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conetado à rede.
- Seus storage arrays locais e remotos são conectados por meio de uma malha Fibre Channel.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)
- Você deve saber a senha para os storages de armazenamento local e remoto.
- Você precisa ter capacidade livre suficiente no storage array remoto para criar um volume secundário igual ou maior que o volume principal que deseja espelhar.
- Você instalou o Web Services Proxy e o Unified Manager. Os pares espelhados são configurados na interface do Unified Manager.
- Os dois storage arrays são descobertos no Unified Manager.

**Qual o impactos que a prioridade de sincronização tem nas taxas de sincronização?**

## A prioridade de sincronização define quanto tempo de processamento é alocado para atividades de sincronização em relação ao desempenho do sistema.

O proprietário do controlador do volume primário executa esta operação em segundo plano. Ao mesmo tempo, o proprietário do controlador processa gravações de e/S locais no volume principal e gravações remotas associadas no volume secundário. Como a ressincronização desvia os recursos de processamento do controlador da atividade de e/S, a ressincronização pode ter um impacto no desempenho do aplicativo host.

Mantenha essas diretrizes em mente para ajudá-lo a determinar quanto tempo uma prioridade de sincronização pode levar e como as prioridades de sincronização podem afetar o desempenho do sistema.

**Sobre as taxas de prioridade de sincronização**

Estas tarifas prioritárias estão disponíveis:

- Mais baixo
- Baixo
- Média
- Alta
- Mais alto

A taxa de prioridade mais baixa suporta o desempenho do sistema, mas a ressincronização leva mais tempo. A taxa de prioridade mais alta é compatível com a ressincronização, mas o desempenho do sistema pode estar comprometido.

Estas orientações aproximam aproximadamente as diferenças entre as prioridades.

| Taxa de prioridade para sincronização completa | Tempo decorrido em comparação com a taxa de sincronização mais elevada |
| --- | --- |
| Mais baixo | Aproximadamente oito vezes, desde que na taxa de prioridade mais alta. |
| Baixo | Aproximadamente seis vezes, desde que na taxa de prioridade mais alta. |
| Média | Aproximadamente três vezes e meia, desde que com a taxa de prioridade mais alta. |
| Alta | Aproximadamente o dobro do tempo na taxa de prioridade mais alta. |

As cargas de tamanho de volume e taxa de e/S do host afetam as comparações de tempo de sincronização.

#### Por que é recomendável usar uma política de sincronização manual?

A ressincronização manual é recomendada porque permite gerenciar o processo de ressincronização de uma forma que forneça a melhor oportunidade para recuperar dados.

Se você usar uma política de ressincronização automática e ocorrerem problemas de comunicação intermitente durante a ressincronização, os dados no volume secundário poderão ser corrompidos temporariamente. Quando a ressincronização é concluída, os dados são corrigidos.

# Armazenamento remoto

## Visão geral da funcionalidade de armazenamento remoto

Se tiver a funcionalidade armazenamento remoto, pode importar dados de um sistema de armazenamento remoto para a sua matriz de armazenamento.

#### O que é o recurso de armazenamento remoto?

O recurso *armazenamento remoto* permite importar dados de um sistema de armazenamento remoto para um sistema de armazenamento local e-Series. O sistema remoto pode ser outro sistema e-Series ou um sistema de outro fornecedor. Esse recurso é útil quando você deseja otimizar a migração de dados com o mínimo de tempo de inatividade, como durante atualizações de equipamentos.

Para usar o armazenamento remoto, esse recurso deve estar habilitado no ID do submodelo (SMID).

Saiba mais:

- "Como o armazenamento remoto funciona"
- "Terminologia de armazenamento remoto"
- "Requisitos de armazenamento remoto"

- "Requisitos de volume de armazenamento remoto"

#### Como posso importar dados com esta funcionalidade?

Usando o assistente de armazenamento remoto, você mapeia um dispositivo de armazenamento remoto (a origem da importação de dados) para um volume de destino no sistema e-Series. Este assistente está disponível no **armazenamento › armazenamento remoto**.

Saiba mais:

- "Importar armazenamento remoto"
- "Gerenciar o progresso da importação de dados"

## Conceitos

#### Como o armazenamento remoto funciona

O recurso armazenamento remoto permite importar dados de um sistema de storage remoto para um sistema de storage local e-Series. Esse recurso é útil quando você deseja otimizar a migração de dados com o mínimo de tempo de inatividade, como durante atualizações de equipamentos.

Para configurar o recurso armazenamento remoto, você deve configurar o hardware e usar o Gerenciador do sistema para criar um objeto de armazenamento remoto. Quando esta configuração estiver concluída, o processo de importação será iniciado.

##### Configuração do hardware

Use o fluxo de trabalho a seguir para preparar as conexões de hardware.

Estas etapas são descritas mais adiante no guia do usuário do recurso armazenamento remoto, que está disponível no centro de documentação da série e e SANtricity em "Visão geral dos volumes de armazenamento remoto" , e no "Relatório técnico de armazenamento remoto".

No sistema de storage local e-Series:

1. Certifique-se de que cada controlador tem uma ligação iSCSI ao sistema de armazenamento remoto. Com essa conexão, o sistema local e-Series atua como um iniciador iSCSI que pode ser configurado como um host no sistema remoto.
2. Crie um volume de destino para a operação de importação. Certifique-se de que o volume tem uma capacidade igual ou superior ao volume de origem no sistema de armazenamento remoto, tem um tamanho de bloco correspondente e não está mapeado. "Criar volumes"Consulte .
3. Reúna o IQN (iSCSI Qualified Name) para o sistema e-Series local a partir da interface do System Manager. O IQN será usado posteriormente para configurar o sistema e-Series local como um host no sistema de storage remoto. No System Manager, aceda a: Menu:Definições[sistema > Definições iSCSI > Target IQN].

No sistema de armazenamento remoto:

1. Configure o sistema e-Series local como um host no sistema remoto, usando seu IQN. Certifique-se de definir o tipo de host apropriado, da seguinte forma:

- Se o sistema remoto for um modelo e-Series, "Visão geral dos clusters de hosts e host"consulte . Use um tipo de host de "padrão de fábrica".
- Se o sistema remoto for de outro fornecedor, selecione um tipo de host apropriado com base nas opções disponíveis.

2. Pare todas as I/os, desmonte quaisquer sistemas de arquivos e remova quaisquer atribuições a hosts ou aplicativos para o volume de origem.
3. Atribua o volume ao recém-criado host local do sistema de storage e-Series.
4. Para o volume de origem selecionado, reúna as seguintes informações do sistema de armazenamento remoto para que a importação possa ser criada:
   - Nome qualificado iSCSI (IQN)
   - Endereço IP iSCSI
   - Número LUN do volume de origem

#### Configuração do System Manager

Use o seguinte fluxo de trabalho para criar um objeto de armazenamento remoto para a importação:

1. Usando o assistente de armazenamento remoto na interface do System Manager, mapeie um dispositivo de armazenamento remoto (a origem da importação de dados) para um volume de destino no sistema e-Series. Quando você seleciona **Finish**, o processo de importação é iniciado.
2. Monitorize a importação a partir da caixa de diálogo View Operations (Visualizar operações) ou do painel Operations in Progress (operações em curso). Se necessário, você também pode pausar e retomar o processo.
3. Opcionalmente, quebre a conexão entre os volumes de origem e destino quando a importação for concluída ou mantenha a conexão para importações futuras.

### Terminologia de armazenamento remoto

Saiba como os termos de armazenamento remoto se aplicam ao storage array.

| Prazo | Descrição |
|---|---|
| IQN | Identificador de nome qualificado iSCSI (IQN), que é um nome exclusivo para um iniciador iSCSI ou destino. |
| LUN | Número de unidade lógica, que é usado para identificar uma unidade lógica que pode ser apresentada a um host para acesso. |
| Sistema de storage remoto | O sistema de storage onde os dados residem inicialmente. O sistema de storage remoto pode ser um modelo e-Series ou um sistema de outro fornecedor. |
| Dispositivo de armazenamento remoto | O dispositivo físico ou lógico em que os dados são inicialmente armazenados no sistema remoto. Em um sistema de storage e-Series, isso é chamado de "volume". |

| Prazo | Descrição |
| --- | --- |
| Objeto de storage remoto | Um objeto que contém informações que permite ao sistema e-Series identificar e se conetar ao sistema de storage remoto. Essas informações incluem os endereços IQN e IP do sistema de armazenamento remoto. O objeto de storage remoto representa a comunicação entre o sistema de storage remoto e o sistema e-Series. |
| Volume de armazenamento remoto | Um volume padrão no sistema e-Series que permite o acesso aos dados a um dispositivo de storage remoto. |
| Volume | Um contentor no qual os dados são armazenados. É o componente lógico criado para o host acessar os dados. |

### Requisitos do recurso de armazenamento remoto

Antes de usar o recurso de armazenamento remoto, revise os seguintes requisitos e restrições.

#### Protocolos compatíveis

São suportados os seguintes protocolos:

- ISCSI
- IPv4

Para obter informações atualizadas sobre suporte e configuração do e-Series, consulte "Ferramenta de Matriz de interoperabilidade do NetApp".

#### Requisitos de hardware

O sistema de storage e-Series deve incluir:

- Dois controladores (modo duplex)
- Conexões iSCSI para ambos os controladores e-Series para se comunicar com o sistema de armazenamento remoto através de uma ou mais conexões iSCSI
- SANtricity os 11,71 ou superior
- Recurso de armazenamento remoto habilitado no ID do submodelo (SMID)

O sistema remoto pode ser um sistema de storage e-Series ou um sistema de outro fornecedor. Deve incluir:

- Interfaces compatíveis com iSCSI

#### Restrições

O recurso de armazenamento remoto tem as seguintes restrições:

- O espelhamento deve estar desativado.
- O volume de destino no sistema e-Series não deve ter instantâneos.
- O volume de destino no sistema e-Series não deve ser mapeado para nenhum host antes que a

importação seja iniciada.

- O volume de destino no sistema e-Series deve ter o provisionamento de recursos desativado.
- Mapeamentos diretos do volume de armazenamento remoto para um host ou vários hosts não são suportados.
- O proxy de serviços da Web não é suportado.
- Segredos CHAP iSCSI não são suportados.
- O smcli não é suportado.
- O VMware datastore não é compatível.
- Apenas um sistema de armazenamento no par de relacionamento/importação pode ser atualizado de uma vez em que há um par de importação presente.

**Requisitos de volume de armazenamento remoto**

## Os volumes utilizados para importações devem satisfazer os requisitos de tamanho, estado e outros critérios.

#### Volume de armazenamento remoto

O volume de origem de uma importação é chamado de "volume de armazenamento remoto". Este volume deve satisfazer os seguintes critérios:

- Não pode fazer parte de outra importação
- Tem de ter um estado online

Após a importação começar, o firmware do controlador cria um volume de armazenamento remoto em segundo plano. Devido a esse processo em segundo plano, o volume de armazenamento remoto não é gerenciável no System Manager e só pode ser usado para a operação de importação.

Depois que ele é criado, o volume de storage remoto é Tratado como qualquer outro volume padrão no sistema e-Series, com as seguintes exceções:

- Pode ser usado como proxies para o dispositivo de armazenamento remoto.
- Não pode ser usado como candidatos a outras cópias de volume ou snapshots.
- Não é possível alterar a definição Data Assurance enquanto a importação estiver em curso.
- Não pode ser mapeado para nenhum host, porque eles são reservados estritamente para a operação de importação.

Cada volume de armazenamento remoto está associado a apenas um objeto de armazenamento remoto; no entanto, um objeto de armazenamento remoto pode ser associado a vários volumes de armazenamento remoto. O volume de armazenamento remoto é identificado de forma exclusiva usando uma combinação das seguintes opções:

- Identificador de objeto de armazenamento remoto
- Número LUN do dispositivo de armazenamento remoto

#### Candidatos ao volume-alvo

O volume de destino é o volume de destino no sistema e-Series local. O volume de destino deve satisfazer os seguintes critérios:

- Deve ser um volume RAID/DDP.
- Tem de ter uma capacidade igual ou superior ao volume de armazenamento remoto.
- Deve ter um tamanho de bloco que seja o mesmo que o volume de armazenamento remoto.
- Tem de ter um estado válido (ótimo).
- Não pode ter nenhuma das seguintes relações: Cópia de volume, cópias snapshot, espelhamento assíncrono ou síncrono.
- Não pode estar passando por nenhuma operação de reconfiguração: Expansão dinâmica de volume, expansão dinâmica de capacidade, tamanho de segmento dinâmico, migração dinâmica de RAID, redução dinâmica de capacidade ou desfragmentação.
- Não pode ser mapeado para um host antes que a importação seja iniciada (no entanto, ele pode ser mapeado depois que a importação for concluída).
- Não é possível ativar o Flash Read Cache (FRC).

O System Manager verifica automaticamente esses requisitos como parte do assistente Importar armazenamento remoto. Apenas os volumes que atendem a todos os requisitos são exibidos para a seleção do volume de destino.

## Gerenciar o armazenamento remoto

### Importar armazenamento remoto

Para iniciar uma importação de armazenamento de um sistema remoto para um sistema de armazenamento local e-Series, use o assistente Importar armazenamento remoto.

#### Antes de começar

- O sistema de storage e-Series deve ser configurado para se comunicar com o sistema de storage remoto.

> A configuração do hardware é descrita no guia do usuário do recurso armazenamento remoto, que está disponível no centro de documentação do e-Series e do SANtricity em "Configurar hardware", e no "Relatório técnico de armazenamento remoto".

- Para o sistema de armazenamento remoto, reúna as seguintes informações:
  - IQN iSCSI
  - Endereços IP iSCSI
  - Número LUN do dispositivo de armazenamento remoto (volume de origem)
- Para o sistema de storage local e-Series, crie ou selecione um volume a ser usado para a importação de dados. "Criar volumes"Consulte . O volume de destino deve atender aos seguintes requisitos:
  - Corresponde ao tamanho do bloco do dispositivo de armazenamento remoto (o volume de origem).
  - Tem uma capacidade igual ou superior ao dispositivo de armazenamento remoto.
  - Tem um estado de ótimo e está disponível.

Para obter uma lista completa de requisitos, "Requisitos de volume de storage remoto"consulte .

- **Recomendado:** Faça backup de volumes no sistema de armazenamento remoto antes de iniciar o processo de importação.

#### Sobre esta tarefa

Nessa tarefa, você cria um mapeamento entre o dispositivo de storage remoto e um volume no sistema de storage local e-Series. Quando terminar a configuração, a importação começa.

> Como muitas variáveis podem afetar a operação de importação e seu tempo de conclusão, recomendamos que você primeiro execute importações menores de "teste". Use esses testes para garantir que todas as conexões funcionem conforme esperado e que a operação de importação seja concluída em um período de tempo apropriado.

**Passos**

1. Selecione **armazenamento › armazenamento remoto**.
2. Clique em **Importar armazenamento remoto**.

   É apresentado um assistente para importar armazenamento remoto.

3. Em **passo 1a** do painel Configurar origem, insira as informações de conexão. Se pretender adicionar outra ligação iSCSI, clique em **Adicionar outro endereço IP** para incluir um endereço IP adicional para o armazenamento remoto. Quando terminar, clique em **seguinte**.

   **Detalhes do campo**

   | Definição | Descrição |
   |---|---|
   | Nome | Insira um nome para o dispositivo de armazenamento remoto para identificá-lo na interface do System Manager.<br><br>Um nome pode incluir até 30 carateres e pode conter apenas letras, números e os seguintes carateres especiais: Sublinhado (_), traço (-) e sinal de hash ( Um nome não pode conter espaços. |
   | Propriedades de ligação iSCSI | Introduza as propriedades de ligação do dispositivo de armazenamento remoto:<br><br>• **Nome qualificado iSCSI (IQN)**: Insira o IQN iSCSI.<br>• **Endereço IP**: Introduza o endereço IPv4.<br>• **Porta**: Insira o número da porta a ser usada para comunicações entre os dispositivos de origem e destino. Por padrão, o número da porta é 3260. |

   Depois de clicar em **seguinte**, o **passo 1b** do painel Configurar origem é exibido.

4. No campo **LUN**, selecione o número LUN do dispositivo de armazenamento remoto a ser usado como origem e clique em **Next**.

   O painel Configurar destino abre e exibe os candidatos de volume para servir como destino para a importação. Alguns volumes não são exibidos na lista de candidatos devido ao tamanho do bloco, capacidade ou disponibilidade de volume.

5. Na tabela, selecione um volume de destino no sistema de storage e-Series. Se necessário, use o controle deslizante para alterar a prioridade de importação. Clique em **seguinte**. Confirme a operação na caixa de diálogo seguinte, digitando `continue` e clicando em **continuar**.

Se o volume de destino tiver uma capacidade maior que o volume de origem, essa capacidade adicional não será reportada ao host conetado ao sistema e-Series. Para usar a nova capacidade, você deve executar uma operação de expansão do sistema de arquivos no host depois que a operação de importação for concluída e for desconetada.

Depois de confirmar a configuração na caixa de diálogo, é apresentado o painel Review (Revisão).

6. No painel Review (Revisão), verifique se as definições estão corretas e, em seguida, clique em **Finish** (concluir) para iniciar a importação.

   Outra caixa de diálogo será aberta perguntando se você deseja iniciar outra importação.

7. Se necessário, clique em **Yes** para criar outra importação de armazenamento remoto. Clicar em **Sim** retorna para **Etapa 1a** do painel Configurar origem, onde você pode selecionar a configuração existente ou adicionar uma nova. Se não quiser criar outra importação, clique em **no** para sair da caixa de diálogo.

   Assim que o processo de importação começar, todo o volume de destino é substituído pelos dados copiados. Se o host gravar novos dados no volume de destino durante esse processo, esses novos dados serão propagados de volta para o dispositivo remoto (volume de origem).

8. Visualize o progresso da operação na caixa de diálogo View Operations (Visualizar operações) no painel Remote Storage (armazenamento remoto).

**Resultados**

O tempo necessário para concluir a operação de importação depende do tamanho do sistema de armazenamento remoto, da configuração de prioridade para a importação e da quantidade de carga de e/S em ambos os sistemas de armazenamento e seus volumes associados.

Quando a importação estiver concluída, o volume local é uma cópia do dispositivo de armazenamento remoto.

**Depois de terminar**

Quando estiver pronto para quebrar a relação entre os dois volumes, selecione **Disconnect** no objeto de importação da visualização operações em andamento. Uma vez que a relação é desconetada, o desempenho do volume local retorna ao normal e não é mais afetado pela conexão remota.

### Gerenciar o progresso das importações de armazenamento remoto

Após o início do processo de importação, você pode visualizar e tomar medidas sobre seu progresso.

**Sobre esta tarefa**

Para cada operação de importação, a caixa de diálogo operações em andamento exibe uma porcentagem de conclusão e tempo estimado restante. As ações incluem alterar a prioridade de importação, parar e retomar as operações e desconetar da operação.

Também pode visualizar operações em curso a partir da página inicial (**Página inicial › Mostrar operações em andamento**).

**Passos**

1. Na página armazenamento remoto, selecione **Exibir operações**.

   A caixa de diálogo operações em andamento é exibida.

2. Se desejar, use os links na coluna **ações** para parar e retomar, alterar prioridade ou desconetar de uma operação.
   - **Alterar prioridade** — Selecione **alterar prioridade** para alterar a prioridade de processamento de uma operação em andamento ou pendente. Aplique uma prioridade à operação e clique em **OK**.
   - **Stop** — Selecione **Stop** para pausar a cópia de dados do dispositivo de armazenamento remoto. A relação entre o par de importação ainda está intacta e você pode selecionar **Resume** quando estiver pronto para continuar a operação de importação.
   - **Resume** — Selecione **Resume** para iniciar um processo interrompido ou com falha de onde parou. Em seguida, aplique uma prioridade à operação Retomar e clique em **OK**. Esta operação *não* reinicia a importação desde o início. Se quiser reiniciar o processo desde o início, selecione **Disconnect** e, em seguida, crie novamente a importação através do assistente Importar armazenamento remoto.
   - **Disconnect** — Selecione **Disconnect** para quebrar a relação entre os volumes de origem e destino para uma operação de importação que tenha parado, concluído ou falhado.

#### Modificar as definições de ligação para armazenamento remoto

Pode editar, adicionar ou eliminar definições de ligação para qualquer configuração de armazenamento remoto através da opção Ver/Editar definições.

##### Sobre esta tarefa

Fazer alterações nas propriedades de conexão afetará as importações em andamento. Para evitar interrupções, faça apenas alterações nas propriedades de conexão quando as importações não estiverem em execução.

##### Passos

1. Selecione **armazenamento › armazenamento remoto**.
2. Na lista, selecione o objeto de armazenamento remoto que deseja modificar.
3. Clique em **Exibir/Editar configurações**.

   A caixa de diálogo Configurações de armazenamento remoto é exibida.

4. Clique na guia **Propriedades da conexão**.

   São apresentadas as definições de endereço IP e de porta configuradas para a importação de armazenamento remoto.

5. Execute uma das seguintes ações:
   - **Editar** — clique em **Editar** ao lado do item de linha correspondente para o objeto de armazenamento remoto. Introduza o endereço IP revisto e/ou as informações da porta nos campos.
   - **Add** — clique em **Add** e, em seguida, insira o novo endereço IP e as informações da porta nos campos fornecidos. Clique em **Add** para confirmar e, em seguida, a nova conexão aparece na lista de objetos de armazenamento remoto.
   - **Excluir** — Selecione a conexão desejada na lista e clique em **Excluir**. Confirme a operação digitando `delete` no campo fornecido e clique em **Excluir**. A conexão é removida da lista de objetos de armazenamento remoto.
6. Clique em **Salvar**.

   As configurações de conexão modificadas são aplicadas ao objeto de armazenamento remoto.

### Remova o objeto de armazenamento remoto

Depois que uma importação for concluída, você poderá remover um objeto de armazenamento remoto se não quiser mais copiar dados entre os dispositivos locais e remotos.

#### Antes de começar

Certifique-se de que nenhuma importação está associada ao objeto de armazenamento remoto que pretende remover.

#### Sobre esta tarefa

Quando você remove um objeto de armazenamento remoto, as conexões entre os dispositivos locais e remotos são removidas.

#### Passos

1. Selecione **armazenamento › armazenamento remoto**.
2. Na lista, selecione o objeto de armazenamento remoto que deseja remover.
3. Clique em **Remover**.

   É apresentada a caixa de diálogo Confirm Remove Remote Storage Connection (confirmar remoção da ligação de armazenamento remoto).

4. Confirme a operação digitando `remove` e, em seguida, clicando em **Remover**.

   O objeto de armazenamento remoto selecionado é removido.

## FAQs

### O que eu preciso saber antes de criar uma conexão de armazenamento remoto?

Para configurar a funcionalidade armazenamento remoto, tem de ligar diretamente o dispositivo remoto e os sistemas de armazenamento de destino através de iSCSI.

Para configurar a ligação do sistema iSCSI, consulte:

- "Configurar portas iSCSI"
- "Relatório técnico de armazenamento remoto"

### Por que estou sendo solicitado a remover meus volumes remotos?

Quando atinge o número máximo de volumes remotos, o sistema de armazenamento deteta automaticamente quaisquer volumes remotos não utilizados e solicita que os remova.

Existem alguns casos em que os volumes remotos não utilizados não são limpos durante o processo de criação. Antes de iniciar quaisquer operações de importação adicionais, verifique se os seus sistemas são ideais e as ligações de rede são estáveis.

### Por que não vejo todos os meus volumes na minha matriz de destino?

Ao configurar uma importação para o recurso armazenamento remoto, você pode notar que alguns volumes não aparecem na lista de candidatos alvo devido ao tamanho do bloco, capacidade ou disponibilidade de volume.

Para aparecer na lista, os candidatos ao volume devem ter:

- Capacidade igual ou superior ao volume remoto.
- Tamanho do bloco que é o mesmo que o volume remoto.
- Status atual do Optimal.

Os candidatos a volumes são excluídos da lista se tiverem:

- Qualquer uma das seguintes relações: Cópia de volume, snapshot ou espelhamento.
- Operação de reconfiguração em curso.
- Mapeamento para outro dispositivo (host ou cluster de host).
- Ler cache flash ativado.

### O que eu preciso saber sobre o volume remoto em uma importação?

Ao utilizar a funcionalidade armazenamento remoto, tenha em atenção que o volume remoto é a origem da origem dos dados.

Quando a importação está em andamento, os dados são transferidos do volume remoto para o volume de destino no sistema de armazenamento de destino. Esses dois volumes devem ter um tamanho de bloco correspondente.

### O que eu preciso saber antes de iniciar uma importação de armazenamento remoto?

O recurso armazenamento remoto permite copiar dados de um sistema de storage remoto para um volume em um sistema de storage local e-Series. Antes de usar esse recurso, revise as diretrizes a seguir.

#### Configuração

Antes de criar a importação de armazenamento remoto, você deve concluir as seguintes ações e verificar as seguintes condições:

- Certifique-se de que cada controlador do sistema de storage local e-Series tem uma conexão iSCSI ao sistema de storage remoto.
- No sistema de storage local do e-Series, crie um volume de destino para a operação de importação. Certifique-se de que o volume tem uma capacidade igual ou superior ao volume de origem, tem um tamanho de bloco que corresponde ao volume de origem e não está mapeado. "Criar volumes"Consulte .
- Configure o sistema de storage local e-Series como um host no sistema remoto usando seu nome qualificado iSCSI (IQN). Pode visualizar o IQN a partir do **Definições › sistema › Definições iSCSI › IQN de destino**. Além disso, certifique-se de definir o tipo de host apropriado com base no sistema que está sendo usado.
- Pare todas as I/os, desmonte quaisquer sistemas de arquivos e remova quaisquer atribuições a hosts ou

aplicativos para o volume selecionado no sistema de storage remoto.

- Atribua o volume ao sistema de storage remoto ao recém-criado host local do sistema de storage e-Series.
- Reúna as seguintes informações do sistema de armazenamento remoto para que a importação possa ser criada:
  - Nome qualificado iSCSI (IQN)
  - Endereço IP iSCSI
  - O número LUN do dispositivo de armazenamento remoto, onde os dados de origem são originários
- Assim que o processo de importação começar, todo o volume de destino local é substituído pelos dados copiados. Todos os novos dados gravados no volume de destino local são propagados para o volume no dispositivo de armazenamento remoto após a criação da importação. Portanto, recomendamos que você faça backup de volumes no sistema de armazenamento remoto antes de iniciar o processo de importação.

#### Processo de importação

As etapas a seguir descrevem o processo de importação.

1. Acesse a interface do System Manager e vá para a página **armazenamento remoto**. Selecione **Importar** para iniciar uma nova criação de importação. Para obter instruções detalhadas, "Importar armazenamento remoto"consulte .

   Se você quiser executar uma importação off-line, não mapeie o volume de destino até que a importação seja concluída.

2. Monitorize o progresso da importação.

   Assim que a importação for iniciada, o volume de destino poderá ser mapeado. O tempo necessário para concluir a operação de importação depende do tamanho do dispositivo de armazenamento remoto (volume de origem), da configuração de prioridade para a importação e da quantidade de carga de e/S em ambos os sistemas de armazenamento e seus volumes associados.

   Após a conclusão da importação, o volume de destino é uma cópia da origem.

3. Quando estiver pronto para quebrar a relação de mapeamento, execute um **Disconnect** no objeto de importação do painel **Operations in Progress**.

Quando a importação é desconetada, o desempenho do destino local retorna ao normal e não é mais afetado pela conexão remota.

#### Restrições

O recurso de armazenamento remoto tem as seguintes restrições:

- O espelhamento deve estar desativado.
- O volume de destino no sistema e-Series não deve ter instantâneos.
- O volume de destino no sistema e-Series não deve ser mapeado para nenhum host antes que a importação seja iniciada.
- O volume de destino no sistema e-Series deve ter o provisionamento de recursos desativado.
- Mapeamentos diretos do volume de armazenamento remoto para um host ou vários hosts não são suportados.
- O proxy de serviços da Web não é suportado.

- Segredos CHAP iSCSI não são suportados.
- O smcli não é suportado.
- O VMware datastore não é compatível.
- Apenas um sistema de armazenamento no par de relacionamento/importação pode ser atualizado de uma vez em que há um par de importação presente.

#### Informações adicionais

Para obter mais informações sobre a funcionalidade de armazenamento remoto, consulte a "Relatório técnico de armazenamento remoto" .

# Componentes de hardware

## Visão geral dos componentes de hardware

Você pode verificar o status do componente na página hardware e executar algumas funções relacionadas a esses componentes.

#### Que componentes posso gerir?

Pode verificar o estado do componente e executar algumas funções relacionadas com estes componentes:

- **Prateleiras** — Um *shelf* é um componente que contém o hardware do storage array (controladores, coletores de energia/ventilador e unidades). As gavetas estão disponíveis em três tamanhos para acomodar até 12, 24 ou 60 unidades.
- **Controladores** — Um *controller* é o hardware e firmware combinados que implementa funções de storage e gerenciamento. Ele inclui a memória cache, o suporte da unidade e as portas para conexões de host.
- **Unidades** — Uma *unidade* pode ser uma unidade de disco rígido (HDD) ou uma unidade de estado sólido (SSD). Dependendo do tamanho da gaveta, até 12, 24 ou 60 unidades podem ser instaladas na gaveta.

Saiba mais:

- "Página de hardware"
- "Terminologia de hardware"

#### Como posso ver componentes de hardware?

Vá para a página hardware, que fornece uma representação gráfica dos componentes físicos da matriz de armazenamento. Você pode alternar entre as vistas frontal e traseira das prateleiras de matriz selecionando a guia **Drives** ou **Controllers** no canto superior direito da exibição de prateleira.

Saiba mais:

- "Exibir o status e as configurações do componente do compartimento"
- "Ver as definições do controlador"
- "Ver o estado e as definições da unidade"

## Informações relacionadas

Saiba mais sobre conceitos relacionados ao hardware:

- "estados do controlador"
- "estados da unidade"
- "Proteção contra perda de prateleira e proteção contra perda de gaveta"

## Conceitos

### Página de hardware e componentes

A página hardware fornece uma representação gráfica dos componentes físicos da matriz de armazenamento. A partir daqui, você pode verificar o status do componente e executar algumas funções relacionadas a esses componentes.

#### Compartimentos

Uma gaveta é um componente que contém o hardware para o storage array (controladoras, coletores de energia/ventoinhas e unidades). Existem dois tipos de prateleiras:

- **Compartimento de controladora** — contém as unidades, os coletores de energia/ventilador e os controladores.
- **Compartimento de unidades** (ou **compartimento de expansão**) — contém unidades, coletores de energia/ventilador e dois módulos de entrada/saída (IOMs). As IOMs, também conhecidas como módulos de serviço ambiental (ESMs), incluem portas SAS que conetam o compartimento de unidades ao compartimento de controladora.

As gavetas estão disponíveis em três tamanhos para acomodar até 12, 24 ou 60 unidades. Cada compartimento inclui um número de ID, que é atribuído pelo firmware da controladora. O ID aparece no canto superior esquerdo da exibição da prateleira.

A exibição do compartimento na página hardware mostra os componentes frontal ou traseiro. Você pode alternar entre as duas visualizações selecionando as guias **Drives** ou **Controller** no canto superior direito da exibição da prateleira. Você também pode selecionar **Mostrar tudo frontal** ou **Mostrar tudo de volta** na parte inferior da página. As vistas frontal e traseira mostram o seguinte:

- **Componentes dianteiros** — unidades e compartimentos de unidades vazios.
- **Componentes traseiros** — Controladores e coletores de energia/ventilador (para compartimentos de controladores) ou IOMs e coletores de energia/ventilador (para compartimentos de unidades).

Você pode executar as seguintes funções relacionadas às prateleiras:

- Ligue a luz de localização da prateleira, para que você possa encontrar a localização física da prateleira no gabinete ou rack.
- Altere o número de ID mostrado no canto superior esquerdo da exibição da prateleira.
- Visualize as configurações do compartimento, como os tipos de unidades instaladas e o número de série.
- Mova as exibições do compartimento para cima ou para baixo para corresponder ao layout físico no storage de armazenamento.

#### Controladores

Um controlador é o hardware e firmware combinados que implementa funções de storage e gerenciamento. Ele inclui a memória cache, suporte à unidade e suporte à interface do host.

Você pode executar as seguintes funções relacionadas aos controladores:

- Configure as portas de gerenciamento para endereços IP e velocidade.
- Configurar conexões de host iSCSI (se você tiver hosts iSCSI).
- Configure um servidor NTP (Network Time Protocol) e um servidor DNS (Domain Name System).
- Ver o estado e as definições do controlador.
- Permita que os usuários de fora da rede local iniciem uma sessão SSH e alterem as configurações no controlador.
- Coloque o controlador offline, online ou no modo de serviço.

#### Unidades

O storage array pode incluir unidades de disco rígido (HDDs) ou unidades de estado sólido (SSDs). Dependendo do tamanho da gaveta, até 12, 24 ou 60 unidades podem ser instaladas na gaveta.

Você pode executar as seguintes funções relacionadas às unidades:

- Ligue a luz de localização da unidade, para que você possa encontrar a localização física da unidade na prateleira.
- Ver o estado e as definições da unidade.
- Reatribua uma unidade (substitua logicamente uma unidade com falha por uma unidade não atribuída) e reconstrua manualmente a unidade, se necessário.
- Falhar manualmente uma unidade para que você possa substituí-la. (A falha de uma unidade permite copiar o conteúdo da unidade antes de substituí-la.)
- Atribuir ou anular a atribuição de peças sobressalentes quentes.
- Apagar unidades.

### Terminologia de hardware

Os termos de hardware a seguir se aplicam aos storage arrays.

**Termos gerais de hardware:**

| Componente | Descrição |
| --- | --- |
| Baía | Um compartimento é um slot na prateleira onde uma unidade ou outro componente está instalado. |
| Controlador | Um controlador consiste em uma placa, firmware e software. Controla as unidades e implementa as funções do System Manager. |
| Compartimento do controlador | Um compartimento de controladora contém um conjunto de unidades e um ou mais coletores de controladora. Um recipiente do controlador contém os controladores, placas de interface do host (HICs) e baterias. |
| Condução | Uma unidade é um dispositivo mecânico eletromagnético ou um dispositivo de memória de estado sólido que fornece os meios de armazenamento físico para os dados. |
| Compartimento de unidades | Um compartimento de unidade, também chamado de compartimento de expansão, contém um conjunto de unidades e dois módulos de entrada/saída (IOMs). As IOMs contêm portas SAS que conectam um compartimento de unidade a uma gaveta de controladora ou a outras gavetas de unidades. |
| IOM (ESM) | Uma IOM é um módulo de entrada/saída que inclui portas SAS para conetar o compartimento de unidade à gaveta da controladora. Nos modelos anteriores de controladores, a IOM foi referida como um módulo de serviço ambiental (ESM). |
| Depósito da ventoinha/alimentação | Um recipiente de alimentação/ventilador é um conjunto que desliza para dentro de uma prateleira. Inclui uma fonte de alimentação e uma ventoinha integrada. |
| SFP | Um SFP é um transcetor plugável de fator de forma pequeno (SFP). |
| Gaveta | Uma prateleira é um gabinete instalado em um gabinete ou rack. Ele contém os componentes de hardware para o storage array. Há dois tipos de compartimentos: Um compartimento de controladora e um compartimento de unidade. Um compartimento de controladora inclui controladores e unidades. Um compartimento de unidades inclui módulos de entrada/saída (IOMs) e unidades. |
| Storage array | Um array de storage inclui compartimentos, controladores, unidades, software e firmware. |

**Termos do controlador:**

| Componente | Descrição |
| --- | --- |
| Controlador | Um controlador consiste em uma placa, firmware e software. Controla as unidades e implementa as funções do System Manager. |
| Compartimento do controlador | Um compartimento de controladora contém um conjunto de unidades e um ou mais coletores de controladora. Um recipiente do controlador contém os controladores, placas de interface do host (HICs) e baterias. |
| DHCP | DHCP (Dynamic Host Configuration Protocol) é um protocolo usado em redes IP (Internet Protocol) para distribuir dinamicamente parâmetros de configuração de rede, como endereços IP. |
| DNS | O Domain Name System (DNS) é um sistema de nomes para dispositivos conetados à Internet ou a uma rede privada. O servidor DNS mantém um diretório de nomes de domínio e os converte em endereços IP (Internet Protocol). |
| Configurações duplex | O duplex é uma configuração de módulo de dois controladores dentro da matriz de armazenamento. Os sistemas duplex são totalmente redundantes em relação a controladores, caminhos de volume lógicos e caminhos de disco. Se um controlador falhar, o outro controlador assume sua e/S para manter a disponibilidade. Os sistemas duplex também têm ventiladores e fontes de alimentação redundantes. |
| Conexões full-duplex / half-duplex | Full-duplex e half-duplex referem-se aos modos de conexão. No modo full-duplex, dois dispositivos podem se comunicar simultaneamente em ambas as direções. No modo half-duplex, os dispositivos podem se comunicar em uma direção de cada vez (um dispositivo envia uma mensagem, enquanto o outro dispositivo a recebe). |
| HIC | Uma placa de interface de host (HIC) pode ser instalada opcionalmente dentro de um recipiente de controlador. As portas de host que são incorporadas ao controlador são chamadas portas de host de placa base. As portas de host que são incorporadas ao HIC são chamadas portas HIC. |
| Resposta ICMP PING | O ICMP (Internet Control Message Protocol) é um protocolo usado por sistemas operacionais de computadores em rede para enviar mensagens. As mensagens ICMP determinam se um host é acessível e quanto tempo leva para obter pacotes de e para esse host. |
| Endereço MAC | Identificadores de controle de acesso de Mídia (endereços MAC) são usados pela Ethernet para distinguir entre canais lógicos separados conetando duas portas na mesma interface de rede de transporte físico. |
| cliente de gestão | Um cliente de gerenciamento é o computador em que um navegador está instalado para acessar o System Manager. |

| Componente | Descrição |
| --- | --- |
| MTU | Uma MTU (Maximum Transmission Unit) é o pacote ou quadro de maior tamanho que pode ser enviado em uma rede. |
| NTP | Network Time Protocol (NTP) é um protocolo de rede para sincronização de clock entre sistemas de computador em redes de dados. |
| Configurações simplex | Simplex é uma configuração de módulo de controlador único dentro da matriz de armazenamento. Um sistema simplex não oferece redundância de controlador ou caminho de disco, mas tem ventiladores redundantes e fontes de alimentação. |
| VLAN | Uma rede local virtual (VLAN) é uma rede lógica que se comporta como se estivesse fisicamente separada de outras redes suportadas pelos mesmos dispositivos (switches, roteadores, etc.). |

**Termos da unidade:**

| Componente | Descrição |
| --- | --- |
| DA | O Data Assurance (DA) é um recurso que verifica e corrige erros que podem ocorrer à medida que os dados são transferidos através dos controladores para as unidades. O Data Assurance pode ser ativado no nível de pool ou grupo de volumes, com hosts que usam uma interface de e/S compatível com DA, como Fibre Channel. |
| Recurso de segurança da unidade | O Drive Security é um recurso de storage array que fornece uma camada extra de segurança com unidades de criptografia completa de disco (FDE) ou unidades FIPS (Federal Information Processing Standard). Quando essas unidades são usadas com o recurso Segurança da Unidade, elas precisam de uma chave de segurança para acessar seus dados. Quando as unidades são fisicamente removidas do array, elas não podem operar até serem instaladas em outro array, em que ponto, elas estarão em um estado de segurança bloqueado até que a chave de segurança correta seja fornecida. |
| Compartimento de unidades | Um compartimento de unidade, também chamado de compartimento de expansão, contém um conjunto de unidades e dois módulos de entrada/saída (IOMs). As IOMs contêm portas SAS que conectam um compartimento de unidade a uma gaveta de controladora ou a outras gavetas de unidades. |
| DULBE | Erro de bloco lógico desalocado ou não escrito (DULBE) é uma opção nas unidades NVMe que permite que o storage array EF300 ou EF600 ofereça suporte a volumes provisionados por recursos. |
| Unidades FDE | As unidades Full Disk Encryption (FDE) executam a encriptação na unidade de disco no nível do hardware. O disco rígido contém um chip ASIC que criptografa dados durante gravações e, em seguida, descriptografa dados durante leituras. |
| Unidades FIPS | As unidades FIPS usam Federal Information Processing Standards (FIPS) 140-2 nível 2. Eles são essencialmente unidades FDE que aderem aos padrões do governo dos Estados Unidos para garantir algoritmos e métodos de criptografia fortes. As unidades FIPS têm padrões de segurança mais altos do que as unidades FDE. |
| HDD | Unidades de disco rígido (HDDs) são dispositivos de armazenamento de dados que usam plataformas metálicas rotativas com um revestimento magnético. |
| Unidades hot spare | As peças sobressalentes ativas funcionam como unidades de reserva nos grupos de volumes RAID 1, RAID 5 ou RAID 6. São unidades totalmente funcionais que não contêm dados. Se uma unidade falhar no grupo de volumes, o controlador reconstrói automaticamente os dados da unidade com falha para um hot spare. |

| Componente | Descrição |
| --- | --- |
| NVMe | O Non-volátil Memory Express (NVMe) é uma interface projetada para dispositivos de storage baseados em flash, como unidades SSD. O NVMe reduz a sobrecarga de e/S e inclui melhorias de desempenho em comparação com as interfaces de dispositivos lógicos anteriores. |
| SAS | O Serial Attached SCSI (SAS) é um protocolo serial ponto a ponto que vincula controladores diretamente às unidades de disco. |
| Unidades com capacidade de segurança | As unidades com capacidade segura podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard), que criptografam dados durante gravações e descriptografam dados durante leituras. Essas unidades são consideradas seguras-*Capable* porque podem ser usadas para segurança adicional usando o recurso Segurança da Unidade. Se o recurso Segurança da unidade estiver habilitado para grupos de volume e pools usados com essas unidades, as unidades se tornarão seguras-*enabled*. |
| Unidades habilitadas para segurança | As unidades habilitadas para segurança são usadas com o recurso Segurança da unidade. Quando você ativa o recurso de Segurança da Unidade e, em seguida, aplica o Drive Security a um pool ou grupo de volume em unidades seguras-*capazes*, as unidades ficam seguras___ ativadas. O acesso de leitura e gravação está disponível somente por meio de um controlador configurado com a chave de segurança correta. Essa segurança adicional impede o acesso não autorizado aos dados em uma unidade que é fisicamente removida do storage array. |
| SSD | Os discos de estado sólido (SSDs) são dispositivos de armazenamento de dados que usam memória de estado sólido (flash) para armazenar dados persistentemente. Os SSDs emulam discos rígidos convencionais e estão disponíveis com as mesmas interfaces que os discos rígidos usam. |

**Termos iSCSI:**

| Prazo | Descrição |
| --- | --- |
| CHAP | O método CHAP (Challenge Handshake Authentication Protocol) valida a identidade de alvos e iniciadores durante o link inicial. A autenticação é baseada em uma chave de segurança compartilhada chamada CHAP *secret*. |
| Controlador | Um controlador consiste em uma placa, firmware e software. Controla as unidades e implementa as funções do System Manager. |
| DHCP | DHCP (Dynamic Host Configuration Protocol) é um protocolo usado em redes IP (Internet Protocol) para distribuir dinamicamente parâmetros de configuração de rede, como endereços IP. |
| IB | InfiniBand (IB) é um padrão de comunicação para a transmissão de dados entre servidores de alto desempenho e sistemas de armazenamento. |
| Resposta ICMP PING | O ICMP (Internet Control Message Protocol) é um protocolo usado por sistemas operacionais de computadores em rede para enviar mensagens. As mensagens ICMP determinam se um host é acessível e quanto tempo leva para obter pacotes de e para esse host. |
| IQN | Um identificador IQN (iSCSI Qualified Name) é um nome exclusivo para um iniciador iSCSI ou destino iSCSI. |
| Iser | Extensões iSCSI para RDMA (iSER) é um protocolo que estende o protocolo iSCSI para operação através de transportes RDMA, como InfiniBand ou Ethernet. |
| ISNS | O Internet Storage Name Service (iSNS) é um protocolo que permite a deteção, o gerenciamento e a configuração automatizada de dispositivos iSCSI e Fibre Channel em redes TCP/IP. |
| Endereço MAC | Identificadores de controle de acesso de Mídia (endereços MAC) são usados pela Ethernet para distinguir entre canais lógicos separados conetando duas portas na mesma interface de rede de transporte físico. |
| Cliente de gestão | Um cliente de gerenciamento é o computador em que um navegador está instalado para acessar o System Manager. |
| MTU | Uma MTU (Maximum Transmission Unit) é o pacote ou quadro de maior tamanho que pode ser enviado em uma rede. |
| RDMA | O Acesso remoto à memória direta (RDMA) é uma tecnologia que permite que os computadores de rede troquem dados na memória principal sem envolver o sistema operacional de qualquer computador. |

| Prazo | Descrição |
| --- | --- |
| Sessão de descoberta sem nome | Quando a opção para sessões de descoberta sem nome está ativada, os iniciadores iSCSI não são necessários para especificar o IQN de destino para recuperar as informações do controlador. |

**Termos do NVMe:**

| Prazo | Descrição |
| --- | --- |
| InfiniBand | InfiniBand (IB) é um padrão de comunicação para a transmissão de dados entre servidores de alto desempenho e sistemas de armazenamento. |
| Namespace | Um namespace é o armazenamento NVM formatado para acesso a bloco. É análogo a uma unidade lógica em SCSI, que se relaciona a um volume no storage array. |
| ID do namespace | O ID do namespace é o identificador exclusivo da controladora NVMe para o namespace e pode ser definido como um valor entre 1 e 255. É análogo a um número de unidade lógica (LUN) no SCSI. |
| NQN | O nome qualificado do NVMe (NQN) é usado para identificar o destino do storage remoto (o storage array). |
| NVM | A memória não volátil (NVM) é a memória persistente usada em muitos tipos de dispositivos de armazenamento. |
| NVMe | O Non-volátil Memory Express (NVMe) é uma interface projetada para dispositivos de storage baseados em flash, como unidades SSD. O NVMe reduz a sobrecarga de e/S e inclui melhorias de desempenho em comparação com as interfaces de dispositivos lógicos anteriores. |
| NVMe-of | A memória não volátil Express sobre Fabrics (NVMe-of) é uma especificação que permite a transferência de dados e comandos do NVMe em uma rede entre um host e storage. |
| Controlador NVMe | Uma controladora NVMe é criada durante o processo de conexão do host. Ele fornece um caminho de acesso entre um host e os namespaces no storage array. |
| Fila NVMe | Uma fila é usada para passar comandos e mensagens pela interface NVMe. |
| Subsistema NVMe | O storage array com conexão de host NVMe. |
| RDMA | O acesso remoto à memória direta (RDMA) permite maior movimentação direta de dados dentro e fora de um servidor, implementando um protocolo de transporte no hardware da placa de interface de rede (NIC). |
| ROCE | RDMA over Converged Ethernet (RoCE) é um protocolo de rede que permite acesso remoto à memória direta (RDMA) através de uma rede Ethernet. |

| Prazo | Descrição |
| --- | --- |
| SSD | Os discos de estado sólido (SSDs) são dispositivos de armazenamento de dados que usam memória de estado sólido (flash) para armazenar dados persistentemente. Os SSDs emulam discos rígidos convencionais e estão disponíveis com as mesmas interfaces que os discos rígidos usam. |

## Gerenciar os componentes do compartimento

### Veja os componentes de hardware

A página hardware fornece funções de ordenação e filtragem que facilitam a localização de componentes.

**Passos**

1. Selecione **hardware**.
2. Use as funções descritas na tabela a seguir para exibir componentes de hardware.

| Função | Descrição |
| --- | --- |
| Exibições de unidades, controladores e componentes | Para alternar entre as exibições frontal e traseira, selecione **Drives** ou **Controllers & Components** na extrema direita (o link que aparece depende da exibição atual). A visualização **Drives** mostra as unidades e quaisquer compartimentos de unidade vazios. A visualização **Controllers & Components** mostra os controladores e quaisquer módulos IOM (ESM), coletores de alimentação/ventilador ou compartimentos de controlador vazios. Na parte inferior da página, você também pode selecionar **Mostrar todas as unidades**. |
| Filtros de vista da unidade | Se o storage de armazenamento contiver unidades com diferentes tipos de atributos físicos e lógicos, a página **hardware** inclui filtros de exibição de unidade. Esses campos de filtro ajudam a localizar rapidamente unidades específicas, limitando os tipos de unidades exibidos na página. Em **Mostrar unidades que são…**, clique no campo de filtro à esquerda (por padrão, mostra **qualquer tipo de unidade**) para ver uma lista suspensa de atributos físicos (por exemplo, capacidade e velocidade). Clique no campo de filtro à direita (por padrão, mostra **em qualquer lugar na matriz de armazenamento**) para ver uma lista suspensa de atributos lógicos (por exemplo, atribuição de grupo de volume). Você pode usar esses filtros juntos ou separadamente.<br><br>Se a matriz de armazenamento contiver unidades que compartilham os mesmos atributos físicos, o campo **qualquer tipo de unidade** à esquerda não será exibido. Se todas as unidades estiverem no mesmo local lógico, o campo **em qualquer lugar no storage de armazenamento** à direita não será exibido. |
| Legenda | Os componentes são exibidos em certas cores para descrever seus estados de função. Para expandir e recolher as descrições destes estados, clique em **Legenda**. |

| Função | Descrição |
| --- | --- |
| Mostrar detalhes do ícone de status | Os indicadores de status podem incluir descrições de texto para os estados de disponibilidade. Clique em **Mostrar detalhes do ícone de status** para mostrar ou ocultar este texto de status. |
| Ícones de prateleira/prateleira | Cada exibição de prateleira fornece uma lista de comandos relacionados, juntamente com propriedades e status. Clique em **Shelf** para ver uma lista suspensa de comandos. Você também pode selecionar um dos ícones ao longo da parte superior para ver o status e as propriedades de componentes individuais: Controladores, IOMs (ESMs), fontes de alimentação, ventiladores, temperatura, baterias e SFPs. |
| Ordem de prateleira | As prateleiras podem ser reorganizadas na página hardware. Use as setas para cima e para baixo no canto superior direito de cada exibição de prateleira para alterar a ordem superior/inferior das prateleiras. |

#### Mostrar ou ocultar o estado do componente

Você pode exibir descrições de status para unidades, controladores, ventiladores e fontes de alimentação.

#### Passos

1. Selecione **hardware**.
2. Para ver os componentes posterior ou frontal:
   - Se você quiser ver os componentes do controlador e do recipiente de alimentação/ventilador, mas as unidades forem exibidas, clique na guia **Controllers & Components** (Controladores e componentes).
   - Se você quiser ver as unidades, mas os componentes do controlador e do recipiente de energia/ventilador forem exibidos, clique na guia **unidades**.
3. Para visualizar ou ocultar descrições de estado pop-over:
   - Se você quiser ver uma descrição pop-over dos ícones de status, clique em **Mostrar detalhes do ícone de status** no canto superior direito da exibição da prateleira (marque a caixa de seleção).
   - Para ocultar as descrições pop-up, clique em **Mostrar detalhes do ícone de status** novamente (desmarque a caixa de seleção).
4. Se você quiser ver os detalhes completos do status, selecione o componente na exibição de prateleira e selecione **Configurações de exibição**.
5. Se quiser ver as descrições dos componentes coloridos, selecione **Legenda**.

#### Alterne entre as vistas frontal e traseira

A página hardware pode mostrar a vista frontal ou a vista posterior das prateleiras.

#### Sobre esta tarefa

A vista posterior mostra os controladores/IOMs e os coletores do ventilador de energia. A vista frontal mostra as unidades.

#### Passos

1. Selecione **hardware**.
2. Se o gráfico mostrar as unidades, clique na guia **Controllers & Components** (Controladores e componentes).

   O gráfico muda para mostrar os controladores em vez das unidades.

3. Se o gráfico mostrar os controladores, clique na guia **Drives**.

   O gráfico muda para mostrar as unidades em vez dos controladores.

4. Opcionalmente, você pode selecionar **Mostrar tudo frontal** ou **Mostrar tudo de volta**, localizado na parte inferior da página.

#### Alterar a ordem de visualização das prateleiras

Você pode alterar a ordem das prateleiras exibidas na página hardware para corresponder à ordem física das prateleiras em um gabinete.

**Passos**

1. Selecione **hardware**.
2. No canto superior direito de uma exibição de prateleira, selecione as setas para cima ou para baixo para reorganizar a ordem das prateleiras mostrada na página hardware.

#### Ligue a luz de localização da prateleira

Para encontrar a localização física de uma prateleira mostrada na página hardware, você pode ligar a luz de localização da prateleira.

**Passos**

1. Selecione **hardware**.
2. Selecione a lista suspensa para o compartimento do controlador ou compartimento de unidade e selecione **Ativar luz de localização**.

   A luz de localização da prateleira acende-se.

3. Quando tiver localizado fisicamente a prateleira, volte à caixa de diálogo e selecione **Desligar**.

#### Alterar as IDs de gaveta

O ID do compartimento é um número que identifica exclusivamente uma gaveta no storage array. As prateleiras são numeradas consecutivamente, começando com 00 ou 01, no canto superior esquerdo de cada vista da prateleira.

**Sobre esta tarefa**

O firmware do controlador atribui automaticamente o ID do compartimento, mas você pode alterar esse número se quiser criar um esquema de pedidos diferente.

**Passos**

1. Selecione **hardware**.
2. Selecione a lista suspensa para o compartimento de controladora ou compartimento de unidade e

selecione **alterar ID**.

3. Na caixa de diálogo alterar ID do compartimento, selecione a lista suspensa para exibir os números disponíveis.

   Essa caixa de diálogo não exibe os IDs atribuídos atualmente às gavetas ativas.

4. Selecione um número disponível e clique em **Salvar**.

   Dependendo do número selecionado, a ordem do compartimento pode ser reorganizada na página hardware. Se desejar, você pode usar as setas para cima/para baixo na parte superior direita de cada prateleira para reajustar a ordem.

### Exibir o status e as configurações do componente do compartimento

A página hardware fornece status e configurações para os componentes do compartimento, incluindo fontes de alimentação, ventiladores e baterias.

#### Sobre esta tarefa

Os componentes disponíveis dependem do tipo de prateleira:

- **Compartimento de unidade** — contém um conjunto de unidades, coletores de energia/ventilador, módulos de entrada/saída (IOMs) e outros componentes de suporte em uma única gaveta.
- **Compartimento de controladora** — contém um conjunto de unidades, um ou dois coletores de controladora, coletores de energia/ventilador e outros componentes de suporte em uma única gaveta.

#### Passos

1. Selecione **hardware**.
2. Selecione a lista suspensa para o compartimento do controlador ou compartimento de unidade e selecione **Exibir configurações**.

   A caixa de diálogo Configurações de componentes do compartimento é aberta, com guias que mostram o status e as configurações relacionadas aos componentes do compartimento. Dependendo do tipo de prateleira selecionado, algumas guias descritas na tabela podem não aparecer.

| Separador | Descrição |
| --- | --- |
| Gaveta | A guia **Shelf** mostra as seguintes propriedades:<br>• **ID do compartimento** — identifica exclusivamente uma prateleira na matriz de armazenamento. O firmware do controlador atribui esse número, mas você pode alterá-lo selecionando **shelf › Change ID**.<br>• **Redundância do caminho do compartimento** — especifica se as conexões entre o compartimento e o controlador têm métodos alternativos no lugar (Sim) ou não (não).<br>• **Tipos de unidade atuais** — mostra o tipo de tecnologia incorporada nas unidades (por exemplo, uma unidade SAS com capacidade segura). Se houver mais de um tipo de unidade, ambas as tecnologias são mostradas.<br>• **Número de série** — mostra o número de série da prateleira. |

| Separador | Descrição |
| --- | --- |
| IOMs (ESMs) | A guia **IOMs (ESMs)** mostra o status do módulo de entrada/saída (IOM), que também é chamado de módulo de serviço ambiental (ESM). Ele monitora o status dos componentes em um compartimento de unidades e serve como ponto de conexão entre a bandeja de unidades e a controladora.<br><br>O estado pode ser ótimo, falhou, ótimo (Miswire) ou não certificado. Outras informações incluem a versão do firmware e a versão das definições de configuração.<br><br>Selecione **Mostrar mais definições** para ver as taxas de dados máximas e atuais e o estado da comunicação do cartão (Sim ou não).<br><br>Você também pode exibir esse status selecionando o ícone IOM  , ao lado da lista suspensa prateleira. |
| Fontes de alimentação | O separador **fontes de alimentação** mostra o estado do recipiente da fonte de alimentação e da própria fonte de alimentação. O status pode ser ótimo, Falha, removido ou desconhecido. Também mostra o número de peça da fonte de alimentação.<br><br>Também é possível exibir esse status selecionando o ícone fonte de alimentação  , ao lado da lista suspensa prateleira. |
| Fãs | O separador **Fans** mostra o estado do recipiente do ventilador e do próprio ventilador. O status pode ser ótimo, Falha, removido ou desconhecido.<br><br>Você também pode exibir esse status selecionando o ícone ventilador  , ao lado da lista suspensa prateleira. |
| Temperatura | A guia **temperatura** mostra o status da temperatura dos componentes da prateleira, como sensores, controladores e coletores de energia/ventilador. O estado pode ser ideal, temperatura nominal excedida, temperatura máxima excedida ou desconhecido.<br><br>Você também pode exibir esse status selecionando o ícone temperatura  , ao lado da lista suspensa prateleira. |
| Baterias | O separador **baterias** mostra o estado das pilhas do controlador. O estado pode ser ótimo, falhou, removido ou desconhecido. Outras informações incluem a idade da bateria, dias até a substituição, ciclos de aprendizagem e semanas entre ciclos de aprendizagem.<br><br>Também pode visualizar este estado selecionando o ícone de pilhas  , junto à lista pendente prateleira. |

| Separador | Descrição |
| --- | --- |
| SFPs | A guia **SFPs** mostra o status dos transcetores Small Form-factor Pluggable (SFP) nos controladores. O status pode ser ótimo, Falha ou desconhecido.<br><br>Selecione **Mostrar mais definições** para ver o número de peça, o número de série e o fornecedor dos SFPs.<br><br>Você também pode exibir esse status selecionando o ícone SFP, ao lado da lista suspensa prateleira. |

3. Clique em **Fechar**.

#### Atualize os ciclos de aprendizagem da bateria

Um ciclo de aprendizagem é um ciclo automático para calibrar o indicador inteligente da bateria. Os ciclos são programados para iniciar automaticamente, no mesmo dia e hora, em intervalos de 8 semanas (por controlador). Se você quiser definir uma programação diferente, você pode ajustar os ciclos de aprendizagem.

##### Sobre esta tarefa

A atualização dos ciclos de aprendizagem afeta ambas as baterias do controlador.

##### Passos

1. Selecione **hardware**.
2. Selecione a lista suspensa para o compartimento do controlador e selecione **Exibir configurações**.
3. Selecione o separador **baterias**.
4. Selecione **Atualizar ciclos de aprendizagem da bateria**.

   A caixa de diálogo Atualizar ciclos de aprendizagem da bateria é aberta.

5. Nas listas suspensas, selecione um novo dia e hora.
6. Clique em **Salvar**.

## Gerenciar controladores

#### estados do controlador

Você pode colocar um controlador em três estados diferentes: On-line, off-line e modo de serviço.

##### Estado online

O estado online é o estado de funcionamento normal do controlador. Isso significa que o controlador está operando normalmente e está disponível para operações de e/S.

Quando você coloca um controlador on-line, seu status é definido como ideal.

#### Estado offline

O estado off-line é normalmente usado para preparar um controlador para substituição quando há dois controladores na matriz de armazenamento. Um controlador pode entrar no estado offline de duas maneiras: Você pode emitir um comando explícito ou o controlador pode falhar. Um controlador pode sair do estado offline apenas emitindo outro comando explícito ou substituindo o controlador com falha. Você pode colocar um controlador off-line apenas se houver dois controladores na matriz de armazenamento.

Quando um controlador está no estado offline, as seguintes condições são verdadeiras:

- O controlador não está disponível para e/S
- Não é possível gerenciar o storage array por meio desse controlador.
- Quaisquer volumes atualmente pertencentes a esse controlador são movidos para o outro controlador.
- O espelhamento de cache está desativado e todos os volumes são alterados para gravar através do modo de cache.

#### Modo de assistência

O modo de serviço geralmente é usado apenas pelo suporte técnico para mover todos os volumes de storage array para uma controladora, de modo que a outra controladora possa ser diagnosticada. Um controlador deve ser colocado manualmente no modo de serviço e deve ser colocado manualmente de volta on-line após a conclusão da operação de serviço.

Quando um controlador está no modo de serviço, as seguintes condições são verdadeiras:

- O controlador não está disponível para e/S
- O suporte técnico pode acessar o controlador através da porta serial ou conexão de rede para analisar possíveis problemas.
- Quaisquer volumes atualmente pertencentes a esse controlador são movidos para o outro controlador.
- O espelhamento de cache está desativado e todos os volumes são alterados para gravar através do modo de cache.

### Considerações para atribuir endereços IP

Por padrão, os controladores são fornecidos com DHCP ativado em ambas as portas de rede. Você pode atribuir endereços IP estáticos, usar os endereços IP estáticos padrão ou usar endereços IP atribuídos por DHCP. Você também pode usar a configuração automática sem monitoração de estado IPv6.

> O IPv6 é desativado por padrão em novos controladores, mas você pode configurar os endereços IP da porta de gerenciamento usando um método alternativo e, em seguida, ativar o IPv6 nas portas de gerenciamento usando o System Manager.

Quando a porta de rede está em um estado "link down", ou seja, desconetado de uma LAN, o sistema relata sua configuração como estática, exibindo um endereço IP de 0.0.0.0 (versões anteriores) ou DHCP habilitado sem endereço IP relatado (versões posteriores). Depois que a porta de rede estiver em um estado "link up" (ou seja, conetada a uma LAN), ela tentará obter um endereço IP através do DHCP.

Se o controlador não conseguir obter um endereço DHCP numa determinada porta de rede, este reverte para um endereço IP predefinido, o que poderá demorar até 3 minutos. Os endereços IP padrão são os seguintes:

```
Controller 1 (port 1): IP Address: 192.168.128.101
```

```
Controller 1 (port 2): IP Address: 192.168.129.101
```

```
Controller 2 (port 1): IP Address: 192.168.128.102
```

```
Controller 2 (port 2): IP Address: 192.168.129.102
```

Ao atribuir endereços IP:

- Reserva a porta 2 nos controladores para utilização do suporte ao Cliente. Não altere as definições de rede predefinidas (DHCP ativado).
- Para definir endereços IP estáticos para os controladores E2800 e E5700, use o Gerenciador do sistema SANtricity. Para definir endereços IP estáticos para os controladores E2700 e E5600, use SANtricity Storage Manager. Depois que um endereço IP estático é configurado, ele permanece definido através de todos os eventos de link down/up.
- Para utilizar DHCP para atribuir o endereço IP do controlador, ligue o controlador a uma rede que possa processar pedidos DHCP. Use uma concessão DHCP permanente.

> Os endereços padrão não são persistidos em eventos de link para baixo. Quando uma porta de rede em um controlador está definida para usar DHCP, o controlador tenta obter um endereço DHCP em cada evento de ligação, incluindo inserções de cabos, reinicializações e ciclos de alimentação. Sempre que uma tentativa de DHCP falhar, é utilizado o endereço IP estático predefinido para essa porta.

#### Configurar a porta de gerenciamento

## O controlador inclui uma porta Ethernet utilizada para a gestão do sistema. Se necessário, você pode alterar seus parâmetros de transmissão e endereços IP.

#### Sobre esta tarefa

Durante este procedimento, selecione a porta 1 e, em seguida, determine a velocidade e o método de endereçamento da porta. A porta 1 coneta-se à rede onde o cliente de gerenciamento pode acessar o controlador e o System Manager.

> Não use a porta 2 em nenhum dos controladores. A porta 2 está reservada para uso pelo suporte técnico.

#### Passos

1. Selecione **hardware**.
2. Se o gráfico mostrar as unidades, clique na guia **Controllers & Components** (Controladores e componentes).

O gráfico muda para mostrar os controladores em vez das unidades.

3. Clique no controlador com a porta de gerenciamento que deseja configurar.

   É apresentado o menu de contexto do controlador.

4. Selecione **Configurar portas de gerenciamento**.

   A caixa de diálogo Configurar portas de gerenciamento é aberta.

5. Certifique-se de que a porta 1 é exibida e clique em **Next**.
6. Selecione as definições da porta de configuração e, em seguida, clique em **seguinte**.

   **Detalhes do campo**

| Campo | Descrição |
| --- | --- |
| Velocidade e modo duplex | Mantenha a configuração negociação automática se desejar que o System Manager determine os parâmetros de transmissão entre o storage de armazenamento e a rede; ou se você souber a velocidade e o modo da rede, selecione os parâmetros na lista suspensa. Apenas as combinações de velocidade e duplex válidas aparecem na lista. |
| Ativar IPv4 / ativar IPv6 | Selecione uma ou ambas as opções para ativar o suporte para redes IPv4G e IPv6G. |

   Se selecionar **Ativar IPv4**, abre-se uma caixa de diálogo para selecionar IPv4 definições depois de clicar em **seguinte**. Se selecionar **Ativar IPv6**, abre-se uma caixa de diálogo para selecionar IPv6 definições depois de clicar em **seguinte**. Se você selecionar ambas as opções, a caixa de diálogo para configurações IPv4 será aberta primeiro e, depois de clicar em **Avançar**, a caixa de diálogo para configurações IPv6 será aberta.

7. Configure as definições IPv4 e/ou IPv6, automática ou manualmente.

**Detalhes do campo**

| Campo | Descrição |
| --- | --- |
| Obter automaticamente a configuração do servidor DHCP | Selecione esta opção para obter a configuração automaticamente. |
| Especifique manualmente a configuração estática | Selecione esta opção e, em seguida, introduza o endereço IP do controlador. (Se desejado, você pode cortar e colar endereços nos campos.) Para IPv4, inclua a máscara de sub-rede e o gateway. Para IPv6, inclua o endereço IP roteável e o endereço IP do roteador.<br><br>Se você alterar a configuração do endereço IP, perderá o caminho de gerenciamento para o storage array. Se você usar o Gerenciador Unificado do SANtricity para gerenciar arrays globalmente em sua rede, abra a interface do usuário e vá para o **Gerenciar › descobrir**. Se utilizar o SANtricity Storage Manager, tem de remover o dispositivo da janela de Gestão Empresarial (EMW), adicioná-lo de volta ao EMW selecionando **Editar › Adicionar matriz de armazenamento** e, em seguida, introduza o novo endereço IP. |

8. Clique em **Finish**.

**Resultados**

A configuração da porta de gerenciamento é exibida nas configurações do controlador, guia portas de gerenciamento.

### Configurar endereços de servidor NTP

Você pode configurar uma conexão com o servidor NTP (Network Time Protocol) para que o controlador consulte periodicamente o servidor NTP para atualizar seu relógio interno de hora do dia.

**Antes de começar**

- Um servidor NTP deve ser instalado e configurado na sua rede.
- Você deve saber o endereço do servidor NTP primário e de um servidor NTP de backup opcional. Esses endereços podem ser nomes de domínio totalmente qualificados, endereços IPv4 ou endereços IPv6.

Se você inserir um ou mais nomes de domínio para os servidores NTP, você também deve configurar um servidor DNS para resolver o endereço do servidor NTP. Você precisa configurar o servidor DNS somente nos controladores onde você configurou o NTP e forneceu um nome de domínio.

**Sobre esta tarefa**

O NTP permite que o storage array sincronize automaticamente os relógios do controlador com um host externo usando o Simple Network Time Protocol (SNTP). O controlador consulta periodicamente o servidor

NTP configurado e, em seguida, utiliza os resultados para atualizar o relógio interno do dia-a-dia. Se apenas um controlador tiver o NTP ativado, o controlador alternativo sincroniza periodicamente o relógio com o controlador que tem o NTP ativado. Se nenhum dos controladores tiver o NTP ativado, os controladores sincronizam periodicamente os seus relógios uns com os outros.

> Você não precisa configurar o NTP em ambos os controladores; no entanto, isso melhora a capacidade do storage array de permanecer sincronizado durante falhas de hardware ou comunicação.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar as unidades, clique na guia **Controllers & Components** (Controladores e componentes).

   O gráfico muda para mostrar os controladores em vez das unidades.
3. Clique no controlador que pretende configurar.

   É apresentado o menu de contexto do controlador.
4. Selecione **Configurar servidor NTP**.

   A caixa de diálogo Configurar servidor NTP (Network Time Protocol) é aberta.
5. Selecione **quero ativar o NTP no controlador** (**A** ou **B**).

   Seleções adicionais aparecem na caixa de diálogo.
6. Selecione uma das seguintes opções:
   - * Obter automaticamente endereços de servidor NTP do servidor DHCP* — os endereços de servidor NTP detetados são mostrados.

     > Se o storage array estiver definido para usar um endereço NTP estático, nenhum servidor NTP será exibido.

   - **Especifique manualmente endereços de servidor NTP** — Digite o endereço de servidor NTP primário e um endereço de servidor NTP de backup. O servidor de backup é opcional. (Estes campos de endereço aparecem depois de selecionar o botão de opção.) O endereço do servidor pode ser um nome de domínio totalmente qualificado, endereço IPv4 ou endereço IPv6.
7. **Opcional:** Digite as informações do servidor e as credenciais de autenticação para um servidor NTP de backup.
8. Clique em **Salvar**.

**Resultados**

A configuração do servidor NTP é exibida nas configurações do controlador, guia **DNS / NTP**.

### Configurar endereços de servidor DNS

O sistema de nomes de domínio (DNS) é usado para resolver nomes de domínio totalmente qualificados para os controladores e um servidor NTP (Network Time Protocol). As portas de gerenciamento no storage array podem dar suporte a protocolos

IPv4 ou IPv6 simultaneamente.

**Antes de começar**

- Um servidor DNS deve ser instalado e configurado na rede.
- Você sabe o endereço do servidor DNS primário e um servidor DNS de backup opcional. Esses endereços podem ser IPv4 endereços ou IPv6 endereços.

**Sobre esta tarefa**

Este procedimento descreve como especificar um endereço de servidor DNS primário e de backup. O servidor DNS de backup pode ser configurado opcionalmente para uso se um servidor DNS primário falhar.

> Se já tiver configurado as portas de gestão da matriz de armazenamento com DHCP (Dynamic Host Configuration Protocol) e tiver um ou mais servidores DNS ou NTP associados à configuração DHCP, não terá de configurar manualmente DNS ou NTP. Neste caso, a matriz de armazenamento já deve ter obtido os endereços de servidor DNS/NTP automaticamente. No entanto, você ainda deve seguir as instruções abaixo para abrir a caixa de diálogo e garantir que os endereços corretos sejam detetados.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar as unidades, clique na guia **Controllers & Components** (Controladores e componentes).

   O gráfico muda para mostrar os controladores em vez das unidades.
3. Selecione o controlador a configurar.

   É apresentado o menu de contexto do controlador.
4. Selecione **Configurar servidor DNS**.

   A caixa de diálogo Configurar servidor DNS (Domain Name System) é aberta.
5. Selecione uma das seguintes opções:
   - **Obter automaticamente endereços de servidor DNS do servidor DHCP** — os endereços de servidor DNS detetados são mostrados.

     > Se o storage array estiver definido para usar um endereço DNS estático, nenhum servidor DNS será exibido.

   - **Especifique manualmente endereços de servidor DNS** — Insira um endereço de servidor DNS primário e um endereço de servidor DNS de backup. O servidor de backup é opcional. (Estes campos de endereço aparecem depois de selecionar o botão de opção.) Esses endereços podem ser IPv4 endereços ou IPv6 endereços.
6. Clique em **Salvar**.
7. Repita estes passos para o outro controlador.

**Resultados**

A configuração DNS é exibida nas configurações do controlador, guia **DNS / NTP**.

### Ver as definições do controlador

Você pode exibir informações sobre um controlador, como o status das interfaces de host, interfaces de unidade e portas de gerenciamento.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar as unidades, clique na guia **Controllers & Components** (Controladores e componentes).

   O gráfico muda para mostrar os controladores em vez das unidades.

3. Execute uma das seguintes ações para exibir as configurações do controlador:
   - Clique no controlador para exibir o menu de contexto e selecione **Exibir configurações**.
   - Selecione o ícone do controlador (ao lado da lista suspensa **Shelf**). Para configurações duplex, selecione **Controller A** ou **Controller B** na caixa de diálogo e clique em **Next**.

     A caixa de diálogo Configurações do controlador é aberta.

4. Selecione as guias para mover entre as configurações de propriedade.

   Algumas guias têm um link para **Mostrar mais configurações** no canto superior direito.

**Detalhes do campo**

| Separador | Descrição |
| --- | --- |
| Base | Mostra o status do controlador, o nome do modelo, o número de peça de substituição, a versão atual do firmware e a versão da memória de acesso aleatório estática (NVSRAM) não volátil. |
| Cache | Mostra as configurações de cache do controlador, que incluem o cache de dados, cache do processador e o dispositivo de backup de cache. O dispositivo de backup em cache é usado para fazer backup de dados no cache se você perder energia para o controlador. O status pode ser ótimo, Falha, removido, desconhecido, protegido contra gravação ou incompatível. |
| Interfaces de host | Mostra as informações da interface do host e o status do link de cada porta. A interface do host é a conexão entre o controlador e o host, como Fibre Channel ou iSCSI.<br><br>A localização da placa de interface do host (HIC) está na placa de base ou em um slot (compartimento). "Baseboard" indica que as portas HIC estão incorporadas no controlador. As portas "slot" estão no HIC opcional. |
| Interfaces de unidade | Mostra as informações da interface da unidade e o status do link de cada porta. A interface da unidade é a conexão entre a controladora e as unidades, como SAS. |
| Portas de gerenciamento | Mostra os detalhes da porta de gerenciamento, como o nome do host usado para acessar o controlador e se um login remoto foi ativado. A porta de gerenciamento coneta o controlador e o cliente de gerenciamento, que é onde um navegador é instalado para acessar o System Manager. |
| DNS / NTP | Mostra o método de endereçamento e os endereços IP do servidor DNS e do servidor NTP, se esses servidores tiverem sido configurados no System Manager.<br><br>O Domain Name System (DNS) é um sistema de nomes para dispositivos conetados à Internet ou a uma rede privada. O servidor DNS mantém um diretório de nomes de domínio e os converte em endereços IP (Internet Protocol).<br><br>Network Time Protocol (NTP) é um protocolo de rede para sincronização de clock entre sistemas de computador em redes de dados. |

5. Clique em **Fechar**.

### Configurar login remoto (SSH)

Ao ativar o login remoto, você permite que os usuários de fora da rede local iniciem uma sessão SSH e acessem as configurações no controlador.

Para as versões 11,74 e posteriores do SANtricity, você também pode configurar a autorização multifator (MFA) exigindo que os usuários digitem uma chave SSH e/ou uma senha SSH. Para as versões 11,73 e anteriores do SANtricity, esse recurso *não* inclui uma opção para autorização multifator com chaves SSH e senhas.

**Risco de segurança** — por motivos de segurança, somente o pessoal de suporte técnico deve usar o recurso Login remoto.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar as unidades, clique na guia **Controllers & Components** (Controladores e componentes).

   O gráfico muda para mostrar os controladores em vez das unidades.
3. Clique no controlador para o qual pretende configurar o início de sessão remoto.

   É apresentado o menu de contexto do controlador.
4. Selecione **Configurar login remoto (SSH)**. (Para as versões 11,73 e anteriores do SANtricity, este item de menu é **alterar início de sessão remoto**.)

   A caixa de diálogo abre-se para ativar o início de sessão remoto.
5. Selecione a caixa de verificação **Ativar início de sessão remoto**.

   Esta definição fornece o início de sessão remoto com três opções de autorização:

   - **Somente senha**. Para esta opção, você está pronto e pode clicar em **Salvar**. Se tiver um sistema duplex, pode ativar o início de sessão remoto no segundo controlador seguindo os passos anteriores.
   - * Chave SSH ou senha*. Para esta opção, avance para o passo seguinte.
   - * A senha e a chave SSH*. Para esta opção, selecione a caixa de verificação **Require public key and password for Remote login** e avance para o passo seguinte.
6. Preencha o campo **chave pública autorizada**. Este campo contém uma lista de chaves públicas autorizadas, no formato do arquivo OpenSSH **Authorized_keys**.

   Ao preencher o campo **chave pública autorizada**, esteja ciente das seguintes diretrizes:

   - O campo **chave pública autorizada** aplica-se a ambos os controladores e só precisa ser configurado no primeiro controlador.
   - O arquivo **Authorized_keys** deve conter apenas uma chave por linha. Linhas que começam com no e linhas vazias são ignoradas. Para obter mais informações sobre o formato do arquivo, "Configurando chaves autorizadas para OpenSSH"consulte .
   - Um arquivo **Authorized_keys** deve ser semelhante ao seguinte exemplo:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDJlG20rYTk4ok+xFjkPHYp/R0LfJqEYDLXA5AJ4
9w3DvAWLrUg+1CpNq76WSqmQBmoG9jgbcAB5ABGdswdeMQZHilJcu29iJ3OKKv6SlCulA
j1tHymwtbdhPuipd2wIDAQAB
```

7. Quando terminar, clique em **Salvar**.
8. Para sistemas duplex, você pode ativar o login remoto no segundo controlador seguindo as etapas acima. Se você estiver configurando a opção para uma senha e chave SSH, certifique-se de selecionar a caixa de seleção **Require public key and password for Remote login** novamente.
9. Depois que o suporte técnico terminar a solução de problemas, você pode desativar o login remoto retornando à caixa de diálogo Configurar Login remoto e desmarcar a caixa de seleção **Ativar login remoto**. Se o início de sessão remoto estiver ativado num segundo controlador, abre-se uma caixa de diálogo de confirmação e permite-lhe também desativar o início de sessão remoto no segundo.

   A desativação do login remoto termina todas as sessões SSH atuais e rejeita quaisquer novas solicitações de login.

#### Coloque o controlador online

Se um controlador estiver no estado offline ou no modo de serviço, pode colocá-lo novamente online.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar as unidades, clique na guia **Controllers & Components** (Controladores e componentes).

   O gráfico muda para mostrar os controladores em vez das unidades.

3. Clique em um controlador que esteja no estado offline ou no modo de serviço.

   É apresentado o menu de contexto do controlador.

4. Selecione **Place on-line** e confirme se deseja executar a operação.

**Resultados**

A deteção de um caminho preferido restaurado pelo driver multipath pode levar até 10 minutos.

Todos os volumes originalmente pertencentes a este controlador são automaticamente movidos de volta para o controlador à medida que as solicitações de e/S são recebidas para cada volume. Em alguns casos, você pode precisar redistribuir manualmente os volumes com o comando **redistribuir volumes**.

#### Coloque o controlador offline

Se você for instruído a fazer isso, você pode colocar um controlador off-line.

**Antes de começar**

- Seu storage array precisa ter duas controladoras. O controlador que você não está colocando off-line deve estar on-line (no estado ideal).

- Certifique-se de que não há volumes em uso ou de que você tenha um driver multipath instalado em todos os hosts que usam esses volumes.

**Sobre esta tarefa**

Mais uma vez

> Não coloque um controlador offline a menos que você seja instruído a fazê-lo pelo Recovery Guru ou pelo suporte técnico.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar as unidades, clique na guia **Controllers & Components** (Controladores e componentes).

   O gráfico muda para mostrar os controladores em vez das unidades.
3. Clique no controlador que pretende colocar offline.

   É apresentado o menu de contexto do controlador.
4. Selecione **colocar offline** e confirme que deseja executar a operação.

**Resultados**

Pode demorar vários minutos para o System Manager atualizar o estado do controlador para offline. Não inicie quaisquer outras operações até que o estado tenha sido atualizado.

### Coloque o controlador no modo de serviço

Se você for instruído a fazê-lo, você pode colocar um controlador no modo de serviço.

**Antes de começar**

- O storage array deve ter duas controladoras. O controlador que você não está colocando no modo de serviço deve estar on-line (no estado ideal).
- Certifique-se de que não há volumes em uso ou de que você tenha um driver multipath instalado em todos os hosts que usam esses volumes.

> Colocar um controlador no modo de serviço pode reduzir significativamente o desempenho. Não coloque um controlador no modo de assistência, a menos que seja instruído a fazê-lo através do suporte técnico.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar as unidades, clique na guia **Controllers & Components** (Controladores e componentes).

   O gráfico muda para mostrar os controladores em vez das unidades.
3. Clique no controlador que pretende colocar no modo de serviço.

   É apresentado o menu de contexto do controlador.

4. Selecione **coloque no modo de serviço** e confirme se deseja executar a operação.

### Reiniciar o controlador

Alguns problemas requerem uma reinicialização do controlador (reinicialização). Você pode redefinir o controlador mesmo se você não tiver acesso físico a ele.

#### Antes de começar

- O storage array deve ter duas controladoras. O controlador que você não está redefinindo deve estar on-line (no estado ideal).
- Certifique-se de que não há volumes em uso ou de que você tenha um driver multipath instalado em todos os hosts que usam esses volumes.

#### Passos

1. Selecione **hardware**.
2. Se o gráfico mostrar as unidades, clique na guia **Controllers & Components** (Controladores e componentes).

   O gráfico muda para mostrar os controladores em vez das unidades.

3. Clique no controlador que pretende repor.

   É apresentado o menu de contexto do controlador.

4. Selecione **Reset** e confirme que deseja executar a operação.

## Gerenciar portas iSCSI

### Configurar portas iSCSI

Se o controlador incluir uma ligação de anfitrião iSCSI, pode configurar as definições da porta iSCSI a partir da página hardware.

#### Antes de começar

- O controlador tem de incluir portas iSCSI; caso contrário, as definições iSCSI não estão disponíveis.
- Você deve saber a velocidade da rede (a taxa de transferência de dados entre as portas e o host).

As definições e funções iSCSI só aparecem se a sua matriz de armazenamento suportar iSCSI.

#### Passos

1. Selecione **hardware**.
2. Se o gráfico mostrar as unidades, clique na guia **Controllers & Components** (Controladores e componentes).

   O gráfico muda para mostrar os controladores em vez das unidades.

3. Clique no controlador com as portas iSCSI que pretende configurar.

   É apresentado o menu de contexto do controlador.

4. Selecione **Configurar portas iSCSI**.

   A opção **Configurar portas iSCSI** aparece somente se o System Manager detetar portas iSCSI no controlador.

   Abre-se a caixa de diálogo Configurar portas iSCSI.

5. Na lista suspensa, selecione a porta que deseja configurar e clique em **Avançar**.
6. Selecione as definições da porta de configuração e, em seguida, clique em **seguinte**.

   Para ver todas as configurações de porta, clique no link **Mostrar mais configurações de porta** à direita da caixa de diálogo.

**Detalhes do campo**

| Definição da porta | Descrição |
| --- | --- |
| Velocidade da porta ethernet configurada (aparece apenas para determinados tipos de placas de interface de host) | Selecione a velocidade que corresponde à capacidade de velocidade do SFP na porta. |
| Modo de correção de erro de avanço (FEC) (aparece apenas para determinados tipos de placas de interface de host) | Se desejar, selecione um dos modos FEC para a porta de host especificada.<br>O modo Reed Solomon não suporta a velocidade da porta de 25 Gbps. |
| Ativar IPv4 / ativar IPv6 | Selecione uma ou ambas as opções para ativar o suporte para redes IPv4G e IPv6G.<br>Se pretender desativar o acesso à porta, desmarque ambas as caixas de verificação. |
| Porta de escuta TCP (disponível clicando em **Mostrar mais configurações de porta**.) | Se necessário, introduza um novo número de porta.<br>A porta de escuta é o número da porta TCP que o controlador usa para ouvir logins iSCSI de iniciadores iSCSI do host. A porta de escuta padrão é 3260. Tem de introduzir 3260 ou um valor entre 49152 e 65535. |
| Tamanho MTU (disponível clicando em **Mostrar mais configurações de porta**.) | Se necessário, introduza um novo tamanho em bytes para a unidade máxima de transmissão (MTU).<br>O tamanho padrão da unidade máxima de transmissão (MTU) é de 1500 bytes por quadro. Tem de introduzir um valor entre 1500 e 9000. |
| Ative as respostas ICMP PING | Selecione esta opção para ativar o ICMP (Internet Control Message Protocol). Os sistemas operativos dos computadores em rede utilizam este protocolo para enviar mensagens. Essas mensagens ICMP determinam se um host é acessível e quanto tempo leva para obter pacotes de e para esse host. |

Se você selecionou **Ativar IPv4**, uma caixa de diálogo será aberta para selecionar IPv4 configurações depois de clicar em **Avançar**. Se você selecionou **Ativar IPv6**, uma caixa de diálogo será aberta para selecionar IPv6 configurações depois de clicar em **Avançar**. Se você selecionou ambas as opções, a caixa de diálogo para configurações IPv4 será aberta primeiro e, depois de clicar em **Avançar**, a caixa de diálogo para configurações IPv6 será aberta.

7. Configure as definições IPv4 e/ou IPv6, automática ou manualmente. Para ver todas as configurações de porta, clique no link **Mostrar mais configurações** à direita da caixa de diálogo.

**Detalhes do campo**

| Definição da porta | Descrição |
| --- | --- |
| Obter automaticamente a configuração | Selecione esta opção para obter a configuração automaticamente. |
| Especifique manualmente a configuração estática | Selecione esta opção e, em seguida, introduza um endereço estático nos campos. (Se desejado, você pode cortar e colar endereços nos campos.) Para IPv4, inclua a máscara de sub-rede e o gateway. Para IPv6, inclua o endereço IP roteável e o endereço IP do roteador. |
| Ative o suporte a VLAN (disponível clicando em **Mostrar mais configurações**.) | Selecione esta opção para ativar uma VLAN e introduzir a respetiva ID. Uma VLAN é uma rede lógica que se comporta como se estivesse fisicamente separada de outras redes locais (LANs) físicas e virtuais suportadas pelos mesmos switches, os mesmos roteadores ou ambos. |
| Ativar prioridade ethernet (disponível clicando em **Mostrar mais definições**.) | Selecione esta opção para ativar o parâmetro que determina a prioridade de acesso à rede. Use o controle deslizante para selecionar uma prioridade entre 1 (mais baixa) e 7 (mais alta).<br><br>Em um ambiente de rede local compartilhada (LAN), como Ethernet, muitas estações podem competir pelo acesso à rede. O acesso é por ordem de chegada. Duas estações podem tentar acessar a rede ao mesmo tempo, o que faz com que ambas as estações voltem e esperem antes de tentar novamente. Este processo é minimizado para Ethernet comutada, onde apenas uma estação está conetada a uma porta de switch. |

8. Clique em **Finish**.

### Configurar a autenticação iSCSI

Para segurança adicional numa rede iSCSI, pode definir a autenticação entre controladores (destinos) e hosts (iniciadores).

O System Manager usa o método CHAP (Challenge Handshake Authentication Protocol), que valida a identidade de alvos e iniciadores durante o link inicial. A autenticação é baseada em uma chave de segurança compartilhada chamada *CHAP secret*.

**Antes de começar**

Você pode definir o segredo CHAP para os iniciadores (hosts iSCSI) antes ou depois de definir o segredo CHAP para os alvos (controladores). Antes de seguir as instruções nesta tarefa, você deve esperar até que os hosts tenham feito uma conexão iSCSI primeiro e, em seguida, definir o segredo CHAP nos hosts individuais. Após as conexões serem feitas, os nomes IQN dos hosts e seus segredos CHAP são listados na caixa de diálogo para autenticação iSCSI (descrita nesta tarefa), e você não precisa inseri-los manualmente.

**Sobre esta tarefa**

Você pode selecionar um dos seguintes métodos de autenticação:

- **Autenticação unidirecional** — Use esta configuração para permitir que o controlador autentique a identidade dos hosts iSCSI (autenticação unidirecional).
- **Autenticação bidirecional** — Use esta configuração para permitir que o controlador e os hosts iSCSI executem a autenticação (autenticação bidirecional). Esta configuração fornece um segundo nível de segurança, permitindo que o controlador autentique a identidade dos hosts iSCSI e, por sua vez, os hosts iSCSI para autenticar a identidade do controlador.

> As definições e funções iSCSI só são apresentadas na página Definições se a sua matriz de armazenamento suportar iSCSI.

**Passos**

1. Selecione **Definições › sistema**.
2. Em Configurações iSCSI, clique em **Configurar autenticação**.

   A caixa de diálogo Configurar autenticação é exibida, que mostra o método atualmente definido. Ele também mostra se algum host tem segredos CHAP configurados.

3. Selecione uma das seguintes opções:
   - **Sem autenticação** — se você não quiser que o controlador autentique a identidade de hosts iSCSI, selecione esta opção e clique em **Finish**. A caixa de diálogo fecha-se e você termina com a configuração.
   - **Autenticação unidirecional** — para permitir que o controlador autentique a identidade dos hosts iSCSI, selecione esta opção e clique em **Next** para exibir a caixa de diálogo Configurar CHAP de destino.
   - **Autenticação bidirecional** — para permitir que o controlador e os hosts iSCSI executem a autenticação, selecione esta opção e clique em **Next** para exibir a caixa de diálogo Configurar CHAP de destino.
4. Para autenticação unidirecional ou bidirecional, insira ou confirme o segredo CHAP para o controlador (o destino). O segredo CHAP deve ter entre 12 e 57 carateres ASCII imprimíveis.

   > Se o segredo CHAP para o controlador foi configurado anteriormente, os carateres no campo são mascarados. Se necessário, você pode substituir os carateres existentes (novos carateres não são mascarados).

5. Execute um dos seguintes procedimentos:
   - Se você estiver configurando a autenticação *one-way*, clique em **Finish**. A caixa de diálogo fecha-se e você termina com a configuração.
   - Se você estiver configurando a autenticação *bidirecional*, clique em **Next** para exibir a caixa de diálogo Configure Initiator CHAP.
6. Para autenticação bidirecional, insira ou confirme um segredo CHAP para qualquer um dos hosts iSCSI (os iniciadores), que pode ter entre 12 e 57 carateres ASCII imprimíveis. Se você não quiser configurar a autenticação bidirecional para um host específico, deixe o campo segredo do iniciador CHAP em branco.

   > Se o segredo CHAP de um host foi configurado anteriormente, os carateres no campo são mascarados. Se necessário, você pode substituir os carateres existentes (novos carateres não são mascarados).

7. Clique em **Finish**.

**Resultados**

A autenticação ocorre durante a sequência de login iSCSI entre os controladores e hosts iSCSI, a menos que você não tenha especificado nenhuma autenticação.

### Ativar definições de deteção iSCSI

Pode ativar as definições relacionadas com a deteção de dispositivos de armazenamento numa rede iSCSI.

As Definições de deteção de destino permitem registar as informações iSCSI da matriz de armazenamento utilizando o protocolo iSNS (Internet Storage Name Service) e também determinar se pretende permitir sessões de deteção sem nome.

**Antes de começar**

Se o servidor iSNS usar um endereço IP estático, esse endereço deve estar disponível para o Registro do iSNS. Tanto o IPv4 como o IPv6 são suportados.

**Sobre esta tarefa**

Pode ativar as seguintes definições relacionadas com a deteção iSCSI:

- **Ativar o servidor iSNS para Registrar um destino** — quando ativado, o storage Registra seu nome qualificado iSCSI (IQN) e informações de porta do servidor iSNS. Essa configuração permite a descoberta do iSNS, de modo que um iniciador possa recuperar as informações da IQN e da porta do servidor iSNS.
- **Ativar sessões de descoberta sem nome** — quando sessões de descoberta sem nome estão ativadas, o iniciador (host iSCSI) não precisa fornecer o IQN do destino (controlador) durante a sequência de login para uma conexão do tipo descoberta. Quando desabilitados, os hosts precisam fornecer o IQN para estabelecer uma sessão de descoberta para o controlador. No entanto, o IQN alvo é sempre necessário para uma sessão normal (rolamento de e/S). Desativar esta definição pode impedir que anfitriões iSCSI não autorizados se liguem ao controlador utilizando apenas o seu endereço IP.

> As definições e funções iSCSI só são apresentadas na página Definições se a sua matriz de armazenamento suportar iSCSI.

**Passos**

1. Selecione **Definições › sistema**.
2. Em **iSCSI settings**, clique em **View/Edit Target Discovery Settings**.

   A caixa de diálogo Target Discovery Settings (Definições de deteção de destino) é apresentada. Abaixo do campo **Enable iSNS Server**… (Ativar servidor iSNS*…), a caixa de diálogo indica se o controlador já está registado.

3. Para Registrar o controlador, selecione **Ativar o servidor iSNS para Registrar meu destino** e, em seguida, selecione uma das seguintes opções:
   - **Obter automaticamente a configuração do servidor DHCP** — Selecione essa opção se desejar configurar o servidor iSNS usando um servidor DHCP (Dynamic Host Configuration Protocol). Esteja ciente de que, se você usar essa opção, todas as portas iSCSI no controlador devem ser configuradas para usar DHCP também. Se necessário, atualize as definições da porta iSCSI do controlador para ativar esta opção.

Para que o servidor DHCP forneça o endereço do servidor iSNS, você deve configurar o servidor DHCP para usar a opção 43 — "'informações específicas do fornecedor.'" esta opção precisa conter o endereço do servidor iSNS IPv4 em bytes de dados 0xA-0xd (10-13).

- **Especifique manualmente a configuração estática** — Selecione esta opção se desejar inserir um endereço IP estático para o servidor iSNS. (Se desejado, você pode cortar e colar endereços nos campos.) No campo, insira um endereço IPv4 ou um endereço IPv6. Se você configurou ambos, IPv4 é o padrão. Insira também uma porta de escuta TCP (use o padrão 3205 ou insira um valor entre 49152 e 65535).

4. Para permitir que o storage array participe de sessões de descoberta sem nome, selecione **Ativar sessões de descoberta sem nome**.
   - Quando ativado, os iniciadores iSCSI não são necessários para especificar o IQN de destino para recuperar as informações do controlador.
   - Quando desabilitadas, as sessões de descoberta são impedidas a menos que o iniciador forneça o IQN de destino. Desativar sessões de descoberta sem nome fornece segurança adicional.
5. Clique em **Salvar**.

**Resultados**

Uma barra de progresso aparece quando o System Manager tenta Registrar o controlador no servidor iSNS. Esse processo pode levar até cinco minutos.

### Visualizar pacotes de estatísticas iSCSI

Pode visualizar dados sobre as ligações iSCSI à sua matriz de armazenamento.

**Sobre esta tarefa**

O System Manager mostra estes tipos de estatísticas iSCSI. Todas as estatísticas são apenas de leitura e não podem ser definidas.

Os tipos de estatísticas exibidos no System Manager baseiam-se nas estatísticas disponíveis para seu storage array.

- **Ethernet MAC statistics** — fornece estatísticas para o controle de acesso de Mídia (MAC). O MAC também fornece um mecanismo de endereçamento chamado endereço físico ou endereço MAC. O endereço MAC é um endereço exclusivo atribuído a cada adaptador de rede. O endereço MAC ajuda a entregar pacotes de dados a um destino dentro da sub-rede.
- **Ethernet TCP/IP statistics** — fornece estatísticas para o TCP/IP, que é o Transmission Control Protocol (TCP) e o Internet Protocol (IP) para o dispositivo iSCSI. Com o TCP, os aplicativos em hosts em rede podem criar conexões entre si, sobre as quais eles podem trocar dados em pacotes. O IP é um protocolo orientado a dados que comunica dados através de uma rede interligada por pacotes. As estatísticas de IPv4 e as estatísticas de IPv6 são mostradas separadamente.
- **Estatísticas do kernel Ethernet** — fornece estatísticas para os drivers do kernel da plataforma do dispositivo iSCSI. As estatísticas do kernel exibem dados de rede semelhantes à opção de estatísticas TCP/IP. No entanto, os dados estatísticos do kernel são coletados dos drivers do kernel da plataforma em vez de diretamente do hardware iSCSI.
- **Estatísticas locais de destino/Iniciador (Protocolo)** — mostra estatísticas para o destino iSCSI, que fornece acesso em nível de bloco a sua Mídia de armazenamento e mostra as estatísticas iSCSI para o storage array quando usado como iniciador em operações de espelhamento assíncrono.

- **DCBX Operational States statistics** — exibe os estados operacionais dos vários recursos do Data Center Bridging Exchange (DCBX).
- **LLDP TLV statistics** — exibe as estatísticas do valor de comprimento do tipo (TLV) do Protocolo de descoberta de camada de enlace (LLDP).
- **DCBX TLV statistics** — exibe as informações que identificam as portas de host do storage array em um ambiente DCB (Data Center Bridging). Essas informações são compartilhadas com os pares de rede para fins de identificação e capacidade.

Você pode visualizar cada uma dessas estatísticas como estatísticas em bruto ou como estatísticas de linha de base. As estatísticas em bruto são todas as estatísticas que foram coletadas desde que os controladores foram iniciados. As estatísticas da linha de base são estatísticas pontuais que foram reunidas desde que você definiu o tempo da linha de base.

**Passos**

1. Selecione menu:guia Support [Support Center > Diagnostics] (suporte > Centro de suporte > Diagnóstico).
2. Selecione **Ver Pacotes de Estatísticas iSCSI**.
3. Clique num separador para ver os diferentes conjuntos de estatísticas.
4. Para definir a linha de base, clique em **Definir nova linha de base**.

   Definir a linha de base define um novo ponto de partida para a coleção das estatísticas. A mesma linha de base é utilizada para todas as estatísticas iSCSI.

### Ver sessões iSCSI

Pode visualizar informações detalhadas sobre as ligações iSCSI à sua matriz de armazenamento. Sessões iSCSI podem ocorrer com anfitriões ou matrizes de armazenamento remotas numa relação de espelhamento assíncrono.

**Passos**

1. Selecione **Definições › sistema**.
2. Selecione **View/End iSCSI Sessions** (Ver/terminar sessões iSCSI).

   É apresentada uma lista das sessões iSCSI atuais.

3. **Opcional:** para ver informações adicionais sobre uma sessão iSCSI específica, selecione uma sessão e clique em **Exibir detalhes**.

**Detalhes do campo**

| Item | Descrição |
| --- | --- |
| Identificador de sessão (SSID) | Uma cadeia hexadecimal que identifica uma sessão entre um iniciador iSCSI e um destino iSCSI. O SSID é composto pelo ISID e pelo TPGT. |
| Session ID do iniciador (ISID) | A parte do iniciador do identificador da sessão. O iniciador especifica o ISID durante o login. |
| Target Portal Group | O destino iSCSI. |
| Tag de grupo do Portal de destino (TPGT) | A parte alvo do identificador da sessão. Um identificador numérico de 16 bits para um grupo de portal de destino iSCSI. |
| Nome iSCSI do iniciador | O nome único mundial do iniciador. |
| Etiqueta iSCSI do iniciador | A etiqueta de utilizador definida no System Manager. |
| Alias iSCSI do iniciador | Um nome que também pode ser associado a um nó iSCSI. O alias permite que uma organização associe uma cadeia de carateres amigável ao nome iSCSI. No entanto, o alias não substitui o nome iSCSI. O alias iSCSI do iniciador só pode ser definido no host, não no System Manager |
| Host | Um servidor que envia entrada e saída para o storage array. |
| ID de ligação (CID) | Um nome exclusivo para uma conexão dentro da sessão entre o iniciador e o destino. O iniciador gera esse ID e o apresenta ao alvo durante as solicitações de login. O ID da conexão também é apresentado durante os logouts que fecham as conexões. |
| Identificador da porta | A porta do controlador associada à ligação. |
| Endereço IP do iniciador | O endereço IP do iniciador. |
| Parâmetros de login negociados | Os parâmetros que são transacionados durante o início de sessão da sessão iSCSI. |
| Método de autenticação | A técnica para autenticar usuários que desejam acesso à rede iSCSI. Os valores válidos são **CHAP** e **None**. |
| Método de resumo do cabeçalho | A técnica para mostrar possíveis valores de cabeçalho para a sessão iSCSI. HeaderDigest e DataDigest podem ser **None** ou **CRC32C**. O valor padrão para ambos é **nenhum**. |

| Item | Descrição |
| --- | --- |
| Método de resumo de dados | A técnica para mostrar possíveis valores de dados para a sessão iSCSI. HeaderDigest e DataDigest podem ser **None** ou **CRC32C**. O valor padrão para ambos é **nenhum**. |
| Máximo de ligações | O maior número de conexões permitido para a sessão iSCSI. O número máximo de conexões pode ser de 1 a 4. O valor padrão é **1**. |
| Alias de destino | O rótulo associado ao alvo. |
| Alias do iniciador | O rótulo associado ao iniciador. |
| Endereço IP de destino | O endereço IP do destino para a sessão iSCSI. Nomes DNS não são suportados. |
| Inicial R2T | O estado inicial pronto para transferir. O status pode ser **Sim** ou **não**. |
| Comprimento máximo de rutura | A carga útil máxima SCSI em bytes para esta sessão iSCSI. O comprimento máximo de rutura pode ser de 512 a 262.144 (256 KB). O valor padrão é **262.144 (256 KB)**. |
| Comprimento da primeira explosão | O payload SCSI em bytes para dados não solicitados para esta sessão iSCSI. O primeiro comprimento de rutura pode ser de 512 a 131.072 (128 KB). O valor padrão é **65.536 (64 KB)**. |
| Tempo predefinido para aguardar | O número mínimo de segundos a aguardar antes de tentar efetuar uma ligação após o encerramento da ligação ou uma reposição da ligação. O valor de tempo de espera padrão pode ser de 0 a 3600. A predefinição é **2**. |
| Tempo predefinido para reter | O número máximo de segundos em que a conexão ainda é possível após o término de uma conexão ou uma reinicialização da conexão. O tempo padrão para reter pode ser de 0 a 3600. O valor padrão é **20**. |
| Máximo de R2T | O número máximo de "pronto para transferências" pendentes para esta sessão iSCSI. O valor máximo de pronto a transferir pode ser de 1 a 16. A predefinição é **1**. |
| Nível de recuperação de erro | O nível de recuperação de erros para esta sessão iSCSI. O valor do nível de recuperação de erros é sempre definido como **0**. |
| Comprimento máximo do segmento de dados de receção | A quantidade máxima de dados que o iniciador ou o destino podem receber em qualquer unidade de dados de carga útil iSCSI (PDU). |
| Nome de destino | O nome oficial do alvo (não o alias). O nome de destino com o formato *iqn*. |

| Item | Descrição |
| --- | --- |
| Nome do iniciador | O nome oficial do iniciador (não o alias). O nome do iniciador que usa o formato *iqn* ou *eui*. |

4. **Opcional:** para salvar o relatório em um arquivo, clique em **Salvar**.

   O arquivo é salvo na pasta Downloads do navegador com o nome do `iscsi-session-connections.txt`arquivo .

### Terminar sessão iSCSI

Você pode terminar uma sessão iSCSI que não é mais necessária. Sessões iSCSI podem ocorrer com hosts ou matrizes de armazenamento remotas em uma relação de espelhamento assíncrono.

#### Sobre esta tarefa

Você pode querer terminar uma sessão iSCSI por estes motivos:

- **Acesso não autorizado** — se um iniciador iSCSI estiver conetado e não tiver acesso, você poderá encerrar a sessão iSCSI para forçar o iniciador iSCSI a sair da matriz de armazenamento. O iniciador iSCSI poderia ter feito logon porque o método de autenticação nenhum estava disponível.
- **Tempo de inatividade do sistema** — se você precisar remover uma matriz de armazenamento e ver que os iniciadores iSCSI ainda estão conetados, você pode encerrar as sessões iSCSI para tirar os iniciadores iSCSI da matriz de armazenamento.

#### Passos

1. Selecione **Definições › sistema**.
2. Selecione **View/End iSCSI Sessions** (Ver/terminar sessões iSCSI).

   É apresentada uma lista das sessões iSCSI atuais.

3. Selecione a sessão que pretende terminar
4. Clique em **Terminar sessão** e confirme que pretende executar a operação.

### Configurar o iSER em portas InfiniBand

Se o controlador incluir uma porta iSER over InfiniBand, você poderá configurar a conexão de rede ao host.

#### Antes de começar

- Sua controladora deve incluir uma porta iSER over InfiniBand; caso contrário, as configurações iSER over InfiniBand não estão disponíveis no System Manager.
- Você deve saber o endereço IP da conexão do host.

#### Passos

1. Selecione **hardware**.
2. Se o gráfico mostrar as unidades, clique na guia **Controllers & Components** (Controladores e

componentes).

O gráfico muda para mostrar os controladores em vez das unidades.

3. Clique no controlador com a porta iSER over InfiniBand que você deseja configurar.

É apresentado o menu de contexto do controlador.

4. Selecione **Configure iSER over InfiniBand Ports**.

A caixa de diálogo Configurar portas iSER em InfiniBand é aberta.

5. Na lista suspensa, selecione a porta HIC que deseja configurar e insira o endereço IP do host.
6. Clique em **Configurar**.
7. Conclua a configuração e, em seguida, redefina a porta iSER em InfiniBand clicando em **Yes**.

#### Visualizar estatísticas do iSER em InfiniBand

Se a controladora do storage array incluir uma porta iSER over InfiniBand, você poderá visualizar dados sobre as conexões de host.

##### Sobre esta tarefa

O System Manager mostra os seguintes tipos de estatísticas iSER over InfiniBand. Todas as estatísticas são apenas de leitura e não podem ser definidas.

- **Estatísticas locais de destino (protocolo)** — fornece estatísticas para o destino iSER over InfiniBand, que mostra acesso em nível de bloco a sua Mídia de storage.
- **ISER over InfiniBand Interface statistics** — fornece estatísticas para todas as portas iSER na interface InfiniBand, que inclui estatísticas de desempenho e informações de erro de link associadas a cada porta de switch.

Você pode visualizar cada uma dessas estatísticas como estatísticas em bruto ou como estatísticas de linha de base. As estatísticas em bruto são todas as estatísticas que foram coletadas desde que os controladores foram iniciados. As estatísticas da linha de base são estatísticas pontuais que foram reunidas desde que você definiu o tempo da linha de base.

##### Passos

1. Selecione **Definições › sistema**.
2. Selecione **View iSER over InfiniBand Statistics**.
3. Clique num separador para ver os diferentes conjuntos de estatísticas.
4. **Opcional:** para definir a linha de base, clique em **Definir nova linha de base**.

Definir a linha de base define um novo ponto de partida para a coleção das estatísticas. A mesma linha de base é usada para todas as estatísticas iSER over InfiniBand.

## Gerenciar portas NVMe

#### Visão geral do NVMe

Algumas controladoras incluem uma porta para implementar o NVMe (Non-Volatile

Memory Express) em Fabrics. O NVMe possibilita a comunicação de alto desempenho entre os hosts e o storage array.

#### O que é o NVMe?

*NVM* significa "memória não volátil" e é memória persistente usada em muitos tipos de dispositivos de armazenamento. O *NVMe* (NVM Express) é uma interface ou protocolo padronizado projetado especificamente para comunicação em várias filas de alto desempenho com dispositivos NVM.

#### O que é o NVMe sobre Fabrics?

O *NVMe over Fabrics (NVMe-of)* é uma especificação de tecnologia que permite que comandos e dados baseados em mensagens NVMe transfiram entre um computador host e o storage em uma rede. Um storage array NVMe (chamado de *subsistema*) pode ser acessado por um host usando uma malha. Os comandos NVMe são ativados e encapsulados em camadas de abstração de transporte no lado do host e no lado do subsistema. Isso estende a interface NVMe de alto desempenho de ponta a ponta do host para o storage, padronizando e simplificando o conjunto de comandos.

O storage NVMe-of é apresentado a um host como um dispositivo de storage de bloco local. O volume (chamado de *namespace*) pode ser montado em um sistema de arquivos como em qualquer outro dispositivo de armazenamento de bloco. Você pode usar a API REST, o SMcli ou o Gerenciador de sistemas do SANtricity para provisionar seu storage conforme necessário.

#### O que é um nome qualificado do NVMe (NQN)?

O nome qualificado do NVMe (NQN) é usado para identificar o destino do storage remoto. O nome qualificado do NVMe para o storage array sempre é atribuído pelo subsistema e não pode ser modificado. Há apenas um nome qualificado do NVMe para todo o array. O nome qualificado do NVMe está limitado a 223 carateres. Pode compará-lo com um nome qualificado iSCSI.

#### O que é um namespace e um ID de namespace?

Um namespace é o equivalente a uma unidade lógica no SCSI, que se relaciona a um volume no array. O ID do namespace (NSID) é equivalente a um número de unidade lógica (LUN) no SCSI. Você cria o NSID no tempo de criação do namespace e pode configurá-lo para um valor entre 1 e 255.

#### O que é uma controladora NVMe?

Semelhante a um Nexus I_T SCSI, que representa o caminho do iniciador do host para o destino do sistema de storage, uma controladora NVMe criada durante o processo de conexão do host fornece um caminho de acesso entre um host e os namespaces no storage array. Um NQN para o host, além de um identificador de porta do host, identifica exclusivamente um controlador NVMe. Embora um controlador NVMe só possa ser associado a um único host, ele pode acessar vários namespaces.

Você configura quais hosts podem acessar quais namespaces e definir o ID do namespace para o host usando o Gerenciador de sistema do SANtricity. Em seguida, quando a controladora NVMe é criada, a lista de IDs de namespace acessíveis pela controladora NVMe é criada e usada para configurar as conexões permitidas.

### Configurar portas NVMe em InfiniBand

Se o controlador incluir uma conexão NVMe over InfiniBand, você poderá configurar as configurações da porta NVMe na página hardware.

**Antes de começar**

- Seu controlador deve incluir uma porta de host NVMe over InfiniBand. Caso contrário, as configurações de NVMe em InfiniBand não estão disponíveis no System Manager.
- Você deve saber o endereço IP da conexão do host.

> As configurações e funções do NVMe over InfiniBand aparecerão somente se a controladora do storage array incluir uma porta NVMe over InfiniBand.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar as unidades, clique na guia **Controllers & Components** (Controladores e componentes).

   O gráfico muda para mostrar os controladores em vez das unidades.
3. Clique no controlador com a porta NVMe over InfiniBand que você deseja configurar.

   É apresentado o menu de contexto do controlador.
4. Selecione **Configurar portas NVMe over InfiniBand**.

   A caixa de diálogo Configurar portas NVMe over InfiniBand será exibida.
5. Selecione a porta HIC que pretende configurar na lista pendente e, em seguida, introduza o endereço IP.

   Se você estiver configurando um storage array EF600 com um HIC compatível com 200GB, essa caixa de diálogo exibirá dois campos de Endereço IP, um para uma porta física (externa) e outro para uma porta virtual (interna). Você deve atribuir um endereço IP exclusivo para ambas as portas. Essas configurações permitem que o host estabeleça um caminho entre cada porta e que o HIC alcance o máximo desempenho. Se você não atribuir um endereço IP à porta virtual, o HIC será executado a aproximadamente metade de sua velocidade capaz.
6. Clique em **Configurar**.
7. Conclua a configuração e, em seguida, redefina a porta NVMe over InfiniBand clicando em **Yes**.

**Configurar o NVMe em portas RoCE**

Se o controlador incluir uma conexão para NVMe em RoCE (RDMA em Converged Ethernet), você poderá configurar as configurações da porta NVMe na página hardware.

**Antes de começar**

- Sua controladora deve incluir uma porta de host NVMe em RoCE; caso contrário, as configurações NVMe em RoCE não estarão disponíveis no System Manager.
- Você deve saber o endereço IP da conexão do host.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar as unidades, clique na guia **Controllers & Components** (Controladores e componentes).

   O gráfico muda para mostrar os controladores em vez das unidades.

3. Clique no controlador com a porta NVMe sobre RoCE que você deseja configurar.

   É apresentado o menu de contexto do controlador.

4. Selecione **Configure NVMe over RoCE ports**.

   A caixa de diálogo Configurar portas NVMe em RoCE será aberta.

5. Na lista suspensa, selecione a porta HIC que deseja configurar.
6. Clique em **seguinte**.

   Para ver todas as configurações de porta, clique no link **Mostrar mais configurações de porta** à direita da caixa de diálogo.

   **Detalhes do campo**

| Definição da porta | Descrição |
| --- | --- |
| Velocidade da porta ethernet configurada | Selecione a velocidade que corresponde à capacidade de velocidade do SFP na porta. |
| Ativar IPv4 / ativar IPv6 | Selecione uma ou ambas as opções para ativar o suporte para redes IPv4G e IPv6G.<br><br>Se pretender desativar o acesso à porta, desmarque ambas as caixas de verificação. |
| Tamanho MTU (disponível clicando em **Mostrar mais configurações de porta**.) | Se necessário, introduza um novo tamanho em bytes para a unidade máxima de transmissão (MTU).<br><br>O tamanho padrão da unidade máxima de transmissão (MTU) é de 1500 bytes por quadro. Tem de introduzir um valor entre 1500 e 9000. |

   Se você selecionou **Ativar IPv4**, uma caixa de diálogo será aberta para selecionar IPv4 configurações depois de clicar em **Avançar**. Se você selecionou **Ativar IPv6**, uma caixa de diálogo será aberta para selecionar IPv6 configurações depois de clicar em **Avançar**. Se você selecionou ambas as opções, a caixa de diálogo para configurações IPv4 será aberta primeiro e, depois de clicar em **Avançar**, a caixa de diálogo para configurações IPv6 será aberta.

7. Configure as definições IPv4 e/ou IPv6, automática ou manualmente.

**Detalhes do campo**

| Definição da porta | Descrição |
| --- | --- |
| Obter automaticamente a configuração | Selecione esta opção para obter a configuração automaticamente. |
| Especifique manualmente a configuração estática | Selecione esta opção e, em seguida, introduza um endereço estático nos campos. (Se desejado, você pode cortar e colar endereços nos campos.) Para IPv4, inclua a máscara de sub-rede e o gateway. Para IPv6, inclua o endereço IP roteável e o endereço IP do roteador. Se você estiver configurando um storage array EF600 com um HIC compatível com 200GB, essa caixa de diálogo exibirá dois conjuntos de campos para parâmetros de rede, um para uma porta física (externa) e outro para uma porta virtual (interna). Você deve atribuir parâmetros exclusivos para ambas as portas. Essas configurações permitem que o host estabeleça um caminho entre cada porta e que o HIC alcance o máximo desempenho. Se você não atribuir um endereço IP à porta virtual, o HIC será executado a aproximadamente metade de sua velocidade capaz. |

8. Clique em **Finish**.

### Veja as estatísticas do NVMe sobre Fabrics

É possível visualizar dados sobre as conexões NVMe sobre Fabrics com o storage array.

**Sobre esta tarefa**

O System Manager mostra esses tipos de estatísticas de NVMe sobre Fabrics. Todas as estatísticas são apenas de leitura e não podem ser definidas.

- **Estatísticas do subsistema NVMe** — mostra estatísticas para o controlador NVMe e sua fila. O controlador NVMe fornece um caminho de acesso entre um host e os namespaces no storage array. Você pode revisar as estatísticas do subsistema NVMe para itens como falhas de conexão, reconfigurações e paradas.
- **Estatísticas da interface RDMA** — fornece estatísticas para todas as portas NVMe sobre Fabrics na interface RDMA, que inclui estatísticas de desempenho e informações de erro de link associadas a cada porta do switch. Essa guia só aparece quando as portas NVMe sobre Fabrics estiverem disponíveis.

Você pode visualizar cada uma dessas estatísticas como estatísticas em bruto ou como estatísticas de linha de base. As estatísticas em bruto são todas as estatísticas que foram coletadas desde que os controladores foram iniciados. As estatísticas da linha de base são estatísticas pontuais que foram reunidas desde que você definiu o tempo da linha de base.

**Passos**

1. Selecione **Definições › sistema**.
2. Selecione **View NVMe over Fabrics Statistics**.
3. **Opcional:** para definir a linha de base, clique em **Definir nova linha de base**.

   Definir a linha de base define um novo ponto de partida para a coleção das estatísticas. A mesma linha de base é usada para todas as estatísticas do NVMe.

# Gerenciar unidades

## estados da unidade

O System Manager relata vários estados para unidades.

### estados de acessibilidade

| Estado | Definição |
|---|---|
| Ignorado | A unidade está fisicamente presente, mas o controlador não pode se comunicar com ela em qualquer uma das portas. |
| Incompatível | Existe uma das seguintes condições:<br>• A unidade não é certificada para uso no storage de armazenamento.<br>• A unidade tem um tamanho de setor diferente.<br>• A unidade tem dados de configuração inutilizáveis de uma versão de firmware mais antiga ou mais recente. |
| Removido | A unidade foi removida indevidamente do storage de armazenamento. |
| Presente | O controlador pode se comunicar com a unidade em ambas as portas. |
| Sem resposta | A unidade não está respondendo aos comandos. |

### estados de função

| Estado | Definição |
|---|---|
| Atribuído | A unidade é membro de um pool ou grupo de volume. |
| Hot spare in-use | A unidade está sendo usada atualmente como um substituto para uma unidade que falhou. As peças sobressalentes quentes são usadas apenas em grupos de volume, não em pools. |
| Reserva quente em espera | A unidade está pronta para ser usada como substituição de uma unidade que falhou. As peças sobressalentes quentes são usadas apenas em grupos de volume, não em pools. |
| Não atribuído | A unidade não é membro de um pool ou grupo de volume. |

### estados de disponibilidade

| Estado | Definição |
|---|---|
| Falha | A unidade não está funcionando. Os dados na unidade não estão disponíveis. |

| Estado | Definição |
| --- | --- |
| Avaria iminente | Foi detetado que a unidade poderia falhar em breve. Os dados na unidade ainda estão disponíveis. |
| Offline | A unidade não está disponível para armazenar dados normalmente porque faz parte de um grupo de volumes que está sendo exportado ou está passando por uma atualização de firmware. |
| Ideal | A unidade está funcionando normalmente. |

### Discos de estado sólido (SSDs)

Os discos de estado sólido (SSDs) são dispositivos de armazenamento de dados que usam memória de estado sólido (flash) para armazenar dados persistentemente. Os SSDs emulam discos rígidos convencionais e estão disponíveis com as mesmas interfaces que os discos rígidos usam.

#### Vantagens dos SSDs

As vantagens dos SSDs em relação aos discos rígidos incluem:

- Arranque mais rápido (sem aumento)
- Menor latência
- Operações de e/S mais altas por segundo (IOPS)
- Maior confiabilidade com menos peças móveis
- Menor consumo de energia
- Menos calor produzido e menos resfriamento necessário

#### Identificação de SSDs

Na página hardware, você pode localizar os SSDs na visualização do compartimento frontal. Procure por compartimentos de unidade que exibem um ícone de raio, que indica que um SSD está instalado.

#### Grupos de volume

Todas as unidades de um grupo de volumes devem ser do mesmo tipo de Mídia (todos os SSDs ou todos os discos rígidos). Os grupos de volume não podem ter uma mistura de tipos de Mídia ou tipos de interface.

#### Armazenamento em cache

O armazenamento em cache de gravação da controladora está sempre habilitado para SSDs. O armazenamento em cache de gravação melhora o desempenho e prolonga a vida útil do SSD.

Além do cache da controladora, você pode implementar o recurso cache SSD para melhorar o desempenho geral do sistema. No cache SSD, os dados são copiados de volumes e armazenados em dois volumes RAID internos (um por controladora).

### Limite a vista da unidade

Se a matriz de armazenamento incluir unidades com diferentes tipos de atributos físicos e lógicos, a página hardware fornece campos de filtro que ajudam a limitar a visualização da unidade e localizar unidades específicas.

#### Sobre esta tarefa

Os filtros de unidade podem limitar a exibição a apenas certos tipos de unidades físicas (por exemplo, todas as SAS), com certos atributos de segurança (por exemplo, com capacidade segura), em determinados locais lógicos (por exemplo, Grupo de volume 1). Você pode usar esses filtros juntos ou separadamente.

> Se todas as unidades compartilharem os mesmos atributos físicos, o campo de filtro **Mostrar unidades que são…** não será exibido. Se todas as unidades compartilharem os mesmos atributos lógicos, o campo de filtro **em qualquer lugar no storage de armazenamento** não será exibido.

#### Passos

1. Selecione **hardware**.
2. No primeiro campo de filtro (em **Mostrar unidades que são…**), clique na seta suspensa para exibir os tipos de unidade disponíveis e os atributos de segurança.

   Os tipos de unidade podem incluir:

   - Tipo de suporte de unidade (SSD, HDD)
   - Tipo de interface da unidade
   - Capacidade de transmissão (mais alta para mais baixa)
   - Velocidade da unidade (da mais alta para a mais baixa) os atributos de segurança podem incluir:
   - Com capacidade segura
   - Habilitado para segurança
   - Capacidade DA (Data Assurance)
   - Compatível com FIPS
   - Compatível com FIPS (FIPS 140-2)
   - Compatível com FIPS (FIPS 140-3)

     Se qualquer um desses atributos for o mesmo para todas as unidades, eles não serão exibidos na lista suspensa. Por exemplo, se o storage array incluir todas as unidades SSD com interfaces SAS e velocidades de 15000 RPM, mas alguns SSDs tiverem capacidades diferentes, a lista suspensa exibirá somente as capacidades como opção de filtragem.

   Quando você seleciona uma opção no campo, as unidades que não correspondem aos critérios de filtro ficam esmaecidas na exibição gráfica.

3. Na segunda caixa de filtro, clique na seta suspensa para exibir os locais lógicos disponíveis para as unidades.

> Se você precisar limpar seus critérios de filtro, selecione **Limpar** na extrema direita das caixas de filtro.

Os locais lógicos podem incluir:

- Piscinas
- Grupos de volume
- Hot spare
- Cache SSD
- Não atribuído

  Quando você seleciona uma opção no campo, as unidades que não correspondem aos critérios de filtro ficam esmaecidas na exibição gráfica.

4. Opcionalmente, você pode selecionar **ligar as luzes de localização** na extrema direita dos campos de filtro para ligar as luzes de localização para as unidades exibidas.

   Essa ação ajuda você a localizar fisicamente as unidades no storage array.

### Ligue a luz de localização da unidade

Na página hardware, você pode ativar a luz localizador para encontrar a localização física de uma unidade no storage de armazenamento.

#### Sobre esta tarefa

Você pode localizar unidades individuais ou várias unidades mostradas na página hardware.

#### Passos

1. Selecione **hardware**.
2. Para localizar uma ou mais unidades, execute um dos seguintes procedimentos:
   - * Unidade única* — a partir do gráfico da prateleira, encontre a unidade que você deseja localizar fisicamente no array. (Se o gráfico mostrar os controladores, clique na guia **Drives**.) Clique na unidade para exibir seu menu de contexto e selecione **Ativar luz localizador**.

     A luz de localização da unidade acende-se. Quando tiver localizado fisicamente a unidade, volte à caixa de diálogo e selecione **Desligar**.

   - * Várias unidades* — nos campos de filtro, selecione um tipo de unidade física na lista suspensa esquerda e um tipo de unidade lógica na lista suspensa direita. O número de unidades que correspondem aos seus critérios é mostrado na extrema direita dos campos. Em seguida, você pode clicar em **ligar as luzes do localizador** ou selecionar **Localizar todas as unidades filtradas** no menu de contexto. Quando tiver localizado fisicamente as unidades, volte à caixa de diálogo e selecione **Desligar**.

### Ver o estado e as definições da unidade

Pode visualizar o estado e as definições das unidades, como o tipo de material, o tipo de interface e a capacidade.

#### Passos

1. Selecione **hardware**.
2. Se o gráfico mostrar os controladores, clique na guia **Drives**.

O gráfico muda para mostrar as unidades em vez dos controladores.

3. Selecione a unidade para a qual pretende ver o estado e as definições.

   O menu de contexto da unidade é aberto.

4. Selecione **Ver definições**.

   A caixa de diálogo Configurações da unidade é aberta.

5. Para ver todas as configurações, clique em **Mostrar mais configurações** no canto superior direito da caixa de diálogo.

**Detalhes do campo**

| Definições | Descrição |
| --- | --- |
| Estado | Apresenta a avaria ideal, Offline, não crítica e falhou. O estado ideal indica a condição de trabalho pretendida. |
| Modo | Exibe Assigned, Unassigned, Hot Spare Standby ou Hot Spare em uso. |
| Localização | Mostra o número do compartimento e do compartimento onde a unidade está localizada. |
| Atribuído a/pode proteger/proteger | Se a unidade for atribuída a um pool, grupo de volumes ou cache SSD, este campo exibirá "atribuído a". O valor pode ser um nome de pool, nome de grupo de volume ou nome de cache SSD. Se a unidade for atribuída a um hot spare e o seu modo for Standby, este campo apresenta "CAN Protect for" (pode proteger para). Se o hot spare puder proteger um ou mais grupos de volumes, os nomes dos grupos de volumes serão exibidos. Se não puder proteger um grupo de volumes, ele exibirá 0 grupos de volume.<br><br>Se a unidade for atribuída a um hot spare e o seu modo estiver a ser utilizado, este campo apresenta "protecting" (proteção). O valor é o nome do grupo de volumes afetado.<br><br>Se a unidade não for atribuída, este campo não será exibido. |
| Tipo de material | Apresenta o tipo de suporte de gravação utilizado pela unidade, que pode ser uma unidade de disco rígido (HDD) ou um disco de estado sólido (SSD). |
| Percentagem de resistência utilizada (apenas apresentada se as unidades SSD estiverem presentes) | A quantidade de dados gravados no disco até à data, dividida pelo limite teórico total de escrita. |
| Tipo de interface | Exibe o tipo de interface que a unidade usa, como SAS. |
| Redundância de caminho da unidade | Mostra se as conexões entre a unidade e o controlador são redundantes (Sim) ou não (não). |
| Capacidade (GiB) | Mostra a capacidade utilizável (capacidade total configurada) da unidade. |
| Velocidade (RPM) | Mostra a velocidade em RPM (não aparece para SSDs). |
| Taxa de dados atual | Mostra a taxa de transferência de dados entre a unidade e a matriz de armazenamento. |

| Definições | Descrição |
| --- | --- |
| Tamanho do setor lógico (bytes) | Mostra o tamanho do setor lógico que a unidade usa. |
| Tamanho do setor físico (bytes) | Mostra o tamanho do setor físico utilizado pela unidade. Normalmente, o tamanho do setor físico é de 4096 bytes para unidades de disco rígido. |
| Versão do firmware da unidade | Mostra o nível de revisão do firmware da unidade. |
| Identificador mundial | Mostra o identificador hexadecimal exclusivo para a unidade. |
| ID do produto | Mostra o identificador do produto, que é atribuído pelo fabricante. |
| Número de série | Mostra o número de série da unidade. |
| Fabricante | Mostra o fornecedor da unidade. |
| Data de fabricação | Mostra a data em que a unidade foi construída.<br>Não disponível para unidades NVMe. |
| Com capacidade segura | Mostra se a unidade é segura (Sim) ou não (não). As unidades com capacidade segura podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (nível 140-2 ou 140-3), que criptografam dados durante gravações e descriptografam dados durante leituras. Essas unidades são consideradas seguras-*Capable* porque podem ser usadas para segurança adicional usando o recurso Segurança da Unidade. Se o recurso Segurança da unidade estiver habilitado para grupos de volume e pools usados com essas unidades, as unidades se tornarão seguras-*enabled*. |
| Habilitado para segurança | Mostra se a unidade está ativada para segurança (Sim) ou não (não). As unidades habilitadas para segurança são usadas com o recurso Segurança da unidade. Quando você ativa o recurso de Segurança da Unidade e, em seguida, aplica o Drive Security a um pool ou grupo de volume em unidades seguras-*capazes*, as unidades ficam seguras-*Enabled*. O acesso de leitura e gravação está disponível somente por meio de um controlador configurado com a chave de segurança correta. Essa segurança adicional impede o acesso não autorizado aos dados em uma unidade que é fisicamente removida do storage array. |
| Leitura/gravação acessível | Mostra se a unidade está acessível para leitura/gravação (Sim) ou não (não). |

| Definições | Descrição |
| --- | --- |
| Identificador da chave de segurança da unidade | Mostra a chave de segurança para unidades habilitadas com segurança. O Drive Security é um recurso de storage array que fornece uma camada extra de segurança com unidades de criptografia completa de disco (FDE) ou unidades FIPS (Federal Information Processing Standard). Quando essas unidades são usadas com o recurso Segurança da Unidade, elas precisam de uma chave de segurança para acessar seus dados. Quando as unidades são fisicamente removidas do array, elas não podem operar até serem instaladas em outro array, em que ponto, elas estarão em um estado de segurança bloqueado até que a chave de segurança correta seja fornecida. |
| Capacidade de garantia de dados (DA) | Mostra se a funcionalidade Data Assurance (DA) está ativada (Sim) ou não (não). O Data Assurance (DA) é um recurso que verifica e corrige erros que podem ocorrer à medida que os dados são transferidos através dos controladores para as unidades. O Data Assurance pode ser ativado no nível de pool ou grupo de volumes, com hosts que usam uma interface de e/S compatível com DA, como Fibre Channel. |
| DULBE capaz | Indica se a opção para erro de bloco lógico desalocado ou não escrito (DULBE) está ativada (Sim) ou não (não). O DULBE é uma opção nas unidades NVMe que permite que o storage array EF300 ou EF600 ofereça suporte a volumes provisionados por recursos. |

6. Clique em **Fechar**.

#### Substitua a unidade logicamente

Se uma unidade falhar ou você quiser substituí-la por qualquer outro motivo, você pode logicamente substituir a unidade com falha por uma unidade não atribuída ou um hot spare totalmente integrado.

##### Sobre esta tarefa

Quando você substitui logicamente uma unidade, ela é atribuída e, em seguida, é um membro permanente do pool ou grupo de volume associado.

Você usa a opção de substituição lógica para substituir os seguintes tipos de unidades:

- Unidades com falha
- Unidades em falta
- Unidades SSD que o Recovery Guru avisou que estão se aproximando do fim da vida útil
- Discos rígidos que o Recovery Guru avisou que tem uma falha iminente na unidade
- Unidades atribuídas (disponível apenas para unidades em um grupo de volumes, não em um pool)

##### Antes de começar

O acionamento de substituição deve ter as seguintes caraterísticas:

- No estado ideal

- No estado não atribuído
- Os mesmos atributos que a unidade que está sendo substituída (tipo de Mídia, tipo de interface, etc.)
- A mesma capacidade FDE (recomendada, mas não necessária)
- A mesma capacidade DA (recomendada, mas não necessária)

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar os controladores, clique na guia **Drives**.

   O gráfico muda para mostrar as unidades em vez dos controladores.

3. Clique na unidade que você deseja substituir logicamente.

   É apresentado o menu de contexto da unidade.

4. Clique em **logicamente Substituir**.
5. **Opcional:** Selecione a caixa de seleção **Fail drive após a substituição** para falhar a unidade original após a substituição.

   Esta caixa de verificação só está ativada se a unidade atribuída original não tiver falhado ou estiver em falta.

6. Na tabela **Selecione uma unidade de substituição**, selecione a unidade de substituição que deseja usar.

   A tabela lista apenas as unidades que são compatíveis com a unidade que você está substituindo. Se possível, selecione uma unidade que mantenha a proteção contra perda de gaveta e a proteção contra perda de gaveta.

7. Clique em **Substituir**.

   Se a unidade original estiver com falha ou ausente, os dados serão reconstruídos na unidade de substituição usando as informações de paridade. Esta reconstrução começa automaticamente. As luzes indicadoras de falha da unidade apagam-se e as luzes indicadoras de atividade das unidades no pool ou grupo de volume começam a piscar.

   Se a unidade original não estiver com falha ou ausente, seus dados serão copiados para a unidade de substituição. Esta operação de cópia começa automaticamente. Após a conclusão da operação de cópia, o sistema transfere a unidade original para o estado não atribuído ou, se a caixa de verificação tiver sido selecionada, para o estado Falha.

#### Reconstruir a condução manualmente

A reconstrução da unidade é normalmente iniciada automaticamente após a substituição de uma unidade. Se a reconstrução da unidade não iniciar automaticamente, pode iniciar a reconstrução manualmente.

Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico ou pelo Recovery Guru.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar os controladores, clique na guia **Drives**.

   O gráfico muda para mostrar as unidades em vez dos controladores.

3. Clique na unidade que pretende reconstruir manualmente.

   É apresentado o menu de contexto da unidade.

4. Selecione **Reconstruct** e confirme que deseja executar a operação.

### Inicialize (formate) a unidade

Se você mover unidades atribuídas de um storage array para outro, será necessário inicializar (formatar) as unidades antes que elas possam ser usadas no novo storage array.

#### Sobre esta tarefa

A inicialização remove as informações de configuração anteriores de uma unidade e as retorna ao estado não atribuído. A unidade fica então disponível para adicionar a um novo pool ou grupo de volumes na nova matriz de armazenamento.

Use a operação de inicialização da unidade quando estiver movendo uma única unidade. Não é necessário inicializar unidades se estiver movendo um grupo de volumes inteiro de um storage array para outro.

**Possível perda de dados** — quando você inicializar uma unidade, todos os dados na unidade são perdidos. Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

#### Passos

1. Selecione **hardware**.
2. Se o gráfico mostrar os controladores, clique na guia **Drives**.

   O gráfico muda para mostrar as unidades em vez dos controladores.

3. Clique na unidade que deseja inicializar.

   É apresentado o menu de contexto da unidade.

4. Selecione **Initialize** e confirme se deseja executar a operação.

### Falha na unidade

Se instruído a fazê-lo, você pode falhar manualmente uma unidade.

#### Sobre esta tarefa

O System Manager monitora as unidades na matriz de armazenamento. Quando ele deteta que uma unidade está gerando muitos erros, o Recovery Guru notifica você sobre uma falha iminente de unidade. Se isso acontecer e você tiver uma unidade de substituição disponível, você pode querer falhar a unidade para tomar uma ação preventiva. Se você não tiver uma unidade de substituição disponível, você pode esperar que a unidade falhe por conta própria.

**Possível perda de acesso a dados** — esta operação pode resultar em perda de dados ou perda de redundância de dados. Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico ou pelo Recovery Guru.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar os controladores, clique na guia **Drives**.

   O gráfico muda para mostrar as unidades em vez dos controladores.

3. Clique na unidade que você deseja falhar.

   É apresentado o menu de contexto da unidade.

4. Selecione **Fail**.
5. Mantenha a caixa de seleção **Copiar conteúdo da unidade antes de falhar** selecionada.

   A opção de cópia aparece apenas para unidades atribuídas e para grupos de volume não RAID 0.

   Antes de falhar a unidade, certifique-se de copiar o conteúdo da unidade. Dependendo da sua configuração, você pode potencialmente perder toda a redundância de dados ou dados no pool ou grupo de volumes associado se você não copiar o conteúdo da unidade primeiro.

   A opção de cópia permite uma recuperação mais rápida da unidade do que a reconstrução e reduz a possibilidade de uma falha de volume se outra unidade falhar durante a operação de cópia.

6. Confirme se deseja falhar a unidade.

   Depois que a unidade falhar, aguarde pelo menos 30 segundos antes de removê-la.

### Apagar unidades

Pode utilizar a opção Apagar para preparar uma unidade não atribuída para remoção do sistema. Este procedimento remove permanentemente os dados, garantindo que os dados não podem ser lidos novamente.

#### Antes de começar

A unidade deve estar em um estado não atribuído.

#### Sobre esta tarefa

Utilize a opção Apagar apenas se pretender remover permanentemente todos os dados de uma unidade. Se a unidade estiver habilitada para segurança, a opção Apagar executará uma eliminação criptográfica e redefinirá os atributos de segurança da unidade de volta para a capacidade segura.

O recurso Apagar não suporta alguns modelos de unidade mais antigos. Se tentar apagar um destes modelos mais antigos, é apresentada uma mensagem de erro.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar os controladores, clique na guia **Drives**.

O gráfico muda para mostrar as unidades em vez dos controladores.

3. Opcionalmente, você pode usar os campos de filtro para exibir todas as unidades não atribuídas no compartimento. Na lista suspensa **Mostrar unidades que são…**, selecione **não atribuídas**.

   A vista do compartimento mostra apenas as unidades não atribuídas; todas as outras estão acinzentadas.

4. Para abrir o menu de contexto da unidade, clique em uma unidade que você deseja apagar. (Se você quiser selecionar várias unidades, você pode fazê-lo na caixa de diálogo Apagar unidades.)

   **Possível perda de dados** — a operação Apagar não pode ser desfeita. Certifique-se de que seleciona as unidades corretas durante o procedimento.

5. No menu de contexto, selecione **Apagar**.

   A caixa de diálogo Apagar unidades é aberta, mostrando todas as unidades elegíveis para uma operação de apagamento.

6. Se desejar, selecione unidades adicionais na tabela. Não é possível selecionar *All* drives; certifique-se de que uma unidade permanece desmarcada.
7. Confirme a operação digitando `erase`e clique em **Apagar**.

   Certifique-se de que pretende continuar com esta operação. Depois de clicar em Sim na caixa de diálogo seguinte, a operação não pode ser cancelada.

8. Na caixa de diálogo tempo estimado de conclusão, clique em **Sim** para continuar com a operação de eliminação.

**Resultados**

A operação de eliminação pode demorar vários minutos ou várias horas. Você pode exibir o status no **Home › View Operations in Progress** (Exibir operações em andamento). Quando a operação Apagar for concluída, as unidades estarão disponíveis para uso em outro grupo de volumes ou pool de discos ou em outro storage de armazenamento.

**Depois de terminar**

Se você quiser usar a unidade novamente, você deve iniciá-la primeiro. Para fazer isso, selecione **Initialize** no menu de contexto da unidade.

### Desbloqueie ou redefina unidades NVMe ou FIPS bloqueadas

Se você inserir uma ou mais unidades NVMe ou FIPS bloqueadas em um storage array, poderá desbloquear os dados da unidade adicionando o arquivo de chave de segurança associado às unidades. Se você não tiver uma chave de segurança, poderá executar uma reinicialização em cada unidade bloqueada inserindo seu ID de segurança física (PSID) para redefinir seus atributos de segurança e apagar os dados da unidade.

**Antes de começar**

- Para a opção desbloquear, verifique se o arquivo de chave de segurança (com uma extensão do `.slk`) está disponível no cliente de gerenciamento (o sistema com um navegador usado para acessar o System Manager). Você também deve saber a frase-passe associada à chave.
- Para a opção Redefinir, você deve encontrar o PSID em cada unidade que você deseja redefinir. Para

localizar o PSID, remova fisicamente a unidade e localize a cadeia PSID (máximo de 32 carateres) na etiqueta da unidade e, em seguida, reinstale a unidade.

**Sobre esta tarefa**

Esta tarefa descreve como desbloquear dados em unidades NVMe ou FIPS importando um arquivo de chave de segurança para o storage array. Para situações em que a chave de segurança não está disponível, esta tarefa também descreve como executar uma reinicialização em uma unidade bloqueada.

> Se a unidade foi bloqueada usando um servidor de gerenciamento de chaves externo, selecione **Configurações › sistema › Gerenciamento de chaves de segurança** no System Manager para configurar o gerenciamento de chaves externas e desbloquear a unidade.

Pode aceder à funcionalidade desbloquear a partir da página hardware ou do **Definições › sistema › Gestão da chave de segurança**. A tarefa abaixo fornece instruções na página hardware.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar os controladores, clique na guia **Drives**.

   O gráfico muda para mostrar as unidades em vez dos controladores.

3. Selecione a unidade NVMe ou FIPS que deseja desbloquear ou redefinir.

   O menu de contexto da unidade é aberto.

4. Selecione **Unlock** para aplicar o arquivo de chave de segurança ou **Reset** se você não tiver um arquivo de chave de segurança.

   Essas opções só serão exibidas se você selecionar uma unidade NVMe ou FIPS bloqueada.

   > Durante uma operação de reposição, todos os dados são apagados. Execute apenas uma reinicialização se você não tiver uma chave de segurança. A redefinição de uma unidade bloqueada remove permanentemente todos os dados da unidade e redefine seus atributos de segurança para "segura", mas não ativada. **Esta operação não é reversível.**

5. Execute um dos seguintes procedimentos:
   a. **Unlock**: Na caixa de diálogo **Unlock Secure Drive**, clique em **Browse** e, em seguida, selecione o arquivo de chave de segurança que corresponde à unidade que deseja desbloquear. Em seguida, digite a frase-passe e clique em **Unlock**.
   b. **Reset**: Na caixa de diálogo **Reset locked Drive** (Redefinir unidade bloqueada), insira a cadeia PSID no campo e digite `RESET` para confirmar. Clique em **Reset**.

      Para uma operação de desbloqueio, você só precisa executar essa operação uma vez para desbloquear todas as unidades NVMe ou FIPS. Para uma operação de reinicialização, você deve selecionar individualmente cada unidade que deseja redefinir.

**Resultados**

A unidade agora está disponível para uso em outro grupo de volumes ou pool de discos, ou em outro storage de armazenamento.

# Gerenciar hot spares

## Descrição geral da unidade hot spare

As peças sobressalentes ativas funcionam como unidades de reserva nos grupos de volume RAID 1, RAID 5 ou RAID 6 para o System Manager.

São unidades totalmente funcionais que não contêm dados. Se uma unidade falhar no grupo de volumes, o controlador reconstrói automaticamente os dados da unidade com falha para uma unidade atribuída como hot spare.

As peças sobressalentes quentes não são dedicadas a grupos de volumes específicos. Eles podem ser usados para qualquer unidade com falha na matriz de armazenamento, desde que o hot spare e a unidade compartilhem esses atributos:

- Capacidade igual (ou maior capacidade para o hot spare)
- Mesmo tipo de material (por exemplo, HDD ou SSD)
- Mesmo tipo de interface (por exemplo, SAS)

### Como identificar peças sobressalentes quentes

Você pode atribuir hot spares através do Assistente de configuração inicial ou da página hardware. Para determinar se os hot spares são atribuídos, vá para a página hardware e procure os compartimentos de unidade mostrados em rosa.

### Como funciona a cobertura hot spare

A cobertura hot spare funciona da seguinte forma:

- Você reserva uma unidade não atribuída como hot spare para grupos de volume RAID 1, RAID 5 ou RAID 6.

> Os hot spares não podem ser usados para pools, que têm um método diferente de proteção de dados. Em vez de reservar uma unidade adicional, os pools reservam capacidade extra (chamada *capacidade de preservação*) dentro de cada unidade da piscina. Se uma unidade falhar em um pool, o controlador reconstruirá os dados nessa capacidade extra.

- Se uma unidade dentro de um grupo de volumes RAID 1, RAID 5 ou RAID 6 falhar, a controladora usará automaticamente dados de redundância para reconstruir os dados da unidade com falha. O hot spare é substituído automaticamente pela unidade com falha sem exigir uma troca física.
- Quando você substituiu fisicamente a unidade com falha, uma operação de cópia ocorre da unidade hot spare para a unidade substituída. Se você designou a unidade hot spare como um membro permanente de um grupo de volume, a operação copyback não é necessária.
- A disponibilidade de proteção contra perda de bandeja e proteção contra perda de gaveta para um grupo de volumes depende da localização das unidades que compõem o grupo de volumes. A proteção contra perda de bandeja e a proteção contra perda de gaveta podem ser perdidas devido a uma unidade com falha e à localização da unidade hot spare. Para garantir que a proteção contra perda de bandeja e a proteção contra perda de gaveta não sejam afetadas, você deve substituir uma unidade com falha para iniciar o processo de cópia de segurança.
- O volume do storage array permanece on-line e acessível enquanto você está substituindo a unidade com falha, porque a unidade hot spare é substituída automaticamente pela unidade com falha.

#### Considerações sobre a capacidade da unidade hot spare

Selecione uma unidade com uma capacidade igual ou superior à capacidade total da unidade que pretende proteger. Por exemplo, se você tiver uma unidade de 18 GiB com capacidade configurada de 8 GiB, poderá usar uma unidade de 9 GiB ou maior como hot spare. Geralmente, não atribua uma unidade como hot spare a menos que sua capacidade seja igual ou maior que a capacidade da unidade maior no storage de armazenamento.

> Se as peças sobressalentes quentes não estiverem disponíveis que tenham a mesma capacidade física, uma unidade com menor capacidade pode ser usada como hot spare se a "capacidade usada" da unidade for a mesma ou menor que a capacidade da unidade hot spare.

#### Considerações para tipos de Mídia e interface

A unidade usada como hot spare deve compartilhar o mesmo tipo de Mídia e tipo de interface que as unidades que protegerão. Por exemplo, uma unidade HDD não pode servir como hot spare para unidades SSD.

#### Considerações para unidades com capacidade de segurança

Uma unidade com capacidade segura, como FDE ou FIPS, pode servir como um hot spare para unidades com ou sem recursos de segurança. No entanto, uma unidade que não seja segura não pode servir como hot spare para unidades com recursos de segurança.

Quando você seleciona uma unidade habilitada para segurança a ser usada para um hot spare, o System Manager solicita que você execute uma eliminação segura antes de prosseguir. A eliminação segura repõe os atributos de segurança da unidade para uma capacidade segura, mas não ativada para segurança.

> Quando você ativa o recurso Segurança da Unidade e cria um pool ou grupo de volumes a partir de unidades com capacidade segura, as unidades tornam-se *seguras-ativadas*. O acesso de leitura e gravação está disponível somente por meio de um controlador configurado com a chave de segurança correta. Essa segurança adicional impede o acesso não autorizado aos dados em uma unidade que é fisicamente removida do storage array.

#### Número recomendado de unidades hot spare

Se você usou o assistente de configuração inicial para criar automaticamente hot spares, o System Manager cria um hot spare para cada 30 unidades de um tipo de Mídia e tipo de interface específicos. Caso contrário, você pode criar manualmente unidades hot spare entre os grupos de volume no storage de armazenamento.

### Atribua peças sobressalentes quentes

Você pode atribuir um hot spare como uma unidade de reserva para proteção de dados adicional em grupos de volume RAID 1, RAID 5 ou RAID 6. Se uma unidade falhar em um desses grupos de volume, o controlador reconstrói os dados da unidade com falha para o hot spare.

#### Antes de começar

- Os grupos de volumes RAID 1, RAID 5 ou RAID 6 devem ser criados. (As peças sobressalentes quentes não podem ser usadas para piscinas. Em vez disso, um pool usa capacidade extra em cada unidade para sua proteção de dados.)
- Uma unidade que atenda aos seguintes critérios deve estar disponível:

- Não atribuído, com o estado ideal.
- Mesmo tipo de Mídia que as unidades no grupo de volumes (por exemplo, SSDs).
- Mesmo tipo de interface que as unidades no grupo de volumes (por exemplo, SAS).
- Capacidade igual ou superior à capacidade utilizada das unidades no grupo de volumes.

**Sobre esta tarefa**

Esta tarefa descreve como atribuir manualmente um hot spare a partir da página hardware. A cobertura recomendada é de duas peças sobressalentes quentes por conjunto de unidades.

> Os hot spares também podem ser atribuídos a partir do assistente de configuração inicial. Você pode determinar se os hot spares já estão atribuídos procurando por compartimentos de unidade mostrados em rosa na página hardware.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar os controladores, clique na guia **Drives**.

   O gráfico muda para mostrar as unidades em vez dos controladores.

3. Selecione uma unidade não atribuída (mostrada em cinza) que você deseja usar como hot spare.

   O menu de contexto da unidade é aberto.

4. Selecione **Assign hot spare**.

   Se a unidade estiver habilitada para segurança, a caixa de diálogo Apagar Unidade segura? Será aberta. Para usar uma unidade habilitada para segurança como hot spare, você deve primeiro executar uma operação de apagamento seguro para remover todos os seus dados e redefinir seus atributos de segurança.

   > **Possível perda de dados** — Certifique-se de que selecionou a unidade correta. Depois de concluir a operação de apagamento seguro, não é possível recuperar nenhum dos dados.

   Se a unidade estiver ativada para segurança **not**, a caixa de diálogo confirmar atribuição de unidade sobressalente automática será aberta.

5. Revise o texto na caixa de diálogo e confirme a operação.

   A unidade é exibida em rosa na página hardware, o que indica que agora é um hot spare.

**Resultados**

Se uma unidade dentro de um grupo de volumes RAID 1, RAID 5 ou RAID 6 falhar, a controladora usará automaticamente dados de redundância para reconstruir os dados da unidade com falha para o hot spare.

### Anular a atribuição de peças sobressalentes quentes

Você pode alterar um hot spare de volta para uma unidade não atribuída.

**Antes de começar**

O hot spare tem de estar no estado ideal, em espera.

**Sobre esta tarefa**

Não é possível anular a atribuição de um hot spare que esteja atualmente a assumir uma unidade com falha. Se o hot spare não estiver no estado ideal, siga os procedimentos Recovery Guru para corrigir quaisquer problemas antes de tentar anular a atribuição da unidade.

**Passos**

1. Selecione **hardware**.
2. Se o gráfico mostrar os controladores, clique na guia **Drives**.

   O gráfico muda para mostrar as unidades em vez dos controladores.

3. Selecione a unidade hot spare (exibida em rosa) que você deseja cancelar a atribuição.

   Se houver linhas diagonais através do compartimento de unidade rosa, o hot spare está atualmente em uso e não pode ser desatribuído.

   O menu de contexto da unidade é aberto.

4. Na lista suspensa da unidade, selecione **UnAssign hot spare**.

   A caixa de diálogo mostra quaisquer grupos de volume afetados pela remoção deste hot spare e se quaisquer outros hot spares estiverem protegendo-os.

5. Confirme a operação de não atribuição.

**Resultados**

A unidade é retornada para não atribuída (mostrada em cinza).

## Perguntas frequentes sobre prateleiras

### O que é proteção contra perda de prateleira e proteção contra perda de gaveta?

A proteção contra perda de gaveta e a proteção contra perda de gaveta são atributos de pools e grupos de volumes que permitem manter o acesso aos dados em caso de falha de gaveta ou gaveta única.

#### Proteção contra perda de prateleira

Um compartimento é o compartimento que contém as unidades ou as unidades e a controladora. A proteção contra perda de gaveta garante a acessibilidade aos dados nos volumes em um pool ou grupo de volumes se houver perda total de comunicação com um único compartimento de unidade. Um exemplo de perda total de comunicação pode ser perda de energia para o compartimento de unidades ou falha de ambos os módulos de e/S (IOMs).

> A proteção contra perda de gaveta não é garantida se uma unidade já tiver falhado no pool ou grupo de volumes. Nessa situação, a perda de acesso a um compartimento de unidades e, consequentemente, outra unidade no pool ou grupo de volumes causa a perda de dados.

Os critérios para a proteção contra perdas de prateleira dependem do método de proteção, conforme descrito na seguinte tabela:

| Nível | Critérios para proteção contra perdas de prateleira | Número mínimo de gavetas necessário |
| --- | --- | --- |
| Piscina | O pool deve incluir unidades de pelo menos cinco gavetas, e deve haver um número igual de unidades em cada gaveta. A proteção contra perda de prateleira não é aplicável às prateleiras de alta capacidade; se o sistema contiver prateleiras de alta capacidade, consulte proteção contra perda de gaveta. | 5 |
| RAID 6 | O grupo de volumes não contém mais do que duas unidades em uma única gaveta. | 3 |
| RAID 3 ou RAID 5 | Cada unidade no grupo de volume está localizada em uma gaveta separada. | 3 |
| RAID 1 | Cada unidade em um par RAID 1 deve estar localizada em uma gaveta separada. | 2 |
| RAID 0 | Não é possível obter proteção contra perdas de prateleira. | Não aplicável |

#### Proteção contra perda de gaveta

Uma gaveta é um dos compartimentos de uma prateleira que você puxa para fora para acessar as unidades. Apenas as prateleiras de alta capacidade têm gavetas. A proteção contra perda de gaveta garante a acessibilidade aos dados nos volumes em um pool ou grupo de volumes se ocorrer uma perda total de comunicação com uma única gaveta. Um exemplo de perda total de comunicação pode ser perda de energia para a gaveta ou falha de um componente interno dentro da gaveta.

> A proteção contra perda de gaveta não é garantida se uma unidade já tiver falhado no pool ou grupo de volume. Nesta situação, perder o acesso a uma gaveta (e, consequentemente, outra unidade no pool ou grupo de volume) causa perda de dados.

Os critérios para a proteção contra perda de gaveta dependem do método de proteção, conforme descrito na seguinte tabela:

| Nível | Critérios para proteção contra perda de gaveta | Número mínimo de gavetas necessário |
|---|---|---|
| Piscina | Os candidatos ao pool devem incluir unidades de todas as gavetas, e deve haver um número igual de unidades em cada gaveta.<br><br>O pool deve incluir unidades de pelo menos cinco gavetas e deve haver um número igual de unidades em cada gaveta.<br><br>Um compartimento de 60 unidades pode obter proteção contra perda de gaveta quando o pool contém 15, 20, 25, 30, 35, 40, 45, 50, 55 ou 60 unidades. Incrementos em múltiplos de 5 podem ser adicionados ao pool após a criação inicial. | 5 |
| RAID 6 | O grupo de volumes não contém mais do que duas unidades em uma única gaveta. | 3 |
| RAID 3 ou RAID 5 | Cada unidade do grupo de volume está localizada em uma gaveta separada. | 3 |
| RAID 1 | Cada unidade em um par espelhado deve estar localizada em uma gaveta separada. | 2 |
| RAID 0 | Não é possível obter proteção contra perda de gaveta. | Não aplicável |

**O que são ciclos de aprendizagem da bateria?**

Um ciclo de aprendizagem é um ciclo automático para calibrar o indicador inteligente da bateria.

Um ciclo de aprendizagem consiste nestas fases:

- Descarga controlada da bateria
- Período de repouso
- Carregar

As baterias são descarregadas até um limite predeterminado. Durante esta fase, o indicador da bateria é calibrado.

Um ciclo de aprendizagem requer estes parâmetros:

- Baterias totalmente carregadas
- Sem pilhas sobreaquecidas

Os ciclos de aprendizagem para sistemas de controlador duplex ocorrem simultaneamente. Para controladores com alimentação de backup de mais de uma bateria ou conjunto de células de bateria, os ciclos de aprendizagem ocorrem sequencialmente.

Os ciclos de aprendizagem são programados para iniciar automaticamente em intervalos regulares, ao mesmo tempo e no mesmo dia da semana. O intervalo entre os ciclos é descrito em semanas.

Um ciclo de aprendizagem pode levar várias horas para ser concluído.

## Perguntas frequentes sobre o controlador

### O que é auto-negociação?

Auto-negociação é a capacidade de uma interface de rede coordenar automaticamente seus próprios parâmetros de conexão (velocidade e duplex) com outra interface de rede.

A negociação automática é geralmente a configuração preferida para configurar portas de gerenciamento; no entanto, se a negociação falhar, as configurações de interface de rede incompatíveis podem afetar gravemente o desempenho da rede. Nos casos em que essa condição é inaceitável, você deve definir manualmente as configurações da interface de rede para uma configuração correta. A negociação automática é realizada pelas portas de gerenciamento Ethernet do controlador. A negociação automática não é realizada por adaptadores de barramento de host iSCSI.

Se a negociação automática falhar, o controlador tentará estabelecer uma conexão em 10BASEBASE-T, half-duplex, que é o menor denominador comum.

### O que é a auto-configuração de endereço sem estado IPv6?

Com a configuração automática sem estado, os hosts não obtêm endereços e outras informações de configuração de um servidor.

A configuração automática sem estado no IPv6 apresenta endereços locais de ligação, multicast e o protocolo Neighbor Discovery (ND). O IPv6 pode gerar o ID da interface de um endereço a partir do endereço da camada de enlace de dados subjacente.

A configuração automática sem estado e a configuração automática com estado complementam-se. Por exemplo, o host pode usar a configuração automática sem estado para configurar seus próprios endereços, mas usar a configuração automática com estado para obter outras informações. A configuração automática com estado permite que os hosts obtenham endereços e outras informações de configuração de um servidor. O Internet Protocol versão 6 (IPv6) também define um método pelo qual todos os endereços IP de uma rede podem ser renumerados de uma só vez. IPv6 define um método para que os dispositivos na rede configurem automaticamente seu endereço IP e outros parâmetros sem a necessidade de um servidor.

Os dispositivos executam estas etapas ao usar a configuração automática sem monitoração de estado:

1. **Generate a link-local address** — o dispositivo gera um endereço link-local, que tem 10 bits, seguido de 54 zeros, e seguido pelo ID de interface de 64 bits.

2. **Teste a singularidade de um endereço local de link** — o nó testa para se certificar de que o endereço local de link que ele gera ainda não está em uso na rede local. O nó envia uma mensagem de solicitação de vizinho usando o protocolo ND. Em resposta, a rede local escuta uma mensagem de anúncio vizinho, que indica que outro dispositivo já está usando o endereço local de link. Em caso afirmativo, um novo endereço local de link deve ser gerado ou falha de configuração automática, e outro método deve ser usado.
3. * Atribuir um endereço local de link* — se o dispositivo passar no teste de exclusividade, o dispositivo atribui o endereço local de link à sua interface IP. O endereço local do link pode ser usado para comunicação na rede local, mas não pela Internet.
4. **Contate o roteador** — o nó tenta entrar em Contato com um roteador local para obter mais informações sobre como continuar a configuração. Esse Contato é realizado ouvindo mensagens de anúncio do roteador enviadas periodicamente pelos roteadores ou enviando uma mensagem específica de solicitação do roteador para pedir informações a um roteador sobre o que fazer a seguir.
5. **Forneça direção para o nó** — o roteador fornece direção para o nó sobre como proceder com a configuração automática. Como alternativa, o roteador informa ao host como determinar o endereço global da Internet.
6. **Configure o endereço global** — o host se configura com seu endereço de Internet exclusivo globalmente. Esse endereço geralmente é formado a partir de um prefixo de rede fornecido ao host pelo roteador.

#### O que eu escolho - DHCP ou configuração manual?

O método predefinido para a configuração da rede é o DHCP (Dynamic Host Configuration Protocol). Utilize sempre esta opção, a menos que a rede não tenha um servidor DHCP.

#### O que é um servidor DHCP?

O DHCP (Dynamic Host Configuration Protocol) é um protocolo que automatiza a tarefa de atribuir um endereço IP (Internet Protocol).

Cada dispositivo conetado a uma rede TCP/IP deve ser atribuído um endereço IP exclusivo. Esses dispositivos incluem os controladores em sua matriz de armazenamento.

Sem DHCP, um administrador de rede insere esses endereços IP manualmente. Com o DHCP, quando um cliente precisa iniciar operações TCP/IP, o cliente transmite uma solicitação de informações de endereço. O servidor DHCP recebe a solicitação, atribui um novo endereço por um período de tempo especificado chamado período de concessão e envia o endereço ao cliente. Com o DHCP, um dispositivo pode ter um endereço IP diferente sempre que se conetar à rede. Em alguns sistemas, o endereço IP do dispositivo pode mudar mesmo quando o dispositivo ainda está conetado.

#### Como configuro meu servidor DHCP?

Você deve configurar um servidor DHCP (Dynamic Host Configuration Protocol) para usar endereços IP (Static Internet Protocol) para os controladores em sua matriz de armazenamento.

Os endereços IP atribuídos pelo servidor DHCP são geralmente dinâmicos e podem ser alterados porque têm um período de concessão que expira. Alguns dispositivos, por exemplo, servidores e roteadores, precisam usar endereços estáticos. Os controladores em seu storage array também precisam de endereços IP estáticos.

Para obter informações sobre como atribuir endereços estáticos, consulte a documentação do servidor DHCP.

**Por que eu preciso alterar a configuração da rede do controlador?**

Você deve definir a configuração de rede para cada controlador - seu endereço IP (Internet Protocol), máscara de sub-rede (máscara de sub-rede) e gateway - quando você usa o gerenciamento fora da banda.

Pode definir a configuração de rede utilizando um servidor DHCP (Dynamic Host Configuration Protocol). Se não estiver a utilizar um servidor DHCP, tem de introduzir manualmente a configuração da rede.

**Onde obtenho a configuração de rede?**

Você pode obter o endereço IP (Internet Protocol), a máscara de sub-rede (máscara de sub-rede) e as informações de gateway do administrador da rede.

Você precisa dessas informações quando estiver configurando portas nos controladores.

**O que são respostas ICMP PING?**

O ICMP (Internet Control Message Protocol) é um dos protocolos do conjunto TCP/IP.

As `ICMP echo request` mensagens e(`ICMP echo reply` são comumente conhecidas como `ping` mensagens. `Ping` é uma ferramenta de solução de problemas usada pelos administradores de sistema para testar manualmente a conetividade entre dispositivos de rede e também para testar o atraso da rede e a perda de pacotes. O `ping` comando envia um `ICMP echo request` para um dispositivo na rede e o dispositivo responde imediatamente com um(`ICMP echo reply`. às vezes, a diretiva de segurança de rede de uma empresa exige `ping` (`ICMP echo reply`que o ) seja desativado em todos os dispositivos para torná-los mais difíceis de serem descobertos por pessoas não autorizadas.

**Quando devo atualizar a configuração da porta ou o servidor iSNS a partir do servidor DHCP?**

Atualize o servidor DHCP sempre que o servidor for modificado ou atualizado, e as informações DHCP relevantes para a matriz de armazenamento atual e a matriz de armazenamento que você deseja usar foram alteradas.

Especificamente, atualize a configuração da porta ou o servidor iSNS do servidor DHCP quando souber que o servidor DHCP atribuirá endereços diferentes.

Atualizar uma configuração de porta é destrutivo para todas as conexões iSCSI nessa porta.

**O que devo fazer depois de configurar as portas de gerenciamento?**

Se você tiver alterado o endereço IP da matriz de armazenamento, talvez queira atualizar a exibição global do array no Unified Manager.

Para atualizar a exibição de matriz global no Unified Manager, abra a interface e vá para **Gerenciar › Discover**.

Se você ainda estiver usando o SANtricity Storage Manager, vá para a janela Gerenciamento Empresarial (EMW), onde você deve remover e adicionar novamente o novo endereço IP.

#### Por que o sistema de armazenamento está no modo não ideal?

Um sistema de armazenamento em modo não otimizado deve-se a um estado de Configuração do sistema inválido. Apesar desse estado, o acesso normal de e/S aos volumes existentes é totalmente suportado; no entanto, o System Manager proibirá algumas operações.

Um sistema de armazenamento pode ser transferido para Configuração de sistema inválida por um destes motivos:

- O controlador está fora de conformidade, possivelmente porque tem um código de ID de submodelo (SMID) incorreto ou excedeu o limite de recursos premium.
- Uma operação de serviço interno está em andamento, como um download do firmware da unidade.
- O controlador excedeu o limite de erro de paridade e entrou em bloqueio.
- Ocorreu uma condição geral de bloqueio.

## Perguntas frequentes sobre iSCSI

#### O que acontece quando utilizo um servidor iSNS para registo?

Quando as informações do servidor iSNS (Internet Storage Name Service) são usadas, os hosts (iniciadores) podem ser configurados para consultar o servidor iSNS para recuperar informações do destino (controladores).

Este registo fornece ao servidor iSNS o nome qualificado iSCSI (IQN) e as informações da porta do controlador e permite consultas entre os iniciadores (hosts iSCSI) e os destinos (controladores).

#### Que métodos de registo são suportados automaticamente para iSCSI?

A implementação iSCSI suporta o método de deteção iSNS (Internet Storage Name Service) ou o uso do comando Enviar destinos.

O método iSNS permite a descoberta do iSNS entre os iniciadores (hosts iSCSI) e os destinos (os controladores). Você Registra o controlador de destino para fornecer ao servidor iSNS o nome qualificado iSCSI (IQN) e as informações de porta do controlador.

Se você não configurar o iSNS, o host iSCSI poderá enviar o comando Enviar destinos durante uma sessão de descoberta iSCSI. Em resposta, o controlador retorna as informações da porta (por exemplo, IQN de destino, endereço IP da porta, porta de escuta e Grupo de portas de destino). Esse método de descoberta não é necessário se você usar o iSNS, porque o iniciador do host pode recuperar os IPs de destino do servidor iSNS.

#### Como faço para interpretar estatísticas iSER over InfiniBand?

A caixa de diálogo View iSER over InfiniBand Statistics exibe estatísticas de destino local (protocolo) e estatísticas de interface iSER over InfiniBand (IB). Todas as estatísticas são apenas de leitura e não podem ser definidas.

- **Estatísticas locais de destino (protocolo)** — fornece estatísticas para o destino iSER over InfiniBand, que mostra acesso em nível de bloco a sua Mídia de storage.

- **ISER over InfiniBand Interface statistics** — fornece estatísticas para todas as portas iSER over InfiniBand na interface InfiniBand, que inclui estatísticas de desempenho e informações de erro de link associadas a cada porta do switch.

Você pode visualizar cada uma dessas estatísticas como estatísticas em bruto ou como estatísticas de linha de base. As estatísticas em bruto são todas as estatísticas que foram coletadas desde que os controladores foram iniciados. As estatísticas da linha de base são estatísticas pontuais que foram reunidas desde que você definiu o tempo da linha de base.

#### O que mais preciso fazer para configurar ou diagnosticar iSER em InfiniBand?

A tabela a seguir lista as funções do System Manager que podem ser usadas para configurar e gerenciar sessões iSER over InfiniBand.

As configurações iSER over InfiniBand estarão disponíveis somente se a controladora do storage array incluir uma porta de gerenciamento de host iSER over InfiniBand.

| Ação | Localização |
|---|---|
| Configurar o iSER em portas InfiniBand | 1. Selecione **hardware**.<br>2. Selecione a guia **Controllers & Components** (Controladores e componentes).<br>3. Selecione um controlador.<br>4. Selecione **Configure iSER over InfiniBand Ports**.<br><br>ou<br><br>1. Selecione **Definições › sistema**.<br>2. Role para baixo até **iSER over InfiniBand settings** e selecione **Configure iSER over InfiniBand ports**. |
| Visualizar estatísticas do iSER em InfiniBand | 1. Selecione **Definições › sistema**.<br>2. Role para baixo até **iSER over InfiniBand settings** e selecione **View iSER over InfiniBand Statistics**. |

#### O que mais preciso fazer para configurar ou diagnosticar iSCSI?

Sessões iSCSI podem ocorrer com hosts ou matrizes de armazenamento remoto em uma relação de espelhamento assíncrono. As tabelas a seguir listam as funções do System Manager que podem ser usadas para configurar e gerenciar essas sessões iSCSI.

As definições iSCSI só estão disponíveis se a sua matriz de armazenamento suportar iSCSI.

##### Configurar iSCSI

| Ação | Localização |
| --- | --- |
| Gerir as definições iSCSI | 1. Selecione **Definições › sistema**.<br>2. Role para baixo até **iSCSI settings** para visualizar todas as funções de gerenciamento. |
| Configurar portas iSCSI | 1. Selecione **hardware**.<br>2. Selecione a guia **Controllers & Components** (Controladores e componentes).<br>3. Selecione um controlador.<br>4. Selecione **Configurar portas iSCSI**. |
| Defina o segredo CHAP host | 1. Selecione **Definições › sistema**.<br>2. Role para baixo até **iSCSI settings** e selecione **Configure Authentication**.<br>ou<br>1. Selecione **armazenamento › hosts**.<br>2. Selecione um membro anfitrião.<br>3. Clique no **Exibir/Editar Configurações › Host Ports** guia. |

#### Diagnosticar iSCSI

| Ação | Localização |
| --- | --- |
| Visualizar ou terminar sessões iSCSI | 1. Selecione **Definições › sistema**.<br>2. Role para baixo até **iSCSI settings** e selecione **View/End iSCSI Sessions**.<br>ou<br>1. Selecione menu:guia Support [Support Center > Diagnostics] (suporte > Centro de suporte > Diagnóstico).<br>2. Selecione **View/End iSCSI Sessions** (Ver/terminar sessões iSCSI). |

| Ação | Localização |
| --- | --- |
| Ver estatísticas iSCSI | 1. Selecione **Definições › sistema**.<br>2. Role para baixo até **iSCSI settings** e selecione **View iSCSI Statistics Packages**.<br><br>ou<br><br>1. Selecione menu:guia Support [Support Center > Diagnostics] (suporte > Centro de suporte > Diagnóstico).<br>2. Selecione **Ver Pacotes de Estatísticas iSCSI**. |

## Perguntas frequentes sobre NVMe

**Como interpretar as estatísticas do NVMe sobre Fabrics?**

A caixa de diálogo View NVMe over Fabrics Statistics exibe estatísticas do subsistema NVMe e da interface RDMA. Todas as estatísticas são apenas de leitura e não podem ser definidas.

- **Estatísticas do subsistema NVMe** — mostra estatísticas para o controlador NVMe e sua fila. O controlador NVMe fornece um caminho de acesso entre um host e os namespaces no storage array. Você pode revisar as estatísticas do subsistema NVMe para itens como falhas de conexão, reconfigurações e paradas. Para obter mais informações sobre essas estatísticas, clique em **Exibir legenda para títulos de tabela**.
- **Estatísticas da interface RDMA** — fornece estatísticas para todas as portas NVMe sobre Fabrics na interface RDMA, que inclui estatísticas de desempenho e informações de erro de link associadas a cada porta do switch. Essa guia só aparece quando as portas NVMe sobre Fabrics estiverem disponíveis. Para obter mais informações sobre as estatísticas, clique em **Exibir legenda para títulos de tabela**.

Você pode visualizar cada uma dessas estatísticas como estatísticas em bruto ou como estatísticas de linha de base. As estatísticas em bruto são todas as estatísticas que foram coletadas desde que os controladores foram iniciados. As estatísticas da linha de base são estatísticas pontuais que foram reunidas desde que você definiu o tempo da linha de base.

**O que mais preciso fazer para configurar ou diagnosticar o NVMe em InfiniBand?**

A tabela a seguir lista as funções do System Manager que você pode usar para configurar e gerenciar sessões NVMe over InfiniBand.

> As configurações NVMe over InfiniBand estarão disponíveis somente se a controladora do storage array incluir uma porta NVMe over InfiniBand.

| Ação | Localização |
| --- | --- |
| Configurar portas NVMe em InfiniBand | 1. Selecione **hardware**.<br>2. Selecione a guia **Controllers & Components** (Controladores e componentes).<br>3. Selecione um controlador.<br>4. Selecione **Configurar portas NVMe over InfiniBand**.<br>ou<br>1. Selecione **Definições › sistema**.<br>2. Role para baixo até **NVMe over InfiniBand settings** e selecione **Configurar portas NVMe over InfiniBand**. |
| Visualizar estatísticas do NVMe em InfiniBand | 1. Selecione **Definições › sistema**.<br>2. Role para baixo até **NVMe over InfiniBand settings** e selecione **View NVMe over Fabrics Statistics**. |

**O que mais preciso fazer para configurar ou diagnosticar o NVMe em RoCE?**

Você pode configurar e gerenciar o NVMe sobre RoCE nas páginas hardware e Configurações.

As configurações NVMe em RoCE só estarão disponíveis se a controladora do storage array incluir uma porta NVMe em RoCE.

| Ação | Localização |
| --- | --- |
| Configurar o NVMe em portas RoCE | 1. Selecione **hardware**.<br>2. Selecione a guia **Controllers & Components** (Controladores e componentes).<br>3. Selecione um controlador.<br>4. Selecione **Configure NVMe over RoCE ports**.<br>ou<br>1. Selecione **Definições › sistema**.<br>2. Role para baixo até **NVMe over RoCE settings** e selecione **Configure NVMe over RoCE ports**. |
| Veja as estatísticas do NVMe sobre Fabrics | 1. Selecione **Definições › sistema**.<br>2. Role para baixo até **NVMe over RoCE settings** e selecione **View NVMe over Fabrics Statistics**. |

#### Por que há dois endereços IP para uma porta física?

A matriz de armazenamento EF600 pode incluir dois HICs - um externo e um interno.

Nesta configuração, o HIC externo está ligado a um HIC interno auxiliar. Cada porta física que você pode acessar do HIC externo tem uma porta virtual associada do HIC interno.

Para obter o máximo desempenho de 200GB GbE, você deve atribuir um endereço IP exclusivo para as portas físicas e virtuais para que o host possa estabelecer conexões com cada uma. Se você não atribuir um endereço IP à porta virtual, o HIC será executado a aproximadamente metade de sua velocidade capaz.

#### Por que existem dois conjuntos de parâmetros para uma porta física?

A matriz de armazenamento EF600 pode incluir dois HICs - um externo e um interno.

Nesta configuração, o HIC externo está ligado a um HIC interno auxiliar. Cada porta física que você pode acessar do HIC externo tem uma porta virtual associada do HIC interno.

Para alcançar o máximo de desempenho 200GB, você deve atribuir parâmetros para as portas físicas e virtuais para que o host possa estabelecer conexões com cada uma. Se você não atribuir parâmetros à porta virtual, o HIC será executado a aproximadamente metade de sua velocidade capaz.

## Perguntas frequentes sobre a condução

#### O que é uma unidade de reserva quente?

As peças sobressalentes ativas funcionam como unidades de reserva nos grupos de volumes RAID 1, RAID 5 ou RAID 6. São unidades totalmente funcionais que não contêm dados. Se uma unidade falhar no grupo de volumes, o controlador reconstrói automaticamente os dados da unidade com falha para um hot spare.

Se uma unidade falhar no storage de armazenamento, a unidade hot spare será automaticamente substituída pela unidade com falha sem exigir uma troca física. Se a unidade hot spare estiver disponível quando uma unidade falhar, a controladora usará dados de redundância para reconstruir os dados da unidade com falha para a unidade hot spare.

Uma unidade hot spare não é dedicada a um grupo de volume específico. Em vez disso, você pode usar uma unidade hot spare para qualquer unidade com falha no storage de armazenamento com a mesma capacidade ou capacidade menor. Uma unidade hot spare deve ser do mesmo tipo de Mídia (HDD ou SSD) que as unidades que está protegendo.

> Unidades hot spare não são suportadas com pools. Em vez de unidades hot spare, os pools usam a capacidade de preservação dentro de cada unidade que compreende o pool.

#### O que é a capacidade de preservação?

Capacidade de preservação é a quantidade de capacidade (número de unidades) reservada em um pool para dar suporte a possíveis falhas de unidade.

Quando um pool é criado, o sistema reserva automaticamente uma quantidade padrão de capacidade de preservação, dependendo do número de unidades no pool.

Os pools usam capacidade de preservação durante a reconstrução, enquanto os grupos de volume usam unidades hot spare para o mesmo propósito. O método de capacidade de preservação é uma melhoria em relação às unidades hot spare porque permite que a reconstrução aconteça mais rapidamente. A capacidade de preservação é espalhada por várias unidades no pool em vez de em uma unidade no caso de uma unidade hot spare, portanto, você não está limitado pela velocidade ou disponibilidade de uma unidade.

#### Por que eu substituiria logicamente uma unidade?

Se uma unidade falhar ou você quiser substituí-la por qualquer outro motivo, e você tiver uma unidade não atribuída em sua matriz de armazenamento, você pode logicamente substituir a unidade com falha pela unidade não atribuída. Se você não tiver uma unidade não atribuída, pode substituir fisicamente a unidade.

Os dados da unidade original são copiados ou reconstruídos na unidade de substituição.

#### Onde posso ver o estado de uma unidade em fase de reconstrução?

Pode visualizar o estado de reconstrução da unidade a partir do painel operações em curso.

Na página inicial, clique no link **Exibir operações em andamento** no canto superior direito.

Dependendo da unidade, a reconstrução completa pode demorar um tempo considerável. Se a propriedade de um volume tiver mudado, poderá ocorrer uma reconstrução completa em vez da reconstrução rápida.

# Alertas

## Visão geral dos alertas

Você pode configurar o System Manager para enviar alertas de storage array por e-mail, traps SNMP e mensagens syslog.

#### O que são alertas?

*Alertas* notificar os administradores sobre eventos importantes que ocorrem no storage array. Os eventos podem incluir problemas como uma falha da bateria, um componente que se move do ideal para o Offline ou erros de redundância no controlador. Todos os eventos críticos são considerados "alertable", juntamente com alguns eventos de aviso e informação.

Saiba mais:

- "Como os alertas funcionam"
- "Terminologia de alertas"

#### Como faço para configurar alertas?

Você pode configurar alertas para serem enviados como uma mensagem para um ou mais endereços de e-mail, como uma intercetação SNMP para um servidor SNMP ou como uma mensagem para um servidor syslog. A configuração de alerta está disponível no **Configurações › Alertas**.

Saiba mais:

- "Configure o servidor de e-mail e os destinatários para alertas"
- "Configure o servidor syslog para alertas"
- "Configurar alertas SNMP"

### Informações relacionadas

Saiba mais sobre conceitos relacionados a alertas:

- "Visão geral do log de eventos"
- "Carimbos de hora inconsistentes"

## Conceitos

### Como os alertas funcionam

Os alertas notificam os administradores sobre eventos importantes que ocorrem no storage array. Os alertas podem ser enviados por e-mail, traps SNMP e syslog.

O processo de alertas funciona da seguinte forma:

1. Um administrador configura um ou mais dos seguintes métodos de alerta no System Manager:
   - **Email** — as mensagens são enviadas para endereços de e-mail.
   - **SNMP** — traps SNMP são enviados para um servidor SNMP.
   - **Syslog** — as mensagens são enviadas para um servidor syslog.
2. Quando o monitor de eventos do storage deteta um problema, ele grava informações sobre esse problema no log de eventos (disponível no **suporte › Log de eventos**). Por exemplo, os problemas podem incluir eventos como uma falha de bateria, um componente que se move do Optimal para o Offline ou erros de redundância no controlador.
3. Se o monitor de eventos determinar que o evento é "alertable", ele então envia uma notificação usando os métodos de alerta configurados (e-mail, SNMP e/ou syslog). Todos os eventos críticos são considerados "alertable", juntamente com alguns eventos de aviso e informação.

#### Configuração de alertas

Pode configurar alertas a partir do assistente de configuração inicial (apenas para alertas de e-mail) ou da página Alertas. Para verificar a configuração atual, vá para **Configurações › Alertas**.

O bloco Alertas exibe a configuração de alertas, que pode ser uma das seguintes opções:

- Não configurado.
- Configurado; pelo menos um método de alerta está configurado. Para determinar quais métodos de alerta estão configurados, aponte o cursor para o mosaico.

#### Informações de alertas

Os alertas podem incluir os seguintes tipos de informações:

- Nome do storage array.
- Tipo de erro de evento relacionado a uma entrada de log de eventos.

- Data e hora em que o evento ocorreu.
- Breve descrição do evento.

Os alertas de syslog seguem o padrão de mensagens RFC 5424.

**Terminologia de alertas**

Saiba como os termos de alertas se aplicam ao storage array.

| Componente | Descrição |
|---|---|
| Monitor de eventos | O monitor de eventos reside no storage array e é executado como uma tarefa em segundo plano. Quando o monitor de eventos deteta anomalias no storage array, ele grava informações sobre os problemas no log de eventos. Os problemas podem incluir eventos como uma falha da bateria, um componente que se move do ideal para o Offline ou erros de redundância no controlador. Se o monitor de eventos determinar que o evento é "alertable", ele então envia uma notificação usando os métodos de alerta configurados (e-mail, SNMP e/ou syslog). Todos os eventos críticos são considerados "alertable", juntamente com alguns eventos de aviso e informação. |
| Servidor de correio | O servidor de e-mail é usado para enviar e receber alertas de e-mail. O servidor utiliza o Simple Mail Transfer Protocol (SMTP). |
| SNMP | O SNMP (Simple Network Management Protocol) é um protocolo padrão da Internet usado para gerenciar e compartilhar informações entre dispositivos em redes IP. |
| Trap SNMP | Uma armadilha SNMP é uma notificação enviada para um servidor SNMP. A armadilha contém informações sobre problemas significativos com o storage array. |
| Destino de trap SNMP | Um destino de trap SNMP é um endereço IPv4 ou IPv6 do servidor que executa um serviço SNMP. |
| Nome da comunidade | Um nome de comunidade é uma cadeia de carateres que atua como uma senha para o(s) servidor(es) de rede em um ambiente SNMP. |
| Ficheiro MIB | O arquivo de base de informações de gerenciamento (MIB) define os dados que estão sendo monitorados e gerenciados no storage array. Ele deve ser copiado e compilado no servidor com o aplicativo de serviço SNMP. Este arquivo MIB está disponível com o software System Manager no site de suporte. |
| Variáveis MIB | As variáveis do Management Information base (MIB) podem retornar valores como o nome do storage array, localização do array e uma pessoa de Contato em resposta ao SNMP GetRequest. |
| Syslog | Syslog é um protocolo usado por dispositivos de rede para enviar mensagens de eventos para um servidor de log. |

| Componente | Descrição |
| --- | --- |
| UDP | O User Datagram Protocol (UDP) é um protocolo da camada de transporte que especifica um número de porta de origem e destino em seus cabeçalhos de pacotes. |

## Gerenciar alertas de e-mail

### Configure o servidor de e-mail e os destinatários para alertas

Para configurar alertas de e-mail, você deve especificar um endereço de servidor de e-mail e os endereços de e-mail dos destinatários do alerta. São permitidos até 20 endereços de correio eletrónico.

#### Antes de começar

- O endereço do servidor de e-mail deve estar disponível. O endereço pode ser um endereço IPv4 ou IPv6, ou um nome de domínio totalmente qualificado.

> Para usar um nome de domínio totalmente qualificado, você deve configurar um servidor DNS em ambos os controladores. Pode configurar um servidor DNS a partir da página hardware.

- O endereço de e-mail a ser usado como remetente de alerta deve estar disponível. Este é o endereço que aparece no campo "de" da mensagem de alerta. Um endereço de remetente é necessário no protocolo SMTP; sem ele, um erro resulta.
- O(s) endereço(s) de e-mail do(s) destinatário(s) alerta(s) deve(m) estar disponível(s) Normalmente, o destinatário é um endereço para um administrador de rede ou administrador de armazenamento. Pode introduzir até 20 endereços de correio eletrónico.

#### Sobre esta tarefa

Esta tarefa descreve como configurar o servidor de e-mail, inserir endereços de e-mail para o remetente e destinatários e testar todos os endereços de e-mail inseridos na página Alertas.

> Os alertas de e-mail também podem ser configurados a partir do assistente de configuração inicial.

#### Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Email**.

   Se um servidor de e-mail ainda não estiver configurado, a guia e-mail exibirá "Configurar servidor de e-mail".

3. Selecione **Configure Mail Server**.

   A caixa de diálogo Configurar servidor de correio abre-se.

4. Insira as informações do servidor de e-mail e clique em **Salvar**.
   - **Endereço do servidor de correio** — Insira um nome de domínio totalmente qualificado, endereço IPv4 ou endereço IPv6 do servidor de correio.

Para usar um nome de domínio totalmente qualificado, você deve configurar um servidor DNS em ambos os controladores. Pode configurar um servidor DNS a partir da página hardware.

- **Endereço do remetente de e-mail** — Digite um endereço de e-mail válido para ser usado como remetente do e-mail. Este endereço é exibido no campo "de" da mensagem de e-mail.
- **Criptografia** — se você quiser criptografar mensagens, selecione **SMTPS** ou **STARTTLS** para o tipo de criptografia e, em seguida, selecione o número da porta para mensagens criptografadas. Caso contrário, selecione **nenhum**.
- **Nome de usuário e senha** — se necessário, insira um nome de usuário e senha para autenticação com o remetente de saída e o servidor de e-mail.
- **Inclua informações de Contato no e-mail** — para incluir as informações de Contato do remetente com a mensagem de alerta, selecione esta opção e insira um nome e número de telefone.

  Depois de clicar em **Salvar**, os endereços de e-mail aparecem na guia e-mail da página Alertas.

5. Selecione **Adicionar e-mails**.

   A caixa de diálogo Adicionar e-mails é aberta.

6. Insira um ou mais endereços de e-mail para os destinatários do alerta e clique em **Adicionar**.

   Os endereços de e-mail aparecem na página Alertas.

7. Se você quiser garantir que os endereços de e-mail sejam válidos, clique em **testar todos os e-mails** para enviar mensagens de teste aos destinatários.

**Resultados**

Depois de configurar alertas por e-mail, o monitor de eventos envia mensagens de e-mail para os destinatários especificados sempre que ocorre um evento alertable.

### Editar endereços de e-mail para alertas

Você pode alterar os endereços de e-mail dos destinatários que recebem alertas de e-mail.

**Antes de começar**

O endereço de e-mail que você pretende editar deve ser definido na guia e-mail da página Alertas.

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Email**.
3. Na tabela **Endereço de e-mail**, selecione o endereço que deseja alterar e clique no ícone **Editar** (lápis) na extrema direita.

   A linha se torna um campo editável.

4. Insira um novo endereço e clique no ícone **Salvar** (marca de seleção).

   Se pretender cancelar as alterações, selecione o ícone **Cancelar** (X).

**Resultados**

A guia e-mail da página Alertas exibe os endereços de e-mail atualizados.

### Adicionar endereços de e-mail para alertas

Você pode adicionar até 20 destinatários para alertas de e-mail.

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Email**.
3. Selecione **Adicionar e-mails**.

   A caixa de diálogo Adicionar e-mails é aberta.

4. No campo vazio, insira um novo endereço de e-mail. Se quiser adicionar mais de um endereço, selecione **Adicionar outro email** para abrir outro campo.
5. Clique em **Add**.

**Resultados**

A guia e-mail da página Alertas exibe os novos endereços de e-mail.

### Excluir servidor de e-mail ou endereços de e-mail para alertas

Você pode remover o servidor de e-mail definido anteriormente para que os alertas não sejam mais enviados para os endereços de e-mail ou remover endereços de e-mail individuais.

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Email**.
3. Na tabela, execute um dos seguintes procedimentos:
   - Para remover um servidor de e-mail para que os alertas não sejam mais enviados para os endereços de e-mail, selecione a linha para o servidor de e-mail.
   - Para remover um endereço de e-mail para que os alertas não sejam mais enviados para esse endereço, selecione a linha do endereço de e-mail que deseja excluir. O botão **Delete** no canto superior direito da tabela fica disponível para seleção.
4. Clique em **Delete** e confirme a operação.

### Edite o servidor de e-mail para alertas

Você pode alterar o endereço do servidor de e-mail e o endereço do remetente usado para alertas de e-mail.

**Antes de começar**

O endereço do servidor de correio que está a alterar tem de estar disponível. O endereço pode ser um endereço IPv4 ou IPv6, ou um nome de domínio totalmente qualificado.

Para usar um nome de domínio totalmente qualificado, você deve configurar um servidor DNS em ambos os controladores. Pode configurar um servidor DNS a partir da página hardware.

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Email**.
3. Selecione **Configure Mail Server**.

   A caixa de diálogo Configurar servidor de correio abre-se.

4. Edite o endereço do servidor de correio, as informações do remetente e as informações de contacto.
   - **Endereço do servidor de correio** — edite o nome de domínio totalmente qualificado, endereço IPv4 ou endereço IPv6 do servidor de correio.

     Para usar um nome de domínio totalmente qualificado, você deve configurar um servidor DNS em ambos os controladores. Pode configurar um servidor DNS a partir da página hardware.

   - **Endereço do remetente de e-mail** — edite o endereço de e-mail a ser usado como remetente do e-mail. Este endereço é exibido no campo "de" da mensagem de e-mail.
   - **Inclua informações de Contato no e-mail** — para editar as informações de Contato do remetente, selecione esta opção e edite o nome e o número de telefone.
5. Clique em **Salvar**.

## Gerenciar alertas SNMP

### Configurar alertas SNMP

Para configurar alertas SNMP (Simple Network Management Protocol), você deve identificar pelo menos um servidor onde o monitor de eventos da matriz de armazenamento pode enviar traps SNMP. A configuração requer um nome de comunidade ou um nome de usuário e um endereço IP para o servidor.

**Antes de começar**

- Um servidor de rede deve ser configurado com um aplicativo de serviço SNMP. Você precisa do endereço de rede deste servidor (um endereço IPv4 ou IPv6), para que o monitor de eventos possa enviar mensagens de intercetação para esse endereço. Você pode usar mais de um servidor (até 10 servidores são permitidos).
- O arquivo de base de informações de gerenciamento (MIB) foi copiado e compilado no servidor com o aplicativo de serviço SNMP. Este arquivo MIB define os dados que estão sendo monitorados e gerenciados.

  Se você não tiver o arquivo MIB, poderá obtê-lo no site de suporte da NetApp:

  - Vá para "Suporte à NetApp".
  - Clique na guia **Downloads** e selecione **Downloads**.
  - Clique em **e-Series SANtricity os Controller Software**.

- Selecione **Download Latest Release**.
- Inicie sessão.
- Aceite a declaração de precaução e o contrato de licença.
- Role para baixo até ver o arquivo MIB para o tipo de controlador e clique no link para fazer o download do arquivo.

**Sobre esta tarefa**

Esta tarefa descreve como identificar o servidor SNMP para destinos de intercetação e, em seguida, testar sua configuração.

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

   Na primeira configuração, a guia SNMP exibe "Configurar Comunidades/usuários".

3. Selecione **Configurar Comunidades/usuários**.

   Abre-se a caixa de diálogo Selecionar versão SNMP.

4. Selecione a versão SNMP para os alertas, **SNMPv2c** ou **SNMPv3**.

   Dependendo da seleção, a caixa de diálogo Configurar Comunidades ou a caixa de diálogo Configurar usuários SNMPv3 será aberta.

5. Siga as instruções apropriadas para SNMPv2c (comunidades) ou SNMPv3 (usuários):
   - **SNMPv2c (comunidades)** — na caixa de diálogo Configurar Comunidades, insira uma ou mais strings de comunidade para os servidores de rede. Um nome de comunidade é uma cadeia de carateres que identifica um conjunto conhecido de estações de gerenciamento e é normalmente criado por um administrador de rede. Consiste apenas em carateres ASCII imprimíveis. Você pode adicionar até 256 comunidades. Quando terminar, clique em **Guardar**.
   - **SNMPv3 (usuários)** — na caixa de diálogo Configurar SNMPv3 usuários, clique em **Adicionar** e insira as seguintes informações:
     - **Nome do usuário** — Digite um nome para identificar o usuário, que pode ter até 31 carateres.
     - **Engine ID** — Selecione o Engine ID, que é usado para gerar chaves de autenticação e criptografia para mensagens, e deve ser exclusivo no domínio administrativo. Na maioria dos casos, você deve selecionar **local**. Se você tiver uma configuração não padrão, selecione **Custom**; outro campo aparece onde você deve inserir o ID do mecanismo autorizado como uma cadeia hexadecimal, com um número par de carateres entre 10 e 32 carateres.
     - **Credenciais de autenticação** — Selecione um protocolo de autenticação, que garante a identidade dos usuários. Em seguida, introduza uma palavra-passe de autenticação, que é necessária quando o protocolo de autenticação é definido ou alterado. A senha deve ter entre 8 e 128 carateres.
     - **Credenciais de privacidade** — Selecione um protocolo de privacidade, que é usado para criptografar o conteúdo das mensagens. Em seguida, introduza uma palavra-passe de privacidade, que é necessária quando o protocolo de privacidade é definido ou alterado. A senha deve ter entre 8 e 128 carateres. Quando terminar, clique em **Adicionar** e, em seguida, clique em **Fechar**.
6. Na página Alertas com a guia SNMP selecionada, clique em **Adicionar destinos de armadilha**.

A caixa de diálogo Adicionar destinos de armadilha é aberta.

7. Insira um ou mais destinos de armadilha, selecione seus nomes de comunidade ou de usuário associados e clique em **Adicionar**.
   - **Trap Destination** — Digite um endereço IPv4 ou IPv6 do servidor executando um serviço SNMP.
   - **Nome da comunidade ou Nome do usuário** — na lista suspensa, selecione o nome da comunidade (SNMPv2c) ou nome de usuário (SNMPv3) para esse destino de armadilha. (Se você definiu apenas um, o nome já aparece neste campo.)
   - **Send Authentication Failure Trap** — Selecione essa opção (a caixa de seleção) se você quiser alertar o destino da armadilha sempre que uma solicitação SNMP for rejeitada por causa de um nome de comunidade ou nome de usuário não reconhecido. Depois de clicar em **Add**, os destinos de intercetação e os nomes associados aparecem na guia **SNMP** da página **Alerts**.
8. Para se certificar de que uma armadilha é válida, selecione um destino de armadilha na tabela e clique em **destino de armadilha de teste** para enviar uma armadilha de teste para o endereço configurado.

**Resultados**

O monitor de eventos envia traps SNMP para o(s) servidor(es) sempre que ocorre um evento alertable.

### Adicionar destinos de intercetação para alertas SNMP

Você pode adicionar até 10 servidores para enviar traps SNMP.

**Antes de começar**

- O servidor de rede que você deseja adicionar deve ser configurado com um aplicativo de serviço SNMP. Você precisa do endereço de rede deste servidor (um endereço IPv4 ou IPv6), para que o monitor de eventos possa enviar mensagens de intercetação para esse endereço. Você pode usar mais de um servidor (até 10 servidores são permitidos).
- O arquivo de base de informações de gerenciamento (MIB) foi copiado e compilado no servidor com o aplicativo de serviço SNMP. Este arquivo MIB define os dados que estão sendo monitorados e gerenciados.

  Se você não tiver o arquivo MIB, poderá obtê-lo no site de suporte da NetApp:

  - Vá para "Suporte à NetApp".
  - Clique em **Downloads** e selecione **Downloads**.
  - Clique em **e-Series SANtricity os Controller Software**.
  - Selecione **Download Latest Release**.
  - Inicie sessão.
  - Aceite a declaração de precaução e o contrato de licença.
  - Role para baixo até ver o arquivo MIB para o tipo de controlador e clique no link para fazer o download do arquivo.

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

   Os destinos de armadilha definidos atualmente aparecem na tabela.

3. Selecione **Add Trap Desinations**.

   A caixa de diálogo Adicionar destinos de armadilha é aberta.

4. Insira um ou mais destinos de armadilha, selecione seus nomes de comunidade ou de usuário associados e clique em **Adicionar**.
   - **Trap Destination** — Digite um endereço IPv4 ou IPv6 do servidor executando um serviço SNMP.
   - **Nome da comunidade ou Nome do usuário** — na lista suspensa, selecione o nome da comunidade (SNMPv2c) ou nome de usuário (SNMPv3) para esse destino de armadilha. (Se você definiu apenas um, o nome já aparece neste campo.)
   - **Send Authentication Failure Trap** — Selecione essa opção (a caixa de seleção) se você quiser alertar o destino da armadilha sempre que uma solicitação SNMP for rejeitada por causa de um nome de comunidade ou nome de usuário não reconhecido. Depois de clicar em **Add**, os destinos de intercetação e os nomes de comunidade ou de usuário associados aparecem na tabela.
5. Para se certificar de que uma armadilha é válida, selecione um destino de armadilha na tabela e clique em **destino de armadilha de teste** para enviar uma armadilha de teste para o endereço configurado.

**Resultados**

O monitor de eventos envia traps SNMP para o(s) servidor(es) sempre que ocorre um evento alertable.

### Configurar variáveis MIB SNMP

Para alertas SNMP, você pode opcionalmente configurar variáveis de base de informações de gerenciamento (MIB) que aparecem em traps SNMP. Essas variáveis podem retornar o nome do storage array, o local do array e uma pessoa de Contato.

**Antes de começar**

O arquivo MIB deve ser copiado e compilado no servidor com o aplicativo de serviço SNMP.

Se não tiver um ficheiro MIB, pode obtê-lo da seguinte forma:

- Vá para "Suporte à NetApp".
- Clique em **Downloads** e selecione **Downloads**.
- Clique em **e-Series SANtricity os Controller Software**.
- Selecione **Download Latest Release**.
- Inicie sessão.
- Aceite a declaração de precaução e o contrato de licença.
- Role para baixo até ver o arquivo MIB para o tipo de controlador e clique no link para fazer o download do arquivo.

**Sobre esta tarefa**

Esta tarefa descreve como definir variáveis MIB para traps SNMP. Essas variáveis podem retornar os seguintes valores em resposta ao SNMP GetRequests:

- `sysName` (nome do storage array)
- `sysLocation` (local do storage array)
- `sysContact` (nome de um administrador)

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.
3. Selecione **Configurar variáveis MIB SNMP**.

   A caixa de diálogo Configurar variáveis MIB SNMP é aberta.

4. Introduza um ou mais dos seguintes valores e, em seguida, clique em **Guardar**.
   - **Name** — o valor para a variável MIB `sysName` . Por exemplo, insira um nome para a matriz de armazenamento.
   - **Localização** — o valor para a variável MIB `sysLocation` . Por exemplo, insira um local da matriz de armazenamento.
   - **Contact** — o valor da variável MIB `sysContact` . Por exemplo, insira um administrador responsável pelo storage array.

**Resultados**

Esses valores aparecem em mensagens de intercetação SNMP para alertas de storage array.

### Edite comunidades para SNMPv2c armadilhas

Você pode editar nomes de comunidade para SNMPv2c armadilhas.

**Antes de começar**

Um nome de comunidade deve ser criado.

**Passos**

1. Selecione **Definir › Alertas**.
2. Selecione a guia **SNMP**.

   Os destinos da armadilha e os nomes da comunidade aparecem na tabela.

3. Selecione **Configurar Comunidades**.
4. Digite o novo nome da comunidade e clique em **Salvar**. Os nomes da comunidade podem consistir apenas em carateres ASCII imprimíveis.

**Resultados**

A guia SNMP da página Alertas exibe o nome da comunidade atualizado.

### Edite as configurações do usuário para SNMPv3 traps

Você pode editar definições de usuário para SNMPv3 traps.

**Antes de começar**

Um usuário deve ser criado para o trap SNMPv3.

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

Os destinos e os nomes de utilizador da armadilha são apresentados na tabela.

3. Para editar uma definição de usuário, selecione o usuário na tabela e clique em **Configurar usuários**.
4. Na caixa de diálogo, clique em **Exibir/Editar configurações**.
5. Edite as seguintes informações:
   - **Nome do usuário** — altere o nome que identifica o usuário, que pode ter até 31 carateres.
   - **Engine ID** — Selecione o Engine ID, que é usado para gerar chaves de autenticação e criptografia para mensagens, e deve ser exclusivo no domínio administrativo. Na maioria dos casos, você deve selecionar **local**. Se você tiver uma configuração não padrão, selecione **Custom**; outro campo aparece onde você deve inserir o ID do mecanismo autorizado como uma cadeia hexadecimal, com um número par de carateres entre 10 e 32 carateres.
   - **Credenciais de autenticação** — Selecione um protocolo de autenticação, que garante a identidade dos usuários. Em seguida, introduza uma palavra-passe de autenticação, que é necessária quando o protocolo de autenticação é definido ou alterado. A senha deve ter entre 8 e 128 carateres.
   - **Credenciais de privacidade** — Selecione um protocolo de privacidade, que é usado para criptografar o conteúdo das mensagens. Em seguida, introduza uma palavra-passe de privacidade, que é necessária quando o protocolo de privacidade é definido ou alterado. A senha deve ter entre 8 e 128 carateres.

**Resultados**

O separador SNMP da página Alertas apresenta as definições atualizadas.

#### Adicione comunidades para SNMPv2c armadilhas

Você pode adicionar até 256 nomes de comunidade para SNMPv2c armadilhas.

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

   Os destinos da armadilha e os nomes da comunidade aparecem na tabela.

3. Selecione **Configurar Comunidades**.

   A caixa de diálogo Configurar Comunidades é aberta.

4. Selecione **Adicionar outra comunidade**.
5. Digite o novo nome da comunidade e clique em **Salvar**.

**Resultados**

O novo nome da comunidade aparece na guia SNMP da página Alertas.

#### Adicione usuários para SNMPv3 traps

Você pode adicionar até 256 usuários para SNMPv3 armadilhas.

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

Os destinos e os nomes de utilizador da armadilha são apresentados na tabela.

3. Selecione **Configurar usuários**.

   A caixa de diálogo Configurar usuários SNMPv3 será aberta.

4. Selecione **Adicionar**.
5. Insira as informações a seguir e clique em **Adicionar**.
   - **Nome do usuário** — Digite um nome para identificar o usuário, que pode ter até 31 carateres.
   - **Engine ID** — Selecione o Engine ID, que é usado para gerar chaves de autenticação e criptografia para mensagens, e deve ser exclusivo no domínio administrativo. Na maioria dos casos, você deve selecionar **local**. Se você tiver uma configuração não padrão, selecione **Custom**; outro campo aparece onde você deve inserir o ID do mecanismo autorizado como uma cadeia hexadecimal, com um número par de carateres entre 10 e 32 carateres.
   - **Credenciais de autenticação** — Selecione um protocolo de autenticação, que garante a identidade dos usuários. Em seguida, introduza uma palavra-passe de autenticação, que é necessária quando o protocolo de autenticação é definido ou alterado. A senha deve ter entre 8 e 128 carateres.
   - **Credenciais de privacidade** — Selecione um protocolo de privacidade, que é usado para criptografar o conteúdo das mensagens. Em seguida, introduza uma palavra-passe de privacidade, que é necessária quando o protocolo de privacidade é definido ou alterado. A senha deve ter entre 8 e 128 carateres.

#### Remova comunidades para SNMPv2c armadilhas

Você pode remover um nome de comunidade para SNMPv2c armadilhas.

#### Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

   Os destinos da armadilha e os nomes da comunidade aparecem na página **Alertas**.

3. Selecione **Configurar Comunidades**.

   A caixa de diálogo Configurar Comunidades é aberta.

4. Selecione o nome da comunidade que deseja excluir e clique no ícone **Remover** (X) na extrema direita.

   Se os destinos de intercetação estiverem associados a esse nome de comunidade, a caixa de diálogo confirmar Remover Comunidade mostrará os endereços de destino de intercetação afetados.

5. Confirme a operação e clique em **Remover**.

#### Resultados

O nome da comunidade e seu destino de armadilha associado são removidos da página Alertas.

#### Remova usuários para SNMPv3 armadilhas

Você pode remover um usuário para SNMPv3 traps.

#### Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

   Os destinos de intercetação e os nomes de usuário aparecem na página Alertas.

3. Selecione **Configurar usuários**.

   A caixa de diálogo Configurar usuários SNMPv3 será aberta.

4. Selecione o nome de usuário que deseja excluir e clique em **Excluir**.
5. Confirme a operação e, em seguida, clique em **Delete**.

**Resultados**

O nome de usuário e seu destino de armadilha associado são removidos da página Alertas.

### Eliminar destinos de armadilha

Você pode excluir um endereço de destino de armadilha para que o monitor de eventos da matriz de armazenamento não envie mais traps SNMP para esse endereço.

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

   Os endereços de destino da armadilha aparecem na tabela.

3. Selecione um destino de armadilha e clique em **Excluir** no canto superior direito da página.
4. Confirme a operação e, em seguida, clique em **Delete**.

   O endereço de destino não aparece mais na página Alertas.

**Resultados**

O destino da armadilha excluída não recebe mais traps SNMP do monitor de eventos da matriz de armazenamento.

## Gerenciar alertas syslog

### Configure o servidor syslog para alertas

Para configurar alertas syslog, você deve inserir um endereço de servidor syslog e uma porta UDP. São permitidos até cinco servidores syslog.

**Antes de começar**

- O endereço do servidor syslog deve estar disponível. Este endereço pode ser um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- O número da porta UDP do servidor syslog deve estar disponível. Esta porta é tipicamente 514.

**Sobre esta tarefa**

Esta tarefa descreve como inserir o endereço e a porta para o servidor syslog e, em seguida, testar o endereço digitado.

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Syslog**.

   Se um servidor syslog ainda não estiver definido, a página Alertas exibirá "Adicionar servidores Syslog".

3. Clique em **Add Syslog Servers**.

   A caixa de diálogo Add Syslog Server (Adicionar servidor Syslog) é aberta.

4. Insira informações para um ou mais servidores syslog (máximo de cinco) e clique em **Adicionar**.
   - **Endereço do servidor** — Digite um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
   - **Porta UDP** — normalmente, a porta UDP para syslog é 514. A tabela exibe os servidores syslog configurados.
5. Para enviar um alerta de teste aos endereços do servidor, selecione **testar todos os servidores Syslog**.

**Resultados**

O monitor de eventos envia alertas para o servidor syslog sempre que ocorre um evento alertable. Para configurar ainda mais as configurações do syslog para logs de auditoria, "Configure o servidor syslog para logs de auditoria" consulte .

> Se vários servidores syslog estiverem configurados, todos os servidores syslog configurados receberão um log de auditoria.

### Editar servidores syslog para alertas

Você pode editar o endereço do servidor usado para receber alertas syslog.

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Syslog**.
3. Na tabela, selecione um endereço de servidor syslog e clique no ícone **Editar** (lápis) na extrema direita.

   A linha se torna um campo editável.

4. Edite o endereço do servidor e o número da porta UDP e clique no ícone **Salvar** (marca de seleção).

**Resultados**

O endereço do servidor atualizado é exibido na tabela.

### Adicione servidores syslog para alertas

Você pode adicionar um máximo de cinco servidores para alertas syslog.

**Antes de começar**

- O endereço do servidor syslog deve estar disponível. Este endereço pode ser um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- O número da porta UDP do servidor syslog deve estar disponível. Esta porta é tipicamente 514.

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Syslog**.
3. Selecione **Adicionar servidores Syslog**.

   A caixa de diálogo Add Syslog Server (Adicionar servidor Syslog) é aberta.

4. Selecione **Adicionar outro servidor syslog**.
5. Insira informações para o servidor syslog e clique em **Adicionar**.

   - **Endereço do servidor Syslog** — Insira um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
   - **Porta UDP** — normalmente, a porta UDP para syslog é 514.

   Você pode configurar até cinco servidores syslog.

**Resultados**

Os endereços do servidor syslog aparecem na tabela.

#### Exclua servidores syslog para alertas

Você pode excluir um servidor syslog para que ele não receba mais alertas.

**Passos**

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Syslog**.
3. Selecione um endereço de servidor syslog e clique em **Remover** no canto superior direito.

   A caixa de diálogo confirmar servidor Syslog será aberta.

4. Confirme a operação e, em seguida, clique em **Delete**.

**Resultados**

O servidor removido não recebe mais alertas do monitor de eventos.

## FAQs

#### E se os alertas estiverem desativados?

Se você quiser que os administradores recebam notificações sobre eventos importantes que ocorrem no storage array, configure um método de alerta.

Para storages gerenciados com o Gerenciador de sistemas do SANtricity, você configura alertas na página Alertas. As notificações de alerta podem ser enviadas por e-mail, traps SNMP ou mensagens syslog. Além disso, os alertas de e-mail podem ser configurados a partir do Assistente de configuração inicial.

#### Como configuro alertas SNMP ou syslog?

Além dos alertas por e-mail, você pode configurar alertas para serem enviados por traps

SNMP (Simple Network Management Protocol) ou por mensagens syslog.

Para configurar alertas SNMP ou syslog, vá para **Configurações › Alertas**.

#### Por que os carimbos de data/hora são inconsistentes entre a matriz e os alertas?

Quando o storage array envia alertas, ele não corrige o fuso horário do servidor de destino ou host que recebe os alertas. Em vez disso, o storage array usa a hora local (GMT) para criar o carimbo de data/hora usado para o Registro de alerta. Como resultado, você pode ver inconsistências entre os carimbos de data/hora do storage array e o servidor ou host recebendo um alerta.

Como o storage array não corrige o fuso horário ao enviar alertas, o carimbo de data/hora nos alertas é GMT-Relative, que tem um deslocamento de fuso horário de zero. Para calcular um carimbo de data/hora apropriado ao seu fuso horário local, você deve determinar o deslocamento da hora do GMT e, em seguida, adicionar ou subtrair esse valor dos carimbos de data/hora.

# Configurações de matriz

## Descrição geral das definições

Você pode configurar o System Manager para algumas configurações gerais de array e recursos adicionais.

#### Que definições posso configurar?

As configurações da matriz incluem:

- "Configurações de cache e desempenho"
- <a href="https://docs.netapp.com/pt-br/e-series-santricity-118/sm-settings/automatic-load-balancing-overview.html"">"Balanceamento de carga automático"</a>
- "Recursos adicionais"
- "Segurança da unidade"

#### Tarefas relacionadas

Saiba mais sobre as tarefas relacionadas às Configurações do sistema:

- "Baixar a interface de linha de comando (CLI)"
- "Criar chave de segurança interna"
- "Criar chave de segurança externa"
- "Configurar portas iSCSI"
- "Configurar portas NVMe em IB"
- "Configurar o NVMe em portas RoCE"

# Conceitos

## Configurações de cache e desempenho

A memória cache é uma área de armazenamento temporário volátil no controlador que tem um tempo de acesso mais rápido do que a Mídia da unidade.

Com o armazenamento em cache, o desempenho geral de e/S pode ser aumentado da seguinte forma:

- Os dados solicitados do host para uma leitura podem já estar no cache de uma operação anterior, eliminando assim a necessidade de acesso à unidade.
- Gravar dados é gravado inicialmente no cache, o que libera o aplicativo para continuar em vez de esperar que os dados sejam gravados na unidade.

As configurações padrão de cache atendem aos requisitos da maioria dos ambientes, mas você pode alterá-las se desejar.

### Configurações de cache da matriz de armazenamento

Para todos os volumes no storage array, você pode especificar os seguintes valores na página sistema:

- **Valor inicial para lavagem** — a porcentagem de dados não escritos no cache que aciona um flush cache (gravação no disco). Quando o cache mantém a porcentagem de início especificada de dados não escritos, um flush é acionado. Por padrão, o controlador começa a limpar o cache quando o cache atinge 80 por cento cheio.
- **Cache block size** — o tamanho máximo de cada bloco de cache, que é uma unidade organizacional para gerenciamento de cache. O tamanho do bloco de cache é por padrão 8 KiB, mas pode ser definido como 4, 8, 16 ou 32 KiB. Idealmente, o tamanho do bloco de cache deve ser definido para o tamanho de e/S predominante de suas aplicações. Sistemas de arquivos ou aplicativos de banco de dados geralmente usam tamanhos menores, enquanto um tamanho maior é bom para aplicativos que exigem transferência de dados grande ou e/S sequenciais

### Definições de cache de volume

Para volumes individuais em uma matriz de armazenamento, você pode especificar os seguintes valores na página volumes (**armazenamento › volumes**):

- **Read caching** — o cache de leitura é um buffer que armazena dados que foram lidos das unidades. Os dados para uma operação de leitura podem já estar no cache de uma operação anterior, o que elimina a necessidade de acessar as unidades. Os dados permanecem no cache de leitura até que sejam lavados.
  - * Pré-busca de cache de leitura dinâmica* — Pré-busca de leitura de cache dinâmico permite que o controlador copie blocos de dados sequenciais adicionais para o cache enquanto ele está lendo blocos de dados de uma unidade para o cache. Esse armazenamento em cache aumenta a chance de que futuras solicitações de dados possam ser preenchidas a partir do cache. A pré-busca de leitura de cache dinâmico é importante para aplicativos Multimídia que usam e/S sequenciais A taxa e a quantidade de dados pré-obtidos no cache são auto-ajustáveis com base na taxa e no tamanho da solicitação das leituras do host. O acesso aleatório não faz com que os dados sejam pré-obtidos no cache. Este recurso não se aplica quando o armazenamento em cache de leitura está desativado.
- **Write caching** — o cache de gravação é um buffer que armazena dados do host que ainda não foram gravados nas unidades. Os dados permanecem no cache de gravação até que sejam gravados nas unidades. O armazenamento em cache de gravação pode aumentar a performance de e/S.

**Possível perda de dados** — se você ativar a opção **armazenamento em cache sem baterias** e não tiver uma fonte de alimentação universal para proteção, você pode perder dados. Além disso, você pode perder dados se não tiver baterias do controlador e ativar a opção **armazenamento em cache sem baterias**.

- **Armazenamento em cache sem baterias** — a configuração armazenamento em cache sem baterias permite que o armazenamento em cache continue, mesmo quando as baterias estiverem faltando, falharem, descarregadas completamente ou não estiverem totalmente carregadas. Normalmente, a escolha do armazenamento em cache sem baterias não é recomendada, pois os dados podem ser perdidos se perder energia. Normalmente, o armazenamento em cache de gravação é desligado temporariamente pelo controlador até que as baterias sejam carregadas ou uma bateria com falha seja substituída.
- **Armazenamento em cache com espelhamento** — o armazenamento em cache com espelhamento ocorre quando os dados gravados na memória cache de um controlador também são gravados na memória de cache do outro controlador. Portanto, se um controlador falhar, o outro pode concluir todas as operações de gravação pendentes. O espelhamento do cache de gravação estará disponível somente se o armazenamento em cache de gravação estiver habilitado e duas controladoras estiverem presentes. O armazenamento em cache de gravação com espelhamento é a configuração padrão na criação de volume.

### Descrição geral do balanceamento de carga automático

O balanceamento de carga automático fornece gerenciamento de recursos de e/S aprimorado, reagindo dinamicamente às alterações de carga ao longo do tempo e ajustando automaticamente a propriedade do controlador de volume para corrigir quaisquer problemas de desequilíbrio de carga quando as cargas de trabalho mudam entre os controladores.

A carga de trabalho de cada controlador é continuamente monitorizada e, com a colaboração dos drivers multipath instalados nos hosts, pode ser automaticamente colocada em equilíbrio sempre que necessário. Quando o workload é rebalanceado automaticamente entre os controladores, o administrador de storage fica aliviado da sobrecarga de ajustar manualmente a propriedade do controlador de volume para acomodar alterações de carga no storage array.

Quando o balanceamento de carga automático está ativado, ele executa as seguintes funções:

- Monitora e equilibra automaticamente a utilização de recursos do controlador.
- Ajusta automaticamente a propriedade do controlador de volume quando necessário, otimizando assim a largura de banda de e/S entre os hosts e o storage array.

#### Ativar e desativar o balanceamento de carga automático

O balanceamento de carga automático é ativado por padrão em todos os storages de armazenamento.

Você pode querer desativar o balanceamento de carga automático em seu storage array pelos seguintes motivos:

- Você não deseja alterar automaticamente a propriedade de um volume específico para equilibrar a carga de trabalho.
- Você está operando em um ambiente altamente ajustado onde a distribuição de carga é propositadamente configurada para alcançar uma distribuição específica entre os controladores.

#### Tipos de host que suportam o recurso balanceamento de carga automático

Embora o balanceamento de carga automático esteja habilitado no nível do storage array, o tipo de host selecionado para um host ou cluster de host tem uma influência direta sobre como o recurso opera.

Ao equilibrar a carga de trabalho do storage array entre controladores, o recurso balanceamento de carga automático tenta mover volumes que são acessíveis por ambos os controladores e que são mapeados apenas para um host ou cluster de host capaz de suportar o recurso balanceamento de carga automático.

Esse comportamento impede que um host perca o acesso a um volume devido ao processo de balanceamento de carga; no entanto, a presença de volumes mapeados para hosts que não suportam o balanceamento de carga automático afeta a capacidade do storage array de equilibrar a carga de trabalho. Para que o balanceamento de carga automático equilibre a carga de trabalho, o driver multipath deve suportar TPGS e o tipo de host deve ser incluído na tabela a seguir.

> Para que um cluster de host seja considerado capaz de balanceamento de carga automático, todos os hosts nesse grupo devem ser capazes de suportar balanceamento de carga automático.

| Tipo de host que suporta balanceamento de carga automático | Com este driver multipath |
|---|---|
| Windows ou Windows em cluster | MPIO com NetApp Série e DSM |
| Linux DM-MP (Kernel 3,10 ou posterior) | DM-MP com `scsi_dh_alua` manipulador de dispositivos |
| VMware | Nativo Multipathing Plugin (NMP) com `VMW_SATP_ALUA Storage Array Type` plug-in |

> Com exceções menores, os tipos de host que não suportam o balanceamento de carga automático continuam a operar normalmente, independentemente de o recurso estar ou não ativado. Uma exceção é que, se um sistema tiver um failover, os storages de armazenamento movem volumes não mapeados ou não atribuídos de volta para o controlador proprietário quando o caminho de dados retornar. Quaisquer volumes mapeados ou atribuídos a hosts não automáticos de balanceamento de carga não são movidos.

Consulte o "Ferramenta de Matriz de interoperabilidade" para obter informações de compatibilidade para driver multipath específico, nível de SO e suporte à bandeja de unidades e controlador.

#### Verificando a compatibilidade do SO com o recurso balanceamento de carga automático

Verifique a compatibilidade do sistema operacional com o recurso balanceamento de carga automático antes de configurar um novo (ou migrar um sistema existente).

1. Aceda ao "Ferramenta de Matriz de interoperabilidade" para encontrar a sua solução e verificar o suporte.

   Se o sistema estiver executando o Red Hat Enterprise Linux 6 ou SUSE Linux Enterprise Server 11, entre em Contato com o suporte técnico.

2. Atualize e configure o `/etc/multipath.conf file`.

3. Certifique-se de que ambos `retain_attached_device_handler` e `detect_prio` estão definidos como `yes` para o fornecedor e o produto aplicáveis, ou use as configurações padrão.

## Configure as definições da matriz

### Edite o nome da matriz de armazenamento

Você pode alterar o nome da matriz de armazenamento que aparece na barra de título do Gerenciador de sistema do SANtricity.

**Passos**

1. Selecione **Definições › sistema**.
2. Em **Geral**, procure o campo **Nome:**.

   Se o nome de uma matriz de armazenamento não tiver sido definido, este campo exibirá "desconhecido".

3. Clique no ícone **Edit** (lápis) ao lado do nome da matriz de armazenamento.

   O campo torna-se editável.

4. Introduza um novo nome.

   Um nome pode conter letras, números e os carateres especiais sublinhado (_), traço (-) e sinal de hash ( Um nome não pode conter espaços. Um nome pode ter um comprimento máximo de 30 carateres. O nome deve ser único.

5. Clique no ícone **Save** (marca de seleção).

   Se quiser fechar o campo editável sem fazer alterações, clique no ícone **Cancelar** (X).

**Resultados**

O novo nome é exibido na barra de título do Gerenciador de sistema do SANtricity.

### Ligue as luzes de localização da matriz de armazenamento

Para encontrar a localização física de uma matriz de armazenamento em um gabinete, você pode ligar suas luzes de localizador (LED).

**Passos**

1. Selecione **Definições › sistema**.
2. Em **Geral**, clique em **Ativar as luzes do localizador da matriz de armazenamento**.

   A caixa de diálogo Ativar luzes do localizador de matriz de armazenamento abre-se e as luzes de localização da matriz de armazenamento correspondente acendem-se.

3. Quando tiver localizado fisicamente o storage, retorne à caixa de diálogo e selecione **Desligar**.

**Resultados**

As luzes de localização apagam-se e a caixa de diálogo fecha-se.

### Sincronizar relógios de storage array

Se o Network Time Protocol (NTP) não estiver ativado, você poderá definir manualmente os relógios nos controladores para que eles sejam sincronizados com o cliente de gerenciamento (o sistema usado para executar o navegador que acessa o System Manager).

#### Sobre esta tarefa

A sincronização garante que os carimbos de hora do evento no registo de eventos correspondem aos carimbos de hora gravados nos ficheiros de registo do anfitrião. Durante o processo de sincronização, os controladores permanecem disponíveis e operacionais.

> Se o NTP estiver ativado no System Manager, não use esta opção para sincronizar relógios. Em vez disso, o NTP sincroniza automaticamente os relógios com um host externo usando SNTP (Simple Network Time Protocol).

> Após a sincronização, você pode notar que as estatísticas de desempenho são perdidas ou distorcidas, as programações são afetadas (ASUP, snapshots, etc.) e os carimbos de hora nos dados de log são distorcidos. O uso do NTP evita esse problema.

#### Passos

1. Selecione **Definições › sistema**.
2. Em **General**, clique em **Synchronize Storage Array Clocks**.

   A caixa de diálogo Sincronizar relógios de matriz de armazenamento é aberta. Mostra a data e hora atuais do(s) controlador(es) e do computador usado como cliente de gerenciamento.

   > Para matrizes de armazenamento simplex, apenas um controlador é apresentado.

3. Se os horários mostrados na caixa de diálogo não corresponderem, clique em **Sincronizar**.

#### Resultados

Depois que a sincronização for bem-sucedida, os carimbos de hora do evento são os mesmos para o log de eventos e os logs do host.

### Salve a configuração do storage array

Você pode salvar as informações de configuração de uma matriz de armazenamento em um arquivo de script para economizar tempo configurando matrizes de armazenamento adicionais com a mesma configuração.

#### Antes de começar

O storage array não deve estar passando por nenhuma operação que altere suas configurações lógicas. Exemplos dessas operações incluem a criação ou exclusão de volumes, o download do firmware do controlador, a atribuição ou modificação de unidades hot spare ou a adição de capacidade (unidades) a um grupo de volumes.

#### Sobre esta tarefa

Salvar a configuração do storage array gera um script de interface de linha de comando (CLI) que contém configurações de storage array, configuração de volume, configuração de host ou atribuições de host para

volume para um storage array. Você pode usar esse script de CLI gerado para replicar uma configuração para outro storage array com a mesma configuração de hardware.

No entanto, você não deve usar esse script CLI gerado para recuperação de desastres. Em vez disso, para fazer uma restauração do sistema, use o arquivo de backup do banco de dados de configuração que você cria manualmente ou entre em Contato com o suporte técnico para obter esses dados dos dados mais recentes do Auto-Support.

Esta operação *não* salva essas configurações:

- A vida útil da bateria
- A hora do dia do controlador
- As configurações de memória de acesso aleatório estático não volátil (NVSRAM)
- Quaisquer funcionalidades premium
- A senha do storage array
- O estado de funcionamento e os estados dos componentes de hardware
- O estado de funcionamento (exceto ótimo) e os estados dos grupos de volume
- Serviços de cópia, como espelhamento e cópia de volume

> **Risco de erros de aplicativo** — não use essa opção se o storage array estiver passando por uma operação que mudará qualquer configuração lógica. Exemplos dessas operações incluem a criação ou exclusão de volumes, o download do firmware do controlador, a atribuição ou modificação de unidades hot spare ou a adição de capacidade (unidades) a um grupo de volumes.

**Passos**

1. Selecione **Definições › sistema**.
2. Selecione **Save Storage Array Configuration**.
3. Selecione os itens da configuração que deseja salvar:
   - Configurações da matriz de armazenamento
   - Configuração do volume
   - Configuração de host
   - Atribuições de host para volume

   > Se você selecionar o item **atribuição de host para volume**, o item **Configuração de volume** e o item **Configuração do host** também serão selecionados por padrão. Você não pode salvar "atribuições de host para volume" sem salvar também "Configuração de volume" e "Configuração de host".

4. Clique em **Salvar**.

   O arquivo é salvo na pasta Downloads do navegador com o nome `storage-array-configuration.cfg`.

**Depois de terminar**

Para carregar a configuração do storage array salvo em outro storage array, use a interface de linha de

comando (SMcli) do SANtricity com a `-f` opção de aplicar o `.cfg` arquivo.

Você também pode carregar uma configuração de storage array para outros storage arrays usando a interface do Unified Manager (selecione **Gerenciar › Importar configurações**).

### Limpar a configuração do storage array

Use a operação Limpar configuração quando quiser excluir todos os pools, grupos de volume, volumes, definições de host e atribuições de host do storage de armazenamento.

#### Antes de começar

Antes de limpar a configuração do storage array, faça backup dos dados.

#### Sobre esta tarefa

Existem duas opções de Configuração de matrizes de armazenamento claras:

- **Volume** — normalmente, você pode usar a opção volume para reconfigurar um storage de armazenamento de teste como um storage de produção. Por exemplo, você pode configurar um storage array para teste e, quando terminar de testar, remover a configuração de teste e configurar o storage array para um ambiente de produção.
- **Storage Array** — normalmente, você pode usar a opção Storage Array para mover uma matriz de armazenamento para outro departamento ou grupo. Por exemplo, você pode estar usando um storage array no Engineering, e agora o Engineering está recebendo um novo storage array, então você deseja mover o storage array atual para Administração, onde ele será reconfigurado.

  A opção Storage Array (Matriz de armazenamento) exclui algumas configurações adicionais.

| | Volume | Storage array |
|---|---|---|
| Desativa o ARVM | X | X |
| Exclui pools e grupos de volume | X | X |
| Elimina volumes | X | X |
| Exclui hosts e clusters de host | X | X |
| Exclui atribuições de host | X | X |
| Exclui o nome da matriz de armazenamento | | X |
| Redefine as configurações de cache do storage array para padrão | | X |

**Risco de perda de dados** — esta operação exclui todos os dados da matriz de armazenamento. (Ele não faz uma eliminação segura.) Não é possível cancelar esta operação depois de iniciada. Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

**Passos**

1. Selecione **Definições › sistema**.
2. Selecione **Limpar configuração da matriz de armazenamento**.
3. Na lista suspensa, selecione **volume** ou **Storage Array**.
4. **Opcional:** se você quiser salvar a configuração (não os dados), use os links na caixa de diálogo.
5. Confirme se pretende efetuar a operação.

**Resultados**

- A configuração atual é excluída, destruindo todos os dados existentes no storage array.
- Todas as unidades não são atribuídas.

### Altere as configurações de cache para a matriz de armazenamento

Para todos os volumes na matriz de armazenamento, você pode ajustar as configurações de memória de cache para limpeza e tamanho de bloco.

**Sobre esta tarefa**

A memória cache é uma área de armazenamento temporário volátil no controlador, que tem um tempo de acesso mais rápido do que a Mídia da unidade. Para ajustar o desempenho do cache, você pode ajustar as seguintes configurações:

| Definição de cache | Descrição |
|---|---|
| Inicie a lavagem do cache de demanda | Especifica a porcentagem de dados não escritos no cache que aciona uma descarga de cache (gravação no disco). Por padrão, a lavagem do cache começa quando os dados não escritos atingem a capacidade de 80%. Uma porcentagem maior é uma boa escolha para ambientes com operações de gravação principalmente, portanto, novas solicitações de gravação podem ser processadas pelo cache sem precisar ir para o disco. Configurações mais baixas são melhores em ambientes onde a e/S é irregular (com picos de dados), de modo que o sistema limpa o cache frequentemente entre picos de dados. No entanto, uma porcentagem inicial inferior a 80% pode causar diminuição do desempenho. |
| Tamanho do bloco de cache | O tamanho do bloco de cache determina o tamanho máximo de cada bloco de cache, que é uma unidade organizacional para gerenciamento de cache. Por padrão, o tamanho do bloco é 32 KiB. O sistema permite que o tamanho do bloco de cache seja de 4, 8, 16 ou 32 KiBs. Os aplicativos usam tamanhos de bloco diferentes, o que afeta o desempenho do storage. Um tamanho menor é uma boa escolha para sistemas de arquivos ou aplicativos de banco de dados. Um tamanho maior é ideal para aplicações que geram e/S sequenciais, como Multimídia. |

**Passos**

1. Selecione **Definições › sistema**.
2. Role para baixo até **Configurações adicionais** e clique em **alterar configurações de cache**.

   A caixa de diálogo alterar configurações de cache é aberta.

3. Ajuste os seguintes valores:
   - * Iniciar lavagem de cache de demanda* — escolha uma porcentagem apropriada para a e/S usada em seu ambiente. Se escolher um valor inferior a 80%, poderá notar uma diminuição do desempenho.
   - **Tamanho do bloco de cache —** escolha um tamanho apropriado para seus aplicativos.
4. Clique em **Salvar**.

### Definir o balanceamento de carga automático

O recurso balanceamento de carga automático garante que o tráfego de e/S de entrada dos hosts seja gerenciado e balanceado dinamicamente em ambos os controladores. Esta funcionalidade está ativada por predefinição, mas pode desativá-la a partir do System Manager.

#### Sobre esta tarefa

Quando o balanceamento de carga automático está ativado, ele executa as seguintes funções:

- Monitora e equilibra automaticamente a utilização de recursos do controlador.
- Ajusta automaticamente a propriedade do controlador de volume quando necessário, otimizando assim a largura de banda de e/S entre os hosts e o storage array.

Você pode querer desativar o balanceamento de carga automático em seu storage array pelos seguintes motivos:

- Você não deseja alterar automaticamente a propriedade de um volume específico para equilibrar a carga de trabalho.
- Você está operando em um ambiente altamente ajustado onde a distribuição de carga é propositadamente configurada para alcançar uma distribuição específica entre os controladores.

#### Passos

1. Selecione **Definições › sistema**.
2. Role para baixo até **Configurações adicionais** e clique em **Ativar/Desativar balanceamento de carga automático**.

   O texto abaixo dessa opção indica se o recurso está ativado ou desativado no momento.

   Abre-se uma caixa de diálogo de confirmação.

3. Confirme clicando em **Sim** para continuar.

   Ao selecionar esta opção, pode alternar a funcionalidade entre activado/desativado.

> Se esse recurso for movido de desativado para ativado, o recurso Relatório de conetividade do host também será ativado automaticamente.

#### Ative ou desative a interface de gerenciamento legada

Você pode ativar ou desativar a interface de gerenciamento legado (símbolo), que é um método de comunicação entre o storage array e o cliente de gerenciamento.

##### Sobre esta tarefa

Por padrão, a interface de gerenciamento legada está ativada. Se você desativá-lo, o storage array e o cliente de gerenciamento usarão um método de comunicação mais seguro (API REST sobre https); no entanto, certas ferramentas e tarefas podem ser afetadas se estiverem desativadas.

> Para o sistema de armazenamento EF600, esta funcionalidade está desativada por predefinição.

A definição afeta as operações da seguinte forma:

- **On** (padrão) — a configuração necessária para configurar o espelhamento com a CLI e algumas outras ferramentas, como o adaptador OCI.
- **Off** — definição necessária para impor a confidencialidade nas comunicações entre o storage array e o cliente de gerenciamento, e para acessar ferramentas externas. Configuração recomendada ao configurar um servidor de diretório (LDAP).

##### Passos

1. Selecione **Definições › sistema**.
2. Role para baixo até **Configurações adicionais** e clique em **alterar Interface de Gerenciamento**.
3. Na caixa de diálogo, clique em **Yes** para continuar.

## Configurar recursos adicionais

#### Como os recursos adicionais funcionam

Complementos são recursos que não estão incluídos na configuração padrão do System Manager e podem exigir uma chave para habilitar. Um recurso complementar pode ser um único recurso premium ou um pacote de recursos.

As etapas a seguir fornecem uma visão geral para habilitar um recurso ou um pacote de recursos premium:

1. Obtenha as seguintes informações:
   - O número de série do chassi e o identificador de ativação do recurso, que identificam a matriz de armazenamento para o recurso a ser instalado. Esses itens estão disponíveis no System Manager.
   - Código de ativação do recurso, que está disponível no site de suporte quando você compra o recurso.
2. Obtenha a chave de recurso entrando em Contato com seu provedor de armazenamento ou acessando o site de ativação de recursos Premium. Forneça o número de série do chassi, o identificador de ativação e o código de recurso para ativação.
3. Usando o System Manager, ative o recurso premium ou o pacote de recursos usando o arquivo de chave de recurso.

#### Terminologia de recursos complementares

Saiba como os termos do recurso complementar se aplicam à sua matriz de

armazenamento.

| Prazo | Descrição |
| --- | --- |
| Identificador de ativação de funcionalidade | Um identificador de ativação de recurso é uma cadeia de carateres exclusiva que identifica a matriz de armazenamento específica. Esse identificador garante que, quando você obtém o recurso premium, ele está associado apenas a essa matriz de armazenamento específica. Esta cadeia de carateres é exibida em Complementos na página sistema. |
| Arquivo de chave de recurso | Um arquivo de chave de recurso é um arquivo que você recebe para desbloquear e habilitar um recurso premium ou pacote de recursos. |
| Pacote de funcionalidades | Um pacote de recursos é um pacote que altera os atributos do storage de armazenamento (por exemplo, alterando o protocolo de Fibre Channel para iSCSI). Os pacotes de recursos exigem uma chave especial para ativá-los. |
| Recurso Premium | Um recurso premium é uma opção extra que requer uma chave para ativá-lo. Ele não está incluído na configuração padrão do System Manager. |

### Obter um arquivo de chave de recurso

Para habilitar um recurso premium ou um pacote de recursos em seu storage array, primeiro você deve obter um arquivo de chave de recurso. Uma chave é associada a apenas um storage array.

#### Sobre esta tarefa

Esta tarefa descreve como reunir as informações necessárias para o recurso e, em seguida, enviar uma solicitação para um arquivo de chave de recurso. As informações necessárias incluem:

- Número de série do chassis
- Identificador de ativação de funcionalidade
- Código de ativação do recurso

#### Passos

1. No System Manager, localize e registe o número de série do chassis. Você pode visualizar este número de série passando o Mouse sobre o bloco do Centro de suporte.
2. No System Manager, localize o identificador de ativação da funcionalidade. Vá para **Configurações › sistema** e role para baixo até **Complementos**. Procure o **Feature Enable Identifier**. Registe o número do identificador de ativação da funcionalidade.
3. Localize e grave o código para a ativação da funcionalidade. Para pacotes de recursos, esse código é fornecido nas instruções apropriadas para executar a conversão.

   As instruções do NetApp estão disponíveis em "Centro de Documentação de sistemas NetApp e-Series".

   Para recursos premium, você pode acessar o código de ativação no site de suporte, como segue:

   a. Inicie sessão no "Suporte à NetApp".

   b. Aceda a **licenças de software** para o seu produto.

c. Insira o número de série do chassi do storage de armazenamento e clique em **Go**.

d. Procure os códigos de ativação da funcionalidade na coluna **chave de licença**.

e. Registre o Código de ativação do recurso para o recurso desejado.

4. Solicite um arquivo de chave de recurso enviando um e-mail ou um documento de texto para o fornecedor de armazenamento com as seguintes informações: Número de série do chassi, o identificador de ativação e o código para ativação de recursos.

   Também pode aceder "Ativação de licença do NetApp: Ativação do recurso Premium do storage array" e introduzir as informações necessárias para obter a funcionalidade ou o pacote de funcionalidades. (As instruções neste site são para recursos premium, não pacotes de recursos.)

**Depois de terminar**

Quando você tem um arquivo de chave de recurso, você pode ativar o recurso premium ou o pacote de recursos.

### Ative um recurso premium

Um recurso premium é uma opção extra que requer uma chave para ativar.

**Antes de começar**

- Obteve uma tecla de função. Se necessário, contacte o suporte técnico para obter uma chave.
- Você carregou o arquivo de chave no cliente de gerenciamento (o sistema com um navegador para acessar o System Manager).

**Sobre esta tarefa**

Esta tarefa descreve como usar o System Manager para habilitar um recurso premium.

> Se você quiser desativar um recurso premium, use o comando Desativar recurso de storage (`disable storageArray (featurePack | feature=featureAttributeList`) na interface de linha de comando (CLI).

**Passos**

1. Selecione **Definições › sistema**.
2. Em **Complementos**, selecione **Ativar recurso Premium**.

   A caixa de diálogo Ativar um recurso Premium é aberta.

3. Clique em **Browse** e selecione o arquivo de chave.

   O nome do arquivo é exibido na caixa de diálogo.

4. Clique em **Ativar**.

### Ativar o pacote de funcionalidades

Um pacote de recursos é um pacote que altera os atributos do storage de armazenamento (por exemplo, alterando o protocolo de Fibre Channel para iSCSI). Os pacotes de recursos exigem uma chave especial para a capacitação.

**Antes de começar**

- Você seguiu as instruções apropriadas que descrevem a conversão e a preparação para os novos atributos de storage array. Para obter instruções de conversão do protocolo do host, consulte o guia de manutenção de hardware do modelo do controlador.
- O storage array está offline, portanto, nenhum host ou aplicativo está acessando-o.
- É feito backup de todos os dados.
- Você obteve um arquivo de pacote de recursos.

  O arquivo do pacote de recursos é carregado no cliente de gerenciamento (o sistema com um navegador para acessar o System Manager).

> É necessário agendar uma janela de manutenção de tempo de inatividade e parar todas as operações de e/S entre o host e os controladores. Além disso, esteja ciente de que você não pode acessar dados no storage array até que você tenha concluído com êxito a conversão.

**Sobre esta tarefa**

Esta tarefa descreve como utilizar o Gestor do sistema para ativar um pacote de funcionalidades. Quando terminar, você deve reiniciar o storage array.

**Passos**

1. Selecione **Definições › sistema**.
2. Em **Add-ons**, selecione **Change Feature Pack**.
3. Clique em **Browse** e selecione o arquivo de chave.

   O nome do arquivo é exibido na caixa de diálogo.

4. Digite `change` o campo.
5. Clique em **alterar**.

   A migração do pacote de recursos começa e os controladores reiniciam. Os dados de cache não escritos são excluídos, o que garante nenhuma atividade de e/S. Ambos os controladores reiniciam automaticamente para que o novo pacote de recursos tenha efeito. O storage array retorna a um estado responsivo após a reinicialização ser concluída.

## Baixar a interface de linha de comando (CLI)

No System Manager, você pode baixar o pacote de interface de linha de comando (CLI).

A CLI fornece um método baseado em texto para configurar e monitorar matrizes de armazenamento. Ele se comunica via https e usa a mesma sintaxe que a CLI disponível no pacote de software de gerenciamento instalado externamente. Nenhuma chave é necessária para baixar o CLI.

**Antes de começar**

Um Java Runtime Environment (JRE), versão 8 e superior, deve estar disponível no sistema de gerenciamento onde você planeja executar os comandos CLI.

**Passos**

1. Selecione **Definições › sistema**.
2. Em **Complementos**, selecione **Interface de linha de comando**.

O pacote ZIP é baixado para o navegador.

3. Salve o arquivo ZIP no sistema de gerenciamento onde você planeja executar comandos CLI para o storage array e, em seguida, extraia o arquivo.

   Agora você pode executar comandos CLI a partir de um prompt do sistema operacional, como o prompt dos C:. Uma referência de comando CLI está disponível no menu Ajuda no canto superior direito da interface do usuário do System Manager.

## FAQs

**O que é balanceamento de carga automático?**

### O recurso balanceamento de carga automático fornece balanceamento de e/S automatizado e garante que o tráfego de e/S recebido dos hosts seja gerenciado e balanceado dinamicamente entre ambos os controladores.

O recurso balanceamento de carga automático fornece gerenciamento de recursos de e/S aprimorado, reagindo dinamicamente às alterações de carga ao longo do tempo e ajustando automaticamente a propriedade do controlador de volume para corrigir quaisquer problemas de desequilíbrio de carga quando as cargas de trabalho mudam entre os controladores.

A carga de trabalho de cada controlador é continuamente monitorizada e, com a colaboração dos drivers multipath instalados nos hosts, pode ser automaticamente colocada em equilíbrio sempre que necessário. Quando o workload é rebalanceado automaticamente entre os controladores, o administrador de storage fica aliviado da sobrecarga de ajustar manualmente a propriedade do controlador de volume para acomodar alterações de carga no storage array.

Quando o balanceamento de carga automático está ativado, ele executa as seguintes funções:

- Monitora e equilibra automaticamente a utilização de recursos do controlador.
- Ajusta automaticamente a propriedade do controlador de volume quando necessário, otimizando assim a largura de banda de e/S entre os hosts e o storage array.

> Qualquer volume atribuído para usar o cache SSD de um controlador não é elegível para uma transferência automática de balanceamento de carga.

**O que é cache de controladora?**

### O cache do controlador é um espaço de memória física que simplifica dois tipos de operações de e/S (entrada/saída): Entre os controladores e os hosts e entre os controladores e os discos.

Para transferências de dados de leitura e gravação, os hosts e controladores se comunicam por conexões de alta velocidade. No entanto, as comunicações do back-end do controlador para os discos são mais lentas, porque os discos são dispositivos relativamente lentos.

Quando o cache do controlador recebe dados, o controlador reconhece aos aplicativos host que agora está segurando os dados. Dessa forma, os aplicativos host não precisam esperar que a e/S seja gravada no disco. Em vez disso, os aplicativos podem continuar as operações. Os dados armazenados em cache também são facilmente acessíveis por aplicativos de servidor, eliminando a necessidade de leituras adicionais de disco para acessar os dados.

O cache da controladora afeta o desempenho geral do storage de várias maneiras:

- O cache funciona como um buffer, para que as transferências de dados de host e disco não precisem ser sincronizadas.
- Os dados para uma operação de leitura ou gravação do host podem estar em cache de uma operação anterior, o que elimina a necessidade de acessar o disco.
- Se o cache de gravação for usado, o host poderá enviar comandos de gravação subsequentes antes que os dados de uma operação de gravação anterior sejam gravados no disco.
- Se a pré-busca de cache estiver ativada, o acesso de leitura sequencial será otimizado. A pré-busca de cache torna uma operação de leitura mais provável de encontrar seus dados no cache, em vez de ler os dados do disco.

**Possível perda de dados** — se você ativar a opção **armazenamento em cache sem baterias** e não tiver uma fonte de alimentação universal para proteção, você pode perder dados. Além disso, você pode perder dados se não tiver baterias do controlador e ativar a opção **armazenamento em cache sem baterias**.

**O que é a lavagem de cache?**

Quando a quantidade de dados não escritos no cache atinge um determinado nível, o controlador grava periodicamente dados em cache em uma unidade. Este processo de gravação é chamado de "lavagem".

O controlador usa dois algoritmos para a lavagem do cache: Baseado na demanda e baseado em idade. O controlador usa um algoritmo baseado em demanda até que a quantidade de dados em cache caia abaixo do limite de descarga do cache. Por padrão, um flush começa quando 80% do cache está em uso.

No System Manager, você pode definir o limite "'Start Demand cache flushing'" para melhor suportar o tipo de e/S usado em seu ambiente. Em um ambiente que é principalmente operações de gravação, você deve definir a porcentagem de ""Limpeza de cache de demanda inicial"" alta para aumentar a probabilidade de que quaisquer novas solicitações de gravação possam ser processadas pelo cache sem ter que ir para o disco. Uma configuração de porcentagem alta limita o número de fluxos de cache para que mais dados permaneçam no cache, o que aumenta a chance de mais acertos no cache.

Em um ambiente onde a e/S é irregular (com picos de dados), você pode usar a lavagem de cache baixo para que o sistema flushes o cache frequentemente entre picos de dados. Em um ambiente de e/S diversificado que processa uma variedade de cargas, ou quando o tipo de cargas é desconhecido, defina o limite em 50% como um bom meio-terra. Esteja ciente de que, se você escolher uma porcentagem inicial inferior a 80%, poderá ver uma redução no desempenho porque os dados necessários para uma leitura de host podem não estar disponíveis. Escolher uma porcentagem menor também aumenta o número de gravações de disco necessárias para manter o nível de cache, o que aumenta a sobrecarga do sistema.

O algoritmo baseado em idade especifica o período de tempo durante o qual os dados de gravação podem permanecer no cache antes de serem elegíveis para serem lavados para os discos. Os controladores usam o algoritmo baseado em idade até que o limite de descarga do cache seja atingido. O padrão é de 10 segundos, mas esse período de tempo é contado apenas durante períodos de inatividade. Você não pode modificar o tempo de flush no System Manager; em vez disso, você deve usar o comando **Set Storage Array** na interface de linha de comando (CLI).

**Possível perda de dados** — se você ativar a opção **armazenamento em cache sem baterias** e não tiver uma fonte de alimentação universal para proteção, você pode perder dados. Além disso, você pode perder dados se não tiver baterias do controlador e ativar a opção **armazenamento em cache sem baterias**.

#### O que é o tamanho do bloco de cache?

O controlador do storage organiza seu cache em "blocos", que são pedaços de memória que podem ser 8, 16, 32 KiB de tamanho. Todos os volumes no sistema de armazenamento compartilham o mesmo espaço de cache; portanto, os volumes podem ter apenas um tamanho de bloco de cache.

Os aplicativos usam tamanhos de bloco diferentes, o que pode ter um impacto no desempenho de storage. Por padrão, o tamanho do bloco no System Manager é de 32 KiB, mas você pode definir o valor para 8, 16, 32 KiBs. Um tamanho menor é uma boa escolha para sistemas de arquivos ou aplicativos de banco de dados. Um tamanho maior é uma boa escolha para aplicativos que exigem grande transferência de dados, e/S sequencial ou alta largura de banda, como Multimídia.

#### Quando devo sincronizar relógios de storage?

Você deve sincronizar manualmente os relógios do controlador na matriz de armazenamento se notar que os carimbos de hora mostrados no System Manager não estão alinhados com os carimbos de hora mostrados no cliente de gerenciamento (o computador que está acessando o System Manager através do navegador). Esta tarefa só é necessária se o NTP (Network Time Protocol) não estiver ativado no System Manager.

É altamente recomendável que você use um servidor NTP em vez de sincronizar manualmente os relógios. NTP sincroniza automaticamente os relógios com um servidor externo usando SNTP (Simple Network Time Protocol).

Você pode verificar o status da sincronização na caixa de diálogo Sincronizar relógios de storage de armazenamento, que está disponível na página sistema. Se os horários mostrados na caixa de diálogo não corresponderem, execute uma sincronização. Você pode visualizar periodicamente essa caixa de diálogo, que indica se as exibições de tempo dos relógios do controlador se afastaram e não estão mais sincronizadas.

# Segurança da unidade

## Visão geral do Drive Security

Você pode configurar o Drive Security e o gerenciamento de chaves na página Security Key Management (Gerenciamento de chaves de segurança).

#### O que é o Drive Security?

*Drive Security* é um recurso que impede o acesso não autorizado a dados em unidades habilitadas para segurança quando removido do storage array. Essas unidades podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard). Quando as unidades FDE ou FIPS são removidas fisicamente do storage, elas não podem operar até serem instaladas em outro storage, e nesse

ponto, as unidades estarão em um estado de segurança bloqueado até que a chave de segurança correta seja fornecida. A *security key* é uma cadeia de carateres que é compartilhada entre esses tipos de unidades e os controladores em um storage array.

Saiba mais:

- "Como funciona o recurso Segurança da Unidade"
- "Como funciona o gerenciamento de chaves de segurança"
- "Terminologia de segurança da unidade"

#### Como faço para configurar o gerenciamento de chaves?

Para implementar o Drive Security, é necessário ter unidades FDE ou FIPS instaladas no array. Para configurar a gestão de chaves para estas unidades, aceda ao **Definições › sistema › Gestão de chaves de segurança**, onde pode criar uma chave interna a partir da memória persistente do controlador ou uma chave externa a partir de um servidor de gestão de chaves. Por fim, você ativa a Segurança da Unidade para pools e grupos de volume selecionando "segura-capaz" nas configurações de volume.

Saiba mais:

- "Criar chave de segurança interna"
- "Criar chave de segurança externa"
- "Criar pool manualmente"
- "Criar grupos de volume"

#### Como posso desbloquear unidades?

Se você tiver configurado o gerenciamento de chaves e, em seguida, mover unidades habilitadas para segurança de um storage array para outro, será necessário atribuir novamente a chave de segurança ao novo storage array para obter acesso aos dados criptografados nas unidades.

Saiba mais:

- "Desbloqueie unidades ao usar o gerenciamento de chaves internas"
- "Desbloqueie unidades ao usar o gerenciamento de chaves externas"

#### Informações relacionadas

Saiba mais sobre tarefas relacionadas ao gerenciamento de chaves:

- "Use certificados assinados pela CA para autenticação com um servidor de gerenciamento de chaves"
- "Faça backup da chave de segurança"

## Conceitos

#### Como funciona o recurso Segurança da Unidade

O Drive Security é um recurso de storage array que fornece uma camada extra de segurança com unidades de criptografia completa de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).

Quando essas unidades são usadas com o recurso Segurança da Unidade, elas precisam de uma chave de segurança para acessar seus dados. Quando as unidades são fisicamente removidas do array, elas não podem operar até serem instaladas em outro array, em que ponto, elas estarão em um estado de segurança bloqueado até que a chave de segurança correta seja fornecida.

#### Como implementar o Drive Security

Para implementar o Drive Security, execute as etapas a seguir.

1. Equipe seu storage array com unidades com capacidade segura, unidades FDE ou FIPS. (Para volumes que exigem suporte FIPS, use apenas unidades FIPS. A combinação de unidades FIPS e FDE em um grupo de volumes ou pool resultará no tratamento de todas as unidades como unidades FDE. Além disso, uma unidade FDE não pode ser adicionada ou usada como sobressalente em um grupo ou pool de volumes totalmente FIPS.)
2. Crie uma chave de segurança, que é uma cadeia de carateres que é compartilhada pelo controlador e unidades para acesso de leitura/gravação. Você pode criar uma chave interna a partir da memória persistente do controlador ou uma chave externa de um servidor de gerenciamento de chaves. Para o gerenciamento de chaves externas, a autenticação deve ser estabelecida com o servidor de gerenciamento de chaves.
3. Ative a segurança da unidade para pools e grupos de volumes:
   - Crie um pool ou grupo de volumes (procure **Sim** na coluna **compatível com segurança** na tabela candidatos).
   - Selecione um pool ou grupo de volumes quando criar um novo volume (procure **Sim** ao lado de **compatível com segurança** na tabela de candidatos ao grupo de grupos de volumes e pool).

#### Como o Drive Security funciona no nível da unidade

Uma unidade com capacidade segura, FDE ou FIPS, criptografa os dados durante gravações e descriptografa dados durante leituras. Essa criptografia e descriptografia não afetam o desempenho ou o fluxo de trabalho do usuário. Cada unidade tem sua própria chave de criptografia exclusiva, que nunca pode ser transferida da unidade.

O recurso Drive Security fornece uma camada extra de proteção com unidades com capacidade de segurança. Quando grupos de volume ou pools nessas unidades são selecionados para o Drive Security, as unidades procuram uma chave de segurança antes de permitir o acesso aos dados. Você pode ativar o Drive Security para pools e grupos de volumes a qualquer momento, sem afetar os dados existentes na unidade. No entanto, não é possível desativar o Drive Security sem apagar todos os dados da unidade.

#### Como o Drive Security funciona no nível da matriz de armazenamento

Com o recurso Segurança da unidade, você cria uma chave de segurança compartilhada entre as unidades e os controladores habilitados para segurança em um storage de armazenamento. Sempre que a alimentação das unidades é desligada e ligada, as unidades ativadas por segurança mudam para um estado de Segurança bloqueada até que o controlador aplique a chave de segurança.

Se uma unidade habilitada para segurança for removida da matriz de armazenamento e reinstalada em uma matriz de armazenamento diferente, a unidade estará em um estado de segurança bloqueado. A unidade relocada procura a chave de segurança antes de tornar os dados acessíveis novamente. Para desbloquear os dados, você aplica a chave de segurança do storage array de origem. Após um processo de desbloqueio bem-sucedido, a unidade relocada usará a chave de segurança já armazenada no storage de armazenamento de destino e o arquivo de chave de segurança importado não será mais necessário.

Para o gerenciamento de chaves internas, a chave de segurança real é armazenada no controlador em um local não acessível. Não está em formato legível por humanos, nem é acessível ao usuário.

#### Como o Drive Security funciona no nível do volume

Ao criar um pool ou grupo de volumes a partir de unidades com capacidade segura, também é possível ativar a Segurança da unidade para esses pools ou grupos de volumes. A opção Segurança da unidade torna as unidades e os grupos de volume e pools associados seguros-*enabled*.

Tenha em mente as seguintes diretrizes antes de criar grupos e pools de volume habilitados para segurança:

- Os grupos de volumes e pools devem ser compostos inteiramente de unidades com capacidade de segurança. (Para volumes que exigem suporte FIPS, use apenas unidades FIPS. A combinação de unidades FIPS e FDE em um grupo de volumes ou pool resultará no tratamento de todas as unidades como unidades FDE. Além disso, uma unidade FDE não pode ser adicionada ou usada como sobressalente em um grupo ou pool de volumes totalmente FIPS.)
- Os grupos de volume e os pools devem estar em um estado ideal.

### Como funciona o gerenciamento de chaves de segurança

Quando você implementa o recurso Segurança da unidade, as unidades habilitadas para segurança (FIPS ou FDE) exigem uma chave de segurança para acesso aos dados. Uma chave de segurança é uma cadeia de carateres que é compartilhada entre esses tipos de unidades e os controladores em um storage array.

Sempre que a alimentação das unidades é desligada e ligada, as unidades ativadas por segurança mudam para um estado de Segurança bloqueada até que o controlador aplique a chave de segurança. Se uma unidade habilitada para segurança for removida da matriz de armazenamento, os dados da unidade serão bloqueados. Quando a unidade é reinstalada em uma matriz de armazenamento diferente, ela procura a chave de segurança antes de tornar os dados acessíveis novamente. Para desbloquear os dados, tem de aplicar a chave de segurança original.

Você pode criar e gerenciar chaves de segurança usando um dos seguintes métodos:

- Gerenciamento de chaves internas na memória persistente do controlador.
- Gerenciamento de chaves externas em um servidor de gerenciamento de chaves externo.

#### Gerenciamento de chaves internas

As chaves internas são mantidas e "ocultas" em um local não acessível na memória persistente do controlador. Para implementar o gerenciamento de chaves internas, execute as seguintes etapas:

1. Instale unidades com capacidade segura no storage de armazenamento. Essas unidades podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).
2. Certifique-se de que a funcionalidade de Segurança da unidade está ativada. Se necessário, entre em Contato com o fornecedor de armazenamento para obter instruções sobre como ativar o recurso Segurança da unidade.
3. Crie uma chave de segurança interna, que envolve a definição de um identificador e uma frase-passe. O identificador é uma cadeia de carateres associada à chave de segurança e é armazenada no controlador e em todas as unidades associadas à chave. A frase-passe é usada para criptografar a chave de

segurança para fins de backup. Para criar uma chave interna, aceda ao **Definições › sistema › Gestão da chave de segurança › criar chave interna**.

A chave de segurança é armazenada no controlador num local oculto e não acessível. Em seguida, você pode criar grupos de volume ou pools habilitados para segurança ou habilitar a segurança em grupos de volumes e pools existentes.

#### Gerenciamento de chaves externas

As chaves externas são mantidas em um servidor de gerenciamento de chaves separado, usando um KMIP (Key Management Interoperability Protocol). Para implementar o gerenciamento de chaves externas, execute as seguintes etapas:

1. Instale unidades com capacidade segura no storage de armazenamento. Essas unidades podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).
2. Certifique-se de que a funcionalidade de Segurança da unidade está ativada. Se necessário, entre em Contato com o fornecedor de armazenamento para obter instruções sobre como ativar o recurso Segurança da unidade.
3. Obtenha um arquivo de certificado de cliente assinado. Um certificado de cliente valida os controladores do storage array, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP.
   a. Primeiro, você conclui e faz o download de uma solicitação de assinatura de certificado de cliente (CSR). Aceda ao **Definições › certificados › Gestão de chaves › CSR completo**.
   b. Em seguida, você solicita um certificado de cliente assinado de uma CA confiável pelo servidor de gerenciamento de chaves. (Você também pode criar e baixar um certificado de cliente a partir do servidor de gerenciamento de chaves usando o arquivo CSR.)
   c. Depois de ter um arquivo de certificado de cliente, copie esse arquivo para o host onde você está acessando o System Manager.
4. Recupere um arquivo de certificado do servidor de gerenciamento de chaves e copie esse arquivo para o host onde você está acessando o System Manager. Um certificado do servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, de modo que o storage array possa confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou servidor para o servidor de gerenciamento de chaves.
5. Crie uma chave externa, que envolve definir o endereço IP do servidor de gerenciamento de chaves e o número da porta usada para comunicações KMIP. Durante esse processo, você também carrega arquivos de certificado. Para criar uma chave externa, aceda ao **Definições › sistema › Gestão da chave de segurança › criar chave externa**.

O sistema se coneta ao servidor de gerenciamento de chaves com as credenciais inseridas. Em seguida, você pode criar grupos de volume ou pools habilitados para segurança ou habilitar a segurança em grupos de volumes e pools existentes.

### Terminologia de segurança da unidade

Saiba como os termos de segurança da unidade se aplicam à sua matriz de armazenamento.

| Prazo | Descrição |
| --- | --- |
| Recurso de segurança da unidade | O Drive Security é um recurso de storage array que fornece uma camada extra de segurança com unidades de criptografia completa de disco (FDE) ou unidades FIPS (Federal Information Processing Standard). Quando essas unidades são usadas com o recurso Segurança da Unidade, elas precisam de uma chave de segurança para acessar seus dados. Quando as unidades são fisicamente removidas do array, elas não podem operar até serem instaladas em outro array, em que ponto, elas estarão em um estado de segurança bloqueado até que a chave de segurança correta seja fornecida. |
| Unidades FDE | As unidades Full Disk Encryption (FDE) executam a encriptação na unidade de disco no nível do hardware. O disco rígido contém um chip ASIC que criptografa dados durante gravações e, em seguida, descriptografa dados durante leituras. |
| Unidades FIPS | As unidades FIPS usam Federal Information Processing Standards (FIPS) 140-2 nível 2. Eles são essencialmente unidades FDE que aderem aos padrões do governo dos Estados Unidos para garantir algoritmos e métodos de criptografia fortes. As unidades FIPS têm padrões de segurança mais altos do que as unidades FDE. |
| Cliente de gestão | Um sistema local (computador, tablet, etc.) que inclui um navegador para acessar o System Manager. |
| Frase-passe | A frase-passe é usada para criptografar a chave de segurança para fins de backup. A mesma frase-passe usada para criptografar a chave de segurança deve ser fornecida quando a chave de segurança de backup for importada como resultado de uma migração de unidade ou troca de cabeça. Uma frase-passe pode ter entre 8 e 32 carateres.<br><br>A frase-passe para o Drive Security é independente da senha do Administrador do storage. |
| Unidades com capacidade de segurança | As unidades com capacidade segura podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard), que criptografam dados durante gravações e descriptografam dados durante leituras. Essas unidades são consideradas seguras-*Capable* porque podem ser usadas para segurança adicional usando o recurso Segurança da Unidade. Se o recurso Segurança da unidade estiver habilitado para grupos de volume e pools usados com essas unidades, as unidades se tornarão seguras-*enabled*. |
| Unidades habilitadas para segurança | As unidades habilitadas para segurança são usadas com o recurso Segurança da unidade. Quando você ativa o recurso de Segurança da Unidade e, em seguida, aplica o Drive Security a um pool ou grupo de volume em unidades seguras-*capazes*, as unidades ficam seguras___ ativadas. O acesso de leitura e gravação está disponível somente por meio de um controlador configurado com a chave de segurança correta. Essa segurança adicional impede o acesso não autorizado aos dados em uma unidade que é fisicamente removida do storage array. |

| Prazo | Descrição |
| --- | --- |
| Chave de segurança | Uma chave de segurança é uma cadeia de carateres que é compartilhada entre as unidades e controladores habilitados para segurança em um storage array. Sempre que a alimentação das unidades é desligada e ligada, as unidades ativadas por segurança mudam para um estado de Segurança bloqueada até que o controlador aplique a chave de segurança. Se uma unidade habilitada para segurança for removida da matriz de armazenamento, os dados da unidade serão bloqueados. Quando a unidade é reinstalada em uma matriz de armazenamento diferente, ela procura a chave de segurança antes de tornar os dados acessíveis novamente. Para desbloquear os dados, tem de aplicar a chave de segurança original. Você pode criar e gerenciar chaves de segurança usando um dos seguintes métodos:<br>• Gerenciamento de chaves internas — criar e manter chaves de segurança na memória persistente do controlador.<br>• Gerenciamento de chaves externas — Crie e mantenha chaves de segurança em um servidor de gerenciamento de chaves externo. |
| Identificador da chave de segurança | O identificador da chave de segurança é uma cadeia de carateres associada à chave de segurança durante a criação da chave. O identificador é armazenado no controlador e em todas as unidades associadas à chave de segurança. |

## Configurar chaves de segurança

### Criar chave de segurança interna

Para usar o recurso Segurança da unidade, você pode criar uma chave de segurança interna compartilhada pelos controladores e unidades seguras no storage de armazenamento. As chaves internas são mantidas na memória persistente do controlador.

#### Antes de começar

- As unidades com capacidade de segurança devem ser instaladas no storage array. Essas unidades podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).
- O recurso Segurança da unidade deve estar ativado. Caso contrário, uma caixa de diálogo não é possível criar chave de segurança será aberta durante esta tarefa. Se necessário, entre em Contato com o fornecedor de armazenamento para obter instruções sobre como ativar o recurso Segurança da unidade.

> Se as unidades FDE e FIPS estiverem instaladas no storage de armazenamento, todas elas compartilharão a mesma chave de segurança.

#### Sobre esta tarefa

Nesta tarefa, você define um identificador e uma frase-passe para associar à chave de segurança interna.

> A frase-passe para o Drive Security é independente da senha do Administrador do storage.

#### Passos

1. Selecione **Definições › sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **criar chave interna**.

   Se você ainda não gerou uma chave de segurança, a caixa de diálogo criar chave de segurança será aberta.

3. Introduza as informações nos seguintes campos:

   - * Definir um identificador de chave de segurança* — você pode aceitar o valor padrão (nome da matriz de armazenamento e carimbo de hora, que é gerado pelo firmware do controlador) ou inserir seu próprio valor. Pode introduzir até 189 carateres alfanuméricos sem espaços, pontuação ou símbolos.

     Carateres adicionais são gerados automaticamente, anexados a ambas as extremidades da cadeia de carateres inserida. Os carateres gerados garantem que o identificador é exclusivo.

   - * Definir uma frase-passe/re-insira a frase-passe* — Digite e confirme uma frase-passe. O valor pode ter entre 8 e 32 carateres e deve incluir cada um dos seguintes:
     - Uma letra maiúscula (uma ou mais). Tenha em mente que a frase-passe é sensível a maiúsculas e minúsculas.
     - Um número (um ou mais).
     - Um caráter não alfanumérico, como !, *, at (um ou mais).

     **Certifique-se de gravar suas entradas para uso posterior**. Se você precisar mover uma unidade habilitada para segurança do storage, você deve saber o identificador e a frase-passe para desbloquear os dados da unidade.

4. Clique em **criar**.

   A chave de segurança é armazenada no controlador num local não acessível. Junto com a chave real, há um arquivo de chave criptografada que é baixado do seu navegador.

   O caminho para o arquivo baixado pode depender do local de download padrão do seu navegador.

5. Grave o identificador da chave, a frase-passe e a localização do ficheiro de chave transferido e, em seguida, clique em **Fechar**.

**Resultados**

Agora você pode criar grupos de volume ou pools habilitados para segurança ou habilitar a segurança em grupos de volumes e pools existentes.

Sempre que a alimentação das unidades for desligada e novamente ligada, todas as unidades ativadas para segurança mudam para um estado de segurança bloqueado. Neste estado, os dados ficam inacessíveis até que o controlador aplique a chave de segurança correta durante a inicialização da unidade. Se alguém remover fisicamente uma unidade bloqueada e instalá-la em outro sistema, o estado Segurança bloqueada impede o acesso não autorizado aos seus dados.

**Depois de terminar**

Você deve validar a chave de segurança para se certificar de que o arquivo de chave não está corrompido.

### Criar chave de segurança externa

Para usar o recurso Segurança da unidade com um servidor de gerenciamento de chaves, você deve criar uma chave externa compartilhada pelo servidor de gerenciamento de chaves e pelas unidades com capacidade segura no storage de armazenamento.

#### Antes de começar

- As unidades com capacidade de segurança devem ser instaladas no array. Essas unidades podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).

> Se as unidades FDE e FIPS estiverem instaladas no storage de armazenamento, todas elas compartilharão a mesma chave de segurança.

- O recurso Segurança da unidade deve estar ativado. Caso contrário, uma caixa de diálogo não é possível criar chave de segurança será aberta durante esta tarefa. Se necessário, entre em Contato com o fornecedor de armazenamento para obter instruções sobre como ativar o recurso Segurança da unidade.
- Você tem um arquivo de certificado de cliente assinado para os controladores do storage array e copiou esse arquivo para o host onde está acessando o System Manager. Um certificado de cliente valida os controladores do storage array, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP (Key Management Interoperability Protocol).
- Você deve recuperar um arquivo de certificado do servidor de gerenciamento de chaves e, em seguida, copiar esse arquivo para o host onde você está acessando o System Manager. Um certificado do servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, de modo que o storage array possa confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou servidor para o servidor de gerenciamento de chaves.

> Para obter mais informações sobre o certificado do servidor, consulte a documentação do servidor de gerenciamento de chaves.

#### Sobre esta tarefa

Nesta tarefa, você define o endereço IP do servidor de gerenciamento de chaves e o número da porta que ele usa e, em seguida, carrega certificados para gerenciamento de chaves externas.

#### Passos

1. Selecione **Definições › sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **criar chave externa**.

> Se o gerenciamento de chaves internas estiver configurado no momento, uma caixa de diálogo será aberta e solicitará que você confirme se deseja mudar para o gerenciamento de chaves externas.

   A caixa de diálogo criar chave de segurança externa é aberta.

3. Em **conetar ao Key Server**, insira as informações nos campos a seguir.
   - **Endereço do servidor de gerenciamento de chaves** — Digite o nome de domínio totalmente qualificado ou o endereço IP (IPv4 ou IPv6) do servidor usado para o gerenciamento de chaves.

- **Número da porta de gerenciamento de chaves** — Digite o número da porta usada para comunicações KMIP. O número de porta mais comum usado para comunicações do servidor de gerenciamento de chaves é 5696.

  **Opcional:** se você quiser configurar um servidor de chaves de backup, clique em **Add Key Server** e insira as informações desse servidor. O segundo servidor de chaves será usado se o servidor de chaves primárias não puder ser alcançado. Certifique-se de que cada servidor de chaves tenha acesso ao mesmo banco de dados de chaves; caso contrário, o array publicará erros e não poderá usar o servidor de backup.

  Apenas um servidor de chave única é usado de cada vez. Se a matriz de armazenamento não conseguir alcançar o servidor de chave primária, a matriz entrará em Contato com o servidor de chave de backup. Esteja ciente de que você deve manter a paridade entre ambos os servidores; a falha em fazê-lo pode resultar em erros.

- **Selecione o certificado do cliente** — clique no primeiro botão **Procurar** para selecionar o arquivo de certificado para os controladores do storage.
- **Selecione o certificado do servidor de gerenciamento de chaves** — clique no segundo botão **Procurar** para selecionar o arquivo de certificado para o servidor de gerenciamento de chaves. Você pode escolher um certificado de raiz, intermediário ou servidor para o servidor de gerenciamento de chaves.

4. Clique em **seguinte**.
5. Em **Create/Backup Key**, você pode criar uma chave de backup para fins de segurança.

   - (Recomendado) para criar uma chave de cópia de segurança, mantenha a caixa de verificação selecionada e, em seguida, introduza e confirme uma frase-passe. O valor pode ter entre 8 e 32 carateres e deve incluir cada um dos seguintes:
     - Uma letra maiúscula (uma ou mais). Tenha em mente que a frase-passe é sensível a maiúsculas e minúsculas.
     - Um número (um ou mais).
     - Um caráter não alfanumérico, como !, *, at (um ou mais).

   **Certifique-se de gravar suas entradas para uso posterior**. Se você precisar mover uma unidade habilitada para segurança do storage de armazenamento, você deve saber a frase-passe para desbloquear os dados da unidade.

   +

   - Se não pretender criar uma chave de cópia de segurança, desmarque a caixa de verificação.

     Esteja ciente de que se você perder o acesso ao servidor de chaves externo e não tiver uma chave de backup, perderá o acesso aos dados nas unidades se elas forem migradas para outro storage array. Esta opção é o único método para criar uma chave de backup no System Manager.

6. Clique em **Finish**.

   O sistema se coneta ao servidor de gerenciamento de chaves com as credenciais inseridas. Uma cópia da chave de segurança é então armazenada no sistema local.

O caminho para o arquivo baixado pode depender do local de download padrão do seu navegador.

7. Grave a frase-passe e a localização do ficheiro de chave transferido e, em seguida, clique em **Fechar**.

   A página exibe a seguinte mensagem com links adicionais para gerenciamento de chaves externas:

   ```
   Current key management method: External
   ```

8. Teste a conexão entre o storage array e o servidor de gerenciamento de chaves selecionando **Test Communication**.

   Os resultados do teste são exibidos na caixa de diálogo.

**Resultados**

Quando o gerenciamento de chaves externas está habilitado, você pode criar grupos ou pools de volumes habilitados para segurança ou habilitar a segurança em grupos de volumes e pools existentes.

Sempre que a alimentação das unidades for desligada e novamente ligada, todas as unidades ativadas para segurança mudam para um estado de segurança bloqueado. Neste estado, os dados ficam inacessíveis até que o controlador aplique a chave de segurança correta durante a inicialização da unidade. Se alguém remover fisicamente uma unidade bloqueada e instalá-la em outro sistema, o estado Segurança bloqueada impede o acesso não autorizado aos seus dados.

**Depois de terminar**

Você deve validar a chave de segurança para se certificar de que o arquivo de chave não está corrompido.

## Gerenciar chaves de segurança

### Altere a chave de segurança

A qualquer momento, você pode substituir uma chave de segurança por uma nova chave. Talvez seja necessário alterar uma chave de segurança nos casos em que você tenha uma potencial violação de segurança em sua empresa e queira garantir que funcionários não autorizados não possam acessar os dados das unidades.

**Passos**

1. Selecione **Definições › sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **alterar chave**.

   A caixa de diálogo alterar chave de segurança é aberta.

3. Introduza as informações nos seguintes campos.
   - **Defina um identificador de chave de segurança** — (apenas para chaves de segurança internas.) Aceite o valor padrão (nome da matriz de armazenamento e carimbo de data/hora, que é gerado pelo firmware da controladora) ou insira seu próprio valor. Pode introduzir até 189 carateres alfanuméricos sem espaços, pontuação ou símbolos.

Os carateres adicionais são gerados automaticamente e são anexados a ambas as extremidades da cadeia de carateres inserida. Os carateres gerados ajudam a garantir que o identificador é exclusivo.

- **Defina uma frase-passe/digite novamente a frase-passe** — em cada um desses campos, insira sua frase-passe. O valor pode ter entre 8 e 32 carateres e deve incluir cada um dos seguintes:
  - Uma letra maiúscula (uma ou mais). Tenha em mente que a frase-passe é sensível a maiúsculas e minúsculas.
  - Um número (um ou mais).
  - Um caráter não alfanumérico, como !, *, at (um ou mais).

4. Para chaves de segurança externas, se você quiser excluir a chave de segurança antiga quando a nova for criada, marque a caixa de seleção "Excluir chave de segurança atual…" na parte inferior da caixa de diálogo.

**Certifique-se de gravar suas entradas para uso posterior** — se você precisar mover uma unidade habilitada para segurança da matriz de armazenamento, você deve saber o identificador e a frase-passe para desbloquear os dados da unidade.

5. Clique em **alterar**.

   A nova chave de segurança substitui a chave anterior, que não é mais válida.

O caminho para o arquivo baixado pode depender do local de download padrão do seu navegador.

6. Grave o identificador da chave, a frase-passe e a localização do ficheiro de chave transferido e, em seguida, clique em **Fechar**.

**Depois de terminar**

Você deve validar a chave de segurança para se certificar de que o arquivo de chave não está corrompido.

### Mude do gerenciamento de chaves externas para internas

Você pode alterar o método de gerenciamento de segurança de unidade de um servidor de chaves externo para o método interno usado pelo storage array. A chave de segurança definida anteriormente para o gerenciamento de chaves externas é então usada para o gerenciamento de chaves internas.

**Sobre esta tarefa**

Nesta tarefa, desative o gerenciamento de chaves externas e baixe uma nova cópia de backup para o host local. A chave existente ainda é usada para o Drive Security, mas será gerenciada internamente na matriz de armazenamento.

**Passos**

1. Selecione **Definições › sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **Desativar Gerenciamento de chaves externas**.

   A caixa de diálogo Desativar gerenciamento de chaves externas é aberta.

3. Em **defina uma frase-passe/insira novamente a frase-passe**, insira e confirme uma frase-passe para o backup da chave. O valor pode ter entre 8 e 32 carateres e deve incluir cada um dos seguintes:
   - Uma letra maiúscula (uma ou mais). Tenha em mente que a frase-passe é sensível a maiúsculas e minúsculas.
   - Um número (um ou mais).
   - Um caráter não alfanumérico, como !, *, at (um ou mais).

   > *Certifique-se de gravar suas entradas para uso posterior*. Se você precisar mover uma unidade habilitada para segurança do storage, você deve saber o identificador e a frase-passe para desbloquear os dados da unidade.

4. Clique em **Desativar**.

   A chave de cópia de segurança é transferida para o seu anfitrião local.

5. Grave o identificador da chave, a frase-passe e a localização do ficheiro de chave transferido e, em seguida, clique em **Fechar**.

**Resultados**

O Drive Security agora é gerenciado internamente por meio do storage array.

**Depois de terminar**

Você deve validar a chave de segurança para se certificar de que o arquivo de chave não está corrompido.

### Editar as configurações do servidor de gerenciamento de chaves

Se você tiver configurado o gerenciamento de chaves externas, poderá exibir e editar as configurações do servidor de gerenciamento de chaves a qualquer momento.

**Passos**

1. Selecione **Definições › sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **Exibir/Editar Configurações do servidor de gerenciamento de chaves**.
3. Edite informações nos seguintes campos:
   - **Endereço do servidor de gerenciamento de chaves** — Digite o nome de domínio totalmente qualificado ou o endereço IP (IPv4 ou IPv6) do servidor usado para o gerenciamento de chaves.
   - **Número da porta de gerenciamento de chaves** — Digite o número da porta usada para as comunicações KMIP (Key Management Interoperability Protocol).

     **Opcional:** você pode incluir outro servidor de chaves clicando em **Add Key Server**.

4. Clique em **Salvar**.

### Faça backup da chave de segurança

Depois de criar ou alterar uma chave de segurança, você pode criar uma cópia de backup do arquivo de chave caso o original seja corrompido.

**Sobre esta tarefa**

Esta tarefa descreve como fazer backup de uma chave de segurança criada anteriormente. Durante este procedimento, você cria uma nova frase-passe para o backup. Essa frase-passe não precisa corresponder à frase-passe usada quando a chave original foi criada ou alterada pela última vez. A frase-passe é aplicada apenas ao backup que você está criando.

**Passos**

1. Selecione **Definições › sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **Backup Key**.

   A caixa de diálogo fazer backup da chave de segurança é aberta.

3. Nos campos **Definir uma frase-passe/voltar a introduzir frase-passe**, introduza e confirme uma frase-passe para esta cópia de segurança.

   O valor pode ter entre 8 e 32 carateres e deve incluir cada um dos seguintes:

   - Uma letra maiúscula (uma ou mais)
   - Um número (um ou mais)
   - Um caráter não alfanumérico, como !, *, at (um ou mais)

   **Certifique-se de gravar sua entrada para uso posterior**. Você precisa da frase-passe para acessar o backup dessa chave de segurança.

4. Clique em **Backup**.

   Um backup da chave de segurança é baixado para seu host local e a caixa de diálogo **Confirm/Record Security Key Backup** (confirmar/gravar backup da chave de segurança*) será aberta.

   O caminho para o arquivo de chave de segurança baixado pode depender do local de download padrão do navegador.

5. Grave sua frase-passe em um local seguro e clique em **Fechar**.

**Depois de terminar**

Você deve validar a chave de segurança de backup.

### Valide a chave de segurança

Você pode validar a chave de segurança para se certificar de que ela não foi corrompida e para verificar se você tem uma frase-passe correta.

**Sobre esta tarefa**

Esta tarefa descreve como validar a chave de segurança criada anteriormente. Esta é uma etapa importante para se certificar de que o arquivo de chave não está corrompido e a frase-passe está correta, o que garante que você possa acessar mais tarde os dados da unidade se mover uma unidade habilitada para segurança de uma matriz de armazenamento para outra.

**Passos**

1. Selecione **Definições › sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **Validar chave**.

A caixa de diálogo Validar chave de segurança é aberta.

3. Clique em **Procurar** e selecione o ficheiro de chave (por exemplo, `drivesecurity.slk` ).
4. Introduza a frase-passe associada à chave selecionada.

   Quando você seleciona um arquivo de chave válido e uma frase-passe, o botão **Validar** fica disponível.

5. Clique em **Validar**.

   Os resultados da validação são exibidos na caixa de diálogo.

6. Se os resultados mostrarem "a chave de segurança validada com êxito", clique em **Fechar**. Se for apresentada uma mensagem de erro, siga as instruções sugeridas apresentadas na caixa de diálogo.

### Desbloqueie unidades ao usar o gerenciamento de chaves internas

Se você configurou o gerenciamento de chaves internas e depois mover unidades habilitadas para segurança de um storage array para outro, será necessário atribuir novamente a chave de segurança ao novo storage array para obter acesso aos dados criptografados nas unidades.

#### Antes de começar

- Na matriz de origem (a matriz onde você está removendo as unidades), você exportou grupos de volume e removeu as unidades. No array de destino, você instalou novamente as unidades.

  > A função Exportar/Importar não é suportada na interface de usuário do System Manager; você deve usar a interface de linha de comando (CLI) para exportar/importar um grupo de volumes para um storage array diferente.

  Instruções detalhadas para migrar um grupo de volumes são fornecidas no "Base de dados de Conhecimento da NetApp". Certifique-se de seguir as instruções apropriadas para arrays mais recentes gerenciados pelo System Manager ou para sistemas legados.

- O recurso Segurança da unidade deve estar ativado. Caso contrário, uma caixa de diálogo não é possível criar chave de segurança será aberta durante esta tarefa. Se necessário, entre em Contato com o fornecedor de armazenamento para obter instruções sobre como ativar o recurso Segurança da unidade.
- Você deve saber a chave de segurança que está associada às unidades que deseja desbloquear.
- O arquivo de chave de segurança está disponível no cliente de gerenciamento (o sistema com um navegador usado para acessar o System Manager). Se você estiver movendo as unidades para um storage array gerenciado por um sistema diferente, será necessário mover o arquivo de chave de segurança para esse cliente de gerenciamento.

#### Sobre esta tarefa

Quando você usa o gerenciamento de chaves internas, a chave de segurança é armazenada localmente no storage array. Uma chave de segurança é uma cadeia de carateres que é compartilhada pelo controlador e unidades para acesso de leitura/gravação. Quando as unidades são fisicamente removidas da matriz e instaladas em outra, elas não podem operar até que você forneça a chave de segurança correta.

Você pode criar uma chave interna a partir da memória persistente do controlador ou uma chave externa de um servidor de gerenciamento de chaves. Este tópico descreve como desbloquear dados quando o gerenciamento de chaves *internas* é usado. Se você usou o gerenciamento de chaves *externas*, "Desbloqueie unidades ao usar o gerenciamento de chaves externas"consulte . Se você estiver executando uma atualização de controladora e estiver trocando todos os controladores pelo hardware mais recente, siga etapas diferentes conforme descrito no centro de documentação e-Series e SANtricity, em "Desbloquear unidades".

Depois de reinstalar unidades habilitadas para segurança em outro array, esse array descobre as unidades e exibe uma condição de "precisa de atenção" junto com um status de "chave de segurança necessária". Para desbloquear os dados da unidade, selecione o ficheiro da chave de segurança e introduza a frase-passe da chave. (Esta frase-passe não é a mesma que a senha do administrador da matriz de armazenamento.)

Se outras unidades habilitadas para segurança estiverem instaladas no novo storage array, elas poderão usar uma chave de segurança diferente da que você está importando. Durante o processo de importação, a chave de segurança antiga é usada apenas para desbloquear os dados das unidades que você está instalando. Quando o processo de desbloqueio é bem-sucedido, as unidades recém-instaladas são recodificadas para a chave de segurança da matriz de armazenamento de destino.

**Passos**

1. Selecione **Definições › sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **desbloquear unidades seguras**.

   A caixa de diálogo desbloquear unidades seguras abre-se. Todas as unidades que exigem uma chave de segurança são mostradas na tabela.

3. **Opcional:** passe o Mouse sobre um número de unidade para ver a localização da unidade (número de prateleira e número de compartimento).
4. Clique em **Procurar** e selecione o arquivo de chave de segurança que corresponde à unidade que deseja desbloquear.

   O arquivo de chave selecionado aparece na caixa de diálogo.

5. Introduza a frase-passe associada a este ficheiro de chave.

   Os carateres inseridos são mascarados.

6. Clique em **Unlock**.

   Se a operação de desbloqueio for bem-sucedida, a caixa de diálogo exibe: "As unidades seguras associadas foram desbloqueadas."

**Resultados**

Quando todas as unidades estiverem bloqueadas e, em seguida, desbloqueadas, cada controlador na matriz de armazenamento será reiniciado. No entanto, se já houver algumas unidades desbloqueadas no storage de armazenamento de destino, os controladores não serão reinicializados.

**Depois de terminar**

No array de destino (o array com as unidades recém-instaladas), agora você pode importar grupos de volume.

A função Exportar/Importar não é suportada na interface de usuário do System Manager; você deve usar a interface de linha de comando (CLI) para exportar/importar um grupo de volumes para um storage array diferente.

Instruções detalhadas para migrar um grupo de volumes são fornecidas no "Base de dados de Conhecimento da NetApp".

### Desbloqueie unidades ao usar o gerenciamento de chaves externas

Se você configurou o gerenciamento de chaves externas e depois mover unidades habilitadas para segurança de um storage array para outro, será necessário atribuir novamente a chave de segurança ao novo storage array para obter acesso aos dados criptografados nas unidades.

#### Antes de começar

- Na matriz de origem (a matriz onde você está removendo as unidades), você exportou grupos de volume e removeu as unidades. No array de destino, você instalou novamente as unidades.

  A função Exportar/Importar não é suportada na interface de usuário do System Manager; você deve usar a interface de linha de comando (CLI) para exportar/importar um grupo de volumes para um storage array diferente.

  Instruções detalhadas para migrar um grupo de volumes são fornecidas no "Base de dados de Conhecimento da NetApp". Certifique-se de seguir as instruções apropriadas para arrays mais recentes gerenciados pelo System Manager ou para sistemas legados.

- O recurso Segurança da unidade deve estar ativado. Caso contrário, uma caixa de diálogo não é possível criar chave de segurança será aberta durante esta tarefa. Se necessário, entre em Contato com o fornecedor de armazenamento para obter instruções sobre como ativar o recurso Segurança da unidade.
- Você deve saber o endereço IP e o número da porta do servidor de gerenciamento de chaves.
- Você tem um arquivo de certificado de cliente assinado para os controladores do storage array e copiou esse arquivo para o host onde está acessando o System Manager. Um certificado de cliente valida os controladores do storage array, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP (Key Management Interoperability Protocol).
- Você deve recuperar um arquivo de certificado do servidor de gerenciamento de chaves e, em seguida, copiar esse arquivo para o host onde você está acessando o System Manager. Um certificado do servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, de modo que o storage array possa confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou servidor para o servidor de gerenciamento de chaves.

  Para obter mais informações sobre o certificado do servidor, consulte a documentação do servidor de gerenciamento de chaves.

#### Sobre esta tarefa

Quando você usa o gerenciamento de chaves externas, a chave de segurança é armazenada externamente em um servidor projetado para proteger chaves de segurança. Uma chave de segurança é uma cadeia de carateres que é compartilhada pelo controlador e unidades para acesso de leitura/gravação. Quando as unidades são fisicamente removidas da matriz e instaladas em outra, elas não podem operar até que você forneça a chave de segurança correta.

Você pode criar uma chave interna a partir da memória persistente do controlador ou uma chave externa de um servidor de gerenciamento de chaves. Este tópico descreve como desbloquear dados quando o gerenciamento de chaves *external* é usado. Se você usou o gerenciamento de chaves *internas*, "Desbloqueie unidades ao usar o gerenciamento de chaves internas"consulte . Se você estiver executando uma atualização de controladora e estiver trocando todos os controladores pelo hardware mais recente, siga etapas diferentes conforme descrito no centro de documentação e-Series e SANtricity, em "Desbloquear unidades".

Depois de reinstalar unidades habilitadas para segurança em outro array, esse array descobre as unidades e exibe uma condição de "precisa de atenção" junto com um status de "chave de segurança necessária". Para desbloquear os dados da unidade, importe o ficheiro da chave de segurança e introduza a frase-passe da chave. (Esta frase-passe não é a mesma que a senha do administrador da matriz de armazenamento.) Durante esse processo, você configura o storage array para usar um servidor de gerenciamento de chaves externo e, em seguida, a chave segura será acessível. É necessário fornecer informações de Contato do servidor para que a matriz de armazenamento se conete e recupere a chave de segurança.

Se outras unidades habilitadas para segurança estiverem instaladas no novo storage array, elas poderão usar uma chave de segurança diferente da que você está importando. Durante o processo de importação, a chave de segurança antiga é usada apenas para desbloquear os dados das unidades que você está instalando. Quando o processo de desbloqueio é bem-sucedido, as unidades recém-instaladas são recodificadas para a chave de segurança da matriz de armazenamento de destino.

**Passos**

1. Selecione **Definições › sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **criar chave externa**.
3. Conclua o assistente com as informações e certificados de conexão pré-requisito.
4. Clique em **Test Communication** para garantir o acesso ao servidor de gerenciamento de chaves externo.
5. Selecione **Unlock Secure Drives**.

   A caixa de diálogo desbloquear unidades seguras abre-se. Todas as unidades que exigem uma chave de segurança são mostradas na tabela.

6. **Opcional:** passe o Mouse sobre um número de unidade para ver a localização da unidade (número de prateleira e número de compartimento).
7. Clique em **Procurar** e selecione o arquivo de chave de segurança que corresponde à unidade que deseja desbloquear.

   O arquivo de chave selecionado aparece na caixa de diálogo.

8. Introduza a frase-passe associada a este ficheiro de chave.

   Os carateres inseridos são mascarados.

9. Clique em **Unlock**.

   Se a operação de desbloqueio for bem-sucedida, a caixa de diálogo exibe: "As unidades seguras associadas foram desbloqueadas."

**Resultados**

Quando todas as unidades estiverem bloqueadas e, em seguida, desbloqueadas, cada controlador na matriz de armazenamento será reiniciado. No entanto, se já houver algumas unidades desbloqueadas no storage de

armazenamento de destino, os controladores não serão reinicializados.

**Depois de terminar**

No array de destino (o array com as unidades recém-instaladas), agora você pode importar grupos de volume.

> A função Exportar/Importar não é suportada na interface de usuário do System Manager; você deve usar a interface de linha de comando (CLI) para exportar/importar um grupo de volumes para um storage array diferente.

Instruções detalhadas para migrar um grupo de volumes são fornecidas no "Base de dados de Conhecimento da NetApp".

## FAQs

**O que eu preciso saber antes de criar uma chave de segurança?**

Uma chave de segurança é compartilhada por controladores e unidades habilitadas para proteger dentro de um storage array. Se uma unidade habilitada para segurança for removida do storage array, a chave de segurança protegerá os dados contra acesso não autorizado.

Você pode criar e gerenciar chaves de segurança usando um dos seguintes métodos:

- Gerenciamento de chaves internas na memória persistente do controlador.
- Gerenciamento de chaves externas em um servidor de gerenciamento de chaves externo.

**Gerenciamento de chaves internas**

As chaves internas são mantidas e "ocultas" em um local não acessível na memória persistente do controlador. Antes de criar uma chave de segurança interna, você deve fazer o seguinte:

1. Instale unidades com capacidade segura no storage de armazenamento. Essas unidades podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).
2. Certifique-se de que a funcionalidade de Segurança da unidade está ativada. Se necessário, entre em Contato com o fornecedor de armazenamento para obter instruções sobre como ativar o recurso Segurança da unidade.

Em seguida, você pode criar uma chave de segurança interna, que envolve a definição de um identificador e uma frase-passe. O identificador é uma cadeia de carateres associada à chave de segurança e é armazenada no controlador e em todas as unidades associadas à chave. A frase-passe é usada para criptografar a chave de segurança para fins de backup. Quando terminar, a chave de segurança é armazenada no controlador num local não acessível. Em seguida, você pode criar grupos de volume ou pools habilitados para segurança ou habilitar a segurança em grupos de volumes e pools existentes.

**Gerenciamento de chaves externas**

As chaves externas são mantidas em um servidor de gerenciamento de chaves separado, usando um KMIP (Key Management Interoperability Protocol). Antes de criar uma chave de segurança externa, você deve fazer o seguinte:

1. Instale unidades com capacidade segura no storage de armazenamento. Essas unidades podem ser

unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).

2. Certifique-se de que a funcionalidade de Segurança da unidade está ativada. Se necessário, entre em Contato com o fornecedor de armazenamento para obter instruções sobre como ativar o recurso Segurança da unidade.
3. Obtenha um arquivo de certificado de cliente assinado. Um certificado de cliente valida os controladores do storage array, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP.
   a. Primeiro, você conclui e faz o download de uma solicitação de assinatura de certificado de cliente (CSR). Aceda ao **Definições › certificados › Gestão de chaves › CSR completo**.
   b. Em seguida, você solicita um certificado de cliente assinado de uma CA confiável pelo servidor de gerenciamento de chaves. (Você também pode criar e baixar um certificado de cliente do servidor de gerenciamento de chaves usando o arquivo CSR baixado.)
   c. Depois de ter um arquivo de certificado de cliente, copie esse arquivo para o host onde você está acessando o System Manager.
4. Recupere um arquivo de certificado do servidor de gerenciamento de chaves e copie esse arquivo para o host onde você está acessando o System Manager. Um certificado do servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, de modo que o storage array possa confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou servidor para o servidor de gerenciamento de chaves.

Em seguida, você pode criar uma chave externa, que envolve a definição do endereço IP do servidor de gerenciamento de chaves e o número da porta usada para comunicações KMIP. Durante esse processo, você também carrega arquivos de certificado. Quando terminar, o sistema se coneta ao servidor de gerenciamento de chaves com as credenciais inseridas. Em seguida, você pode criar grupos de volume ou pools habilitados para segurança ou habilitar a segurança em grupos de volumes e pools existentes.

**Por que eu preciso definir uma frase-passe?**

A frase-passe é usada para criptografar e descriptografar o arquivo de chave de segurança armazenado no cliente de gerenciamento local. Sem a frase-passe, a chave de segurança não pode ser descriptografada e usada para desbloquear dados de uma unidade habilitada para segurança se for reinstalada em outra matriz de armazenamento.

**Por que é importante Registrar informações de chave de segurança?**

Se você perder as informações da chave de segurança e não tiver um backup, poderá perder dados ao relocar unidades habilitadas ou atualizar um controlador. Você precisa da chave de segurança para desbloquear dados nas unidades.

Certifique-se de gravar o identificador da chave de segurança, a frase-passe associada e o local no host local onde o arquivo da chave de segurança foi salvo.

**O que eu preciso saber antes de fazer backup de uma chave de segurança?**

Se a chave de segurança original ficar corrompida e você não tiver um backup, perderá o acesso aos dados nas unidades se eles forem migrados de um storage array para outro.

Antes de fazer backup de uma chave de segurança, tenha em mente estas diretrizes:

- Certifique-se de que conhece o identificador da chave de segurança e a frase-passe do ficheiro de chave original.

> Somente chaves internas usam identificadores. Quando você criou o identificador, carateres adicionais foram gerados automaticamente e anexados a ambas as extremidades da cadeia de carateres do identificador. Os carateres gerados garantem que o identificador é exclusivo.

- Você cria uma nova frase-passe para o backup. Essa frase-passe não precisa corresponder à frase-passe usada quando a chave original foi criada ou alterada pela última vez. A frase-passe é aplicada apenas ao backup que você está criando.

> A frase-passe para o Drive Security não deve ser confundida com a senha de Administrador do storage. A frase-passe do Drive Security protege os backups de uma chave de segurança. A senha do administrador protege toda a matriz de armazenamento contra acesso não autorizado.

- O arquivo de chave de segurança de backup é baixado para o seu cliente de gerenciamento. O caminho para o arquivo baixado pode depender do local de download padrão do seu navegador. Certifique-se de fazer um Registro de onde as informações da chave de segurança estão armazenadas.

**O que eu preciso saber antes de desbloquear unidades seguras?**

## Para desbloquear os dados de uma unidade ativada de forma segura, tem de importar a respetiva chave de segurança.

Antes de desbloquear unidades seguras, tenha em mente as seguintes diretrizes:

- O storage array já deve ter uma chave de segurança. As unidades migradas serão recodificadas para o storage de armazenamento de destino.
- Para as unidades que você está migrando, você deve saber o identificador da chave de segurança e a frase-passe que corresponde ao arquivo da chave de segurança.
- O arquivo da chave de segurança deve estar disponível no cliente de gerenciamento (o sistema com um navegador usado para acessar o System Manager).
- Se estiver a repor uma unidade NVMe bloqueada, tem de introduzir a ID de segurança da unidade. Para localizar a ID de segurança, você deve remover fisicamente a unidade e encontrar a cadeia PSID (máximo de 32 carateres) na etiqueta da unidade. Certifique-se de que a unidade é reinstalada antes de iniciar a operação.

**O que é acessibilidade de leitura/escrita?**

## A janela Configurações da unidade inclui informações sobre os atributos de segurança da unidade. "Leitura/gravação acessível" é um dos atributos que é exibido se os dados de uma unidade foram bloqueados.

Para exibir os atributos de segurança da unidade, vá para a página hardware. Selecione uma unidade, clique em **View settings** e, em seguida, clique em **Show more settings** (Mostrar mais definições). Na parte inferior da página, o valor do atributo leitura/gravação acessível é **Sim** quando a unidade é desbloqueada. O valor do atributo leitura/gravação acessível é **não, chave de segurança inválida** quando a unidade está bloqueada.

Pode desbloquear uma unidade segura importando uma chave de segurança (aceda ao **Definições › sistema › desbloquear unidades seguras**).

**O que eu preciso saber sobre a validação da chave de segurança?**

Depois de criar uma chave de segurança, você deve validar o arquivo de chave para se certificar de que ele não está corrompido.

Se a validação falhar, faça o seguinte:

- Se o identificador da chave de segurança não corresponder ao identificador no controlador, localize o ficheiro de chave de segurança correto e, em seguida, tente a validação novamente.
- Se o controlador não conseguir desencriptar a chave de segurança para validação, poderá ter introduzido incorretamente a frase-passe. Verifique novamente a frase-passe, volte a introduzi-la, se necessário, e tente a validação novamente. Se a mensagem de erro aparecer novamente, selecione uma cópia de segurança do ficheiro de chave (se disponível) e volte a tentar a validação.
- Se você ainda não conseguir validar a chave de segurança, o arquivo original pode estar corrompido. Crie um novo backup da chave e valide essa cópia.

**Qual é a diferença entre a chave de segurança interna e o gerenciamento de chaves de segurança externas?**

Ao implementar o recurso Segurança da unidade, você pode usar uma chave de segurança interna ou uma chave de segurança externa para bloquear dados quando uma unidade habilitada for removida do storage de armazenamento.

Uma chave de segurança é uma cadeia de carateres, que é compartilhada entre as unidades e controladores habilitados para segurança em um storage array. As chaves internas são mantidas na memória persistente do controlador. As chaves externas são mantidas em um servidor de gerenciamento de chaves separado, usando um KMIP (Key Management Interoperability Protocol).

# Gerenciamento de acesso

## Visão geral do Gerenciamento de Acesso

O Gerenciamento de Acesso é um método para estabelecer a autenticação do usuário no System Manager.

**Quais métodos de autenticação estão disponíveis?**

Os métodos de autenticação incluem RBAC (controle de acesso baseado em função), Directory Services e Security Assertion Markup Language (SAML):

- * Funções de usuário RBAC/local* — a autenticação é gerenciada por meio de recursos RBAC aplicados no storage array. As funções de usuário local incluem perfis de usuário predefinidos e funções com permissões de acesso específicas.
- **Serviços de diretório** — a autenticação é gerenciada por meio de um servidor LDAP (Lightweight Directory Access Protocol) e Serviços de diretório, como o ative Directory da Microsoft.
- **SAML** — a autenticação é gerenciada por meio de um Provedor de identidade (IDP) usando SAML 2,0.

Saiba mais:

- "Como o Gerenciamento de Acesso funciona"
- "Terminologia de Gerenciamento de Acesso"
- "Permissões para funções mapeadas"
- "Funções de utilizador local"
- "Serviços de diretório"
- "SAML"

#### Como faço para configurar a autenticação?

O storage array é pré-configurado para usar funções de usuário locais, que são uma implementação das funcionalidades do RBAC. Se você quiser configurar um método diferente, vá para **Configurações › Gerenciamento de Acesso**.

Saiba mais:

- "Adicione um servidor de diretório LDAP"
- "Configurar SAML"

#### Informações relacionadas

Saiba mais sobre tarefas relacionadas ao gerenciamento de acesso:

- "Alterar senhas"
- "Exibir atividade do log de auditoria"
- "Configure o servidor syslog para logs de auditoria"

## Conceitos

#### Como o Gerenciamento de Acesso funciona

### O Gerenciamento de Acesso é um método para estabelecer a autenticação do usuário no System Manager.

A configuração e a autenticação do usuário funcionam da seguinte forma:

1. Um administrador faz login no System Manager com um perfil de usuário que inclui permissões de administrador de segurança.

   > Para iniciar sessão pela primeira vez, o nome de utilizador `admin` é apresentado automaticamente e não pode ser alterado. O `admin` utilizador tem acesso total a todas as funções do sistema.

2. O administrador navega para acessar o Gerenciamento na interface do usuário. O storage array é pré-configurado para usar funções de usuário locais, que são uma implementação dos recursos RBAC (controle de acesso baseado em função).
3. O administrador configura um ou mais dos seguintes métodos de autenticação:

- **Funções de usuário local** — a autenticação é gerenciada por meio de recursos RBAC aplicados no storage array. As funções de usuário local incluem perfis de usuário predefinidos e funções com permissões de acesso específicas. Os administradores podem usar essas funções de usuário local como o único método de autenticação ou usá-las em combinação com um serviço de diretório. Nenhuma configuração é necessária, além de definir senhas para usuários.
- **Serviços de diretório** — a autenticação é gerenciada por meio de um servidor LDAP (Lightweight Directory Access Protocol) e serviço de diretório, como o ative Directory da Microsoft. Um administrador se coneta ao servidor LDAP e, em seguida, mapeia os usuários LDAP para as funções de usuário local incorporadas na matriz de armazenamento.
- **SAML** — a autenticação é gerenciada por meio de um Provedor de identidade (IDP) usando a Security Assertion Markup Language (SAML) 2,0. Um administrador estabelece a comunicação entre o sistema IDP e o storage array e, em seguida, mapeia os usuários IDP para as funções de usuário local incorporadas no storage array.

4. O administrador fornece aos usuários credenciais de login para o System Manager.
5. Os usuários fazem login no sistema inserindo suas credenciais.

> Se a autenticação for gerenciada com SAML e um SSO (logon único), o sistema poderá ignorar a caixa de diálogo de login do System Manager.

Durante o início de sessão, o sistema executa as seguintes tarefas em segundo plano:

- Autentica o nome de utilizador e a palavra-passe na conta de utilizador.
- Determina as permissões do usuário com base nas funções atribuídas.
- Fornece ao usuário acesso a tarefas na interface do usuário.
- Exibe o nome de usuário no canto superior direito da interface.

#### Tarefas disponíveis no System Manager

O acesso a tarefas depende das funções atribuídas de um usuário, que incluem o seguinte:

- **Storage admin** — Acesso completo de leitura/gravação aos objetos de armazenamento (por exemplo, volumes e pools de discos), mas sem acesso à configuração de segurança.
- **Admin de segurança** — Acesso à configuração de segurança em Gerenciamento de acesso, gerenciamento de certificados, gerenciamento de log de auditoria e a capacidade de ativar ou desativar a interface de gerenciamento legada (símbolo).
- **Support admin** — Acesso a todos os recursos de hardware na matriz de armazenamento, dados de falha, eventos mel e atualizações de firmware do controlador. Sem acesso a objetos de armazenamento ou à configuração de segurança.
- **Monitor** — Acesso somente leitura a todos os objetos de armazenamento, mas sem acesso à configuração de segurança.

Uma tarefa indisponível está a cinzento ou não é apresentada na interface do utilizador. Por exemplo, um usuário com a função Monitor pode exibir todas as informações sobre volumes, mas não pode acessar funções para modificar esse volume. As guias para recursos como **Serviços de cópia** e **Adicionar à carga de trabalho** ficarão esmaecidas; somente **Exibir/Editar configurações** está disponível.

#### Limitações no Unified Manager e no Storage Manager

Se o SAML estiver configurado para um storage array, os usuários não poderão descobrir ou gerenciar o storage desse array a partir do Unified Manager ou das interfaces herdadas do Storage Manager.

Quando as funções de usuário local e os serviços de diretório são configurados, os usuários devem inserir credenciais antes de executar qualquer uma das seguintes funções:

- Renomeando o storage array
- Atualizando o firmware da controladora
- Carregando uma configuração de storage array
- Executando um script
- Tentar executar uma operação ativa quando uma sessão não utilizada tiver terminado o tempo limite

**Terminologia de Gerenciamento de Acesso**

Saiba como os termos do Gerenciamento de Acesso se aplicam ao storage array.

| Prazo | Descrição |
| --- | --- |
| Token de acesso | Os tokens de acesso são usados para autenticar com a API REST ou interface de linha de comando (CLI) no lugar de um nome de usuário e senha. Os tokens são associados a um usuário específico (incluindo usuários LDAP) e incluem um conjunto de permissões e uma expiração. |
| Ative Directory | O ative Directory (AD) é um serviço de diretório da Microsoft que usa LDAP para redes de domínio do Windows. |
| Encadernação | As operações de vinculação são usadas para autenticar clientes no servidor de diretórios. A vinculação geralmente requer credenciais de conta e senha, mas alguns servidores permitem operações anônimas de vinculação. |
| CA | Uma autoridade de certificação (CA) é uma entidade confiável que emite documentos eletrônicos, chamados certificados digitais, para segurança na Internet. Esses certificados identificam proprietários de sites, o que permite conexões seguras entre clientes e servidores. |
| Certificado | Um certificado identifica o proprietário de um site para fins de segurança, o que impede que atacantes personifiquem o site. O certificado contém informações sobre o proprietário do site e a identidade da entidade confiável que certifica (assina) essas informações. |
| IDP | Um Provedor de identidade (IDP) é um sistema externo usado para solicitar credenciais de um usuário e para determinar se esse usuário foi autenticado com êxito. O IDP pode ser configurado para fornecer autenticação multifator e usar qualquer banco de dados de usuários, como o ative Directory. Sua equipe de segurança é responsável por manter o IDP. |
| LDAP | O LDAP (Lightweight Directory Access Protocol) é um protocolo de aplicação para aceder e manter serviços de informação de diretório distribuído. Este protocolo permite que vários aplicativos e serviços diferentes se conetem ao servidor LDAP para validar usuários. |

| Prazo | Descrição |
| --- | --- |
| RBAC | O controle de acesso baseado em função (RBAC) é um método de regular o acesso a recursos de computador ou rede com base nas funções de usuários individuais. Os controles RBAC são aplicados no storage array e incluem funções predefinidas. |
| SAML | Security Assertion Markup Language (SAML) é um padrão baseado em XML para autenticação e autorização entre duas entidades. O SAML permite a autenticação multifator, na qual os usuários devem fornecer dois ou mais itens para provar sua identidade (por exemplo, uma senha e uma impressão digital). O recurso SAML incorporado do storage array é compatível com SAML2,0 para afirmação, autenticação e autorização de identidade. |
| SP | Um provedor de serviços (SP) é um sistema que controla a autenticação e o acesso do usuário. Quando o Gerenciamento de Acesso é configurado com SAML, o storage array atua como o provedor de serviços para solicitar autenticação do provedor de identidade. |
| SSO | Logon único (SSO) é um serviço de autenticação que permite que um conjunto de credenciais de login acesse vários aplicativos. |

#### Permissões para funções mapeadas

Os recursos RBAC (controle de acesso baseado em função) aplicados no storage array incluem perfis de usuário predefinidos com uma ou mais funções mapeadas. Cada função inclui permissões para acessar tarefas no System Manager.

Os perfis de utilizador e as funções mapeadas são acessíveis a partir do **Definições › Gestão de acessos › funções de utilizador local** na interface de utilizador de qualquer Gestor de sistema.

As funções fornecem acesso do usuário a tarefas, como segue:

- **Storage admin** — Acesso completo de leitura/gravação aos objetos de armazenamento (por exemplo, volumes e pools de discos), mas sem acesso à configuração de segurança.
- **Admin de segurança** — Acesso à configuração de segurança em Gerenciamento de acesso, gerenciamento de certificados, gerenciamento de log de auditoria e a capacidade de ativar ou desativar a interface de gerenciamento legada (símbolo).
- **Support admin** — Acesso a todos os recursos de hardware na matriz de armazenamento, dados de falha, eventos mel e atualizações de firmware do controlador. Sem acesso a objetos de armazenamento ou à configuração de segurança.
- **Monitor** — Acesso somente leitura a todos os objetos de armazenamento, mas sem acesso à configuração de segurança.

Se um usuário não tiver permissões para uma determinada tarefa, essa tarefa será exibida em cinza ou não será exibida na interface do usuário.

#### Gerenciamento de acesso com funções de usuário local

Para Gerenciamento de acesso, os administradores podem usar os recursos RBAC

(controle de acesso baseado em função) aplicados no storage array. Esses recursos são chamados de "funções de usuário local".

#### Fluxo de trabalho de configuração

As funções de usuário local são pré-configuradas para o storage array. Para usar funções de usuário local para autenticação, os administradores podem fazer o seguinte:

1. Um administrador faz login no System Manager com um perfil de usuário que inclui permissões de administrador de segurança.

   O `admin` utilizador tem acesso total a todas as funções do sistema.

2. Um administrador analisa os perfis de usuário, que são predefinidos e não podem ser modificados.
3. Opcionalmente, o administrador atribui novas senhas para cada perfil de usuário.
4. Os usuários fazem login no sistema com suas credenciais atribuídas.

#### Gerenciamento

Ao usar apenas funções de usuário local para autenticação, os administradores podem executar as seguintes tarefas de gerenciamento:

- Alterar senhas.
- Defina um comprimento mínimo para senhas.
- Permitir que os usuários façam login sem senhas.

### Gerenciamento de acesso com serviços de diretório

Para Gerenciamento de Acesso, os administradores podem usar um servidor LDAP (Lightweight Directory Access Protocol) e um serviço de diretório, como o ative Directory da Microsoft.

#### Fluxo de trabalho de configuração

Se um servidor LDAP e um serviço de diretório são usados na rede, a configuração funciona da seguinte forma:

1. Um administrador faz login no System Manager com um perfil de usuário que inclui permissões de administrador de segurança.

   O `admin` utilizador tem acesso total a todas as funções do sistema.

2. O administrador insere as configurações do servidor LDAP. As configurações incluem o nome do domínio, URL e informações da conta Bind.
3. Se o servidor LDAP utilizar um protocolo seguro (LDAPS), o administrador carrega uma cadeia de certificados de autoridade de certificação (CA) para autenticação entre o servidor LDAP e a matriz de armazenamento.
4. Depois que a conexão com o servidor é estabelecida, o administrador mapeia os grupos de usuários para as funções do storage array. Essas funções são predefinidas e não podem ser modificadas.

5. O administrador testa a conexão entre o servidor LDAP e o storage array.
6. Os usuários fazem login no sistema com suas credenciais LDAP/Directory Services atribuídas.

#### Gerenciamento

Ao usar serviços de diretório para autenticação, os administradores podem executar as seguintes tarefas de gerenciamento:

- Adicione um servidor de diretório.
- Editar definições do servidor de diretório.
- Mapeie usuários LDAP para funções de usuário locais.
- Remova um servidor de diretório.

### Gerenciamento de acesso com SAML

Para Gerenciamento de Acesso, os administradores podem usar os recursos de Security Assertion Markup Language (SAML) 2,0 incorporados no array.

#### Fluxo de trabalho de configuração

A configuração SAML funciona da seguinte forma:

1. Um administrador faz login no System Manager com um perfil de usuário que inclui permissões de administrador de segurança.

   O `admin` utilizador tem acesso total a todas as funções do System Manager.

2. O administrador vai para a guia **SAML** em Gerenciamento de Acesso.
3. Um administrador configura as comunicações com o Provedor de identidade (IDP). Um IDP é um sistema externo usado para solicitar credenciais de um usuário e determinar se o usuário foi autenticado com êxito. Para configurar as comunicações com a matriz de armazenamento, o administrador transfere o ficheiro de metadados IDP do sistema IDP e, em seguida, utiliza o System Manager para carregar o ficheiro para a matriz de armazenamento.
4. Um administrador estabelece uma relação de confiança entre o Fornecedor de Serviços e o IDP. Um Fornecedor de Serviços controla a autorização do utilizador; neste caso, o controlador na matriz de armazenamento atua como o Fornecedor de Serviços. Para configurar comunicações, o administrador usa o System Manager para exportar um arquivo de metadados do provedor de serviços para cada controlador. A partir do sistema IDP, o administrador então importa esses arquivos de metadados para o IDP.

   Os administradores também devem certificar-se de que o IDP suporta a capacidade de retornar um ID de nome na autenticação.

5. O administrador mapeia as funções do storage array para atributos de usuário definidos no IDP. Para fazer isso, o administrador usa o System Manager para criar os mapeamentos.
6. O administrador testa o login SSO para o URL do IDP. Este teste garante que a matriz de armazenamento e o IDP possam se comunicar.

Uma vez que o SAML está ativado, você *não pode* desabilitá-lo através da interface do usuário, nem pode editar as configurações de IDP. Se você precisar desativar ou editar a configuração SAML, entre em Contato com o suporte técnico para obter assistência.

7. No System Manager, o administrador habilita o SAML para o storage array.
8. Os usuários fazem login no sistema com suas credenciais SSO.

#### Gerenciamento

Ao usar o SAML para autenticação, os administradores podem executar as seguintes tarefas de gerenciamento:

- Modificar ou criar novos mapeamentos de função
- Exportar ficheiros do fornecedor de serviços

#### Restrições de acesso

Quando o SAML está ativado, os usuários não podem descobrir ou gerenciar o storage desse array a partir do Unified Manager ou da interface herdada do Storage Manager.

Além disso, os seguintes clientes não podem acessar os serviços e recursos do storage array:

- Janela de gerenciamento empresarial (EMW)
- Interface de linha de comando (CLI)
- Clientes de Software Developer Kits (SDK)
- Clientes na banda
- Clientes API REST de Autenticação básica HTTP
- Faça login usando o endpoint padrão da API REST

### Acesse tokens

Os tokens de acesso fornecem um método de autenticação com a API REST ou interface de linha de comando (CLI), sem expor nomes de usuário e senhas. Um token é associado a um usuário específico (incluindo usuários LDAP) e inclui um conjunto de permissões e uma expiração.

#### Acesso a token web SAML e JSON

Por padrão, um sistema com SAML habilitado não permite o acesso a ferramentas de linha de comando tradicionais. A API REST e a CLI efetivamente tornam-se inoperáveis porque o fluxo de trabalho MFA requer um redirecionamento para um servidor do Identity Provider para autenticação. Portanto, você deve gerar tokens no System Manager, o que exige que um usuário seja autenticado por meio de MFA.

Não é necessário ter o SAML habilitado para usar tokens da Web, mas o SAML é recomendado para o mais alto nível de segurança.

#### Fluxo de trabalho para criar e usar tokens

1. Crie um token no System Manager e determine sua expiração.

2. Copie o texto do token para a área de transferência ou faça o download em um arquivo e salve o texto do token em um local seguro.
3. Use o token da seguinte forma:
   - **API REST**: Para usar um token em uma solicitação de API REST, adicione um cabeçalho HTTP às suas solicitações. Por exemplo:
     `Authorization: Bearer <access-token-value>`
   - **CLI segura**: Para usar um token na CLI, adicione o valor do token na linha de comando ou use o caminho para um arquivo contendo o valor do token. Por exemplo:
     - Valor do token na linha de comando: `-t access-token-value`
     - Caminho para um arquivo contendo o valor do token: `-T access-token-file`

Saiba mais:

- "Crie tokens de acesso"
- "Editar tokens de acesso"
- "Revogar tokens de acesso"

## Use funções de usuário local

### Ver funções de utilizador locais

Na guia funções de usuário local, você pode exibir os mapeamentos dos perfis de usuário para as funções padrão. Esses mapeamentos fazem parte do RBAC (controles de acesso baseados em função) aplicado no storage array.

#### Antes de começar

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.

#### Sobre esta tarefa

Os perfis de usuário e mapeamentos não podem ser alterados. Apenas as senhas podem ser modificadas.

#### Passos

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **funções de usuário local**.

   Os perfis de utilizador são apresentados na tabela:

   - * Admin root* (admin) — Super administrador que tem acesso a todas as funções do sistema. Este perfil de usuário inclui todas as funções.
   - **Storage admin** (armazenamento) — o administrador responsável por todo o provisionamento de armazenamento. Esse perfil de usuário inclui as seguintes funções: Administrador de storage, administrador de suporte e monitor.
   - **Security admin** (security) — o usuário responsável pela configuração de segurança, incluindo gerenciamento de acesso, gerenciamento de certificados e funções de unidade habilitadas para segurança. Este perfil de usuário inclui as seguintes funções: Admin de segurança e Monitor.
   - **Support admin** (suporte) — o usuário responsável por recursos de hardware, dados de falha e

atualizações de firmware. Este perfil de usuário inclui as seguintes funções: Admin de suporte e Monitor.

- **Monitor** (monitor) — Um usuário com acesso somente leitura ao sistema. Este perfil de usuário inclui apenas a função Monitor.

### Alterar senhas

Você pode alterar as senhas de usuário para cada perfil de usuário no Gerenciamento de acesso.

#### Antes de começar

- Você deve estar logado como administrador local, o que inclui permissões de administrador raiz.
- Você deve saber a senha do administrador local.

#### Sobre esta tarefa

Tenha em mente estas diretrizes ao escolher uma senha:

- Quaisquer novas senhas de usuário local devem atender ou exceder a configuração atual para uma senha mínima (em Configurações de visualização/edição).
- As senhas diferenciam maiúsculas de minúsculas.
- Os espaços de saída não são removidos das senhas quando são definidos. Tenha cuidado para incluir espaços se eles foram incluídos na senha.
- Para maior segurança, use pelo menos 15 carateres alfanuméricos e altere a senha com frequência.

> Alterar a senha no System Manager também a altera na interface de linha de comando (CLI). Além disso, as alterações de senha fazem com que a sessão ativa do usuário seja encerrada.

#### Passos

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **funções de usuário local**.
3. Selecione um usuário na tabela.

   O botão alterar senha fica disponível.

4. Selecione **alterar palavra-passe**.

   A caixa de diálogo alterar senha será exibida.

5. Se não estiver definido um comprimento mínimo de palavra-passe para palavras-passe de utilizador local, pode marcar a caixa para exigir que o utilizador selecionado introduza uma palavra-passe para aceder à matriz de armazenamento e, em seguida, pode introduzir a nova palavra-passe para o utilizador selecionado.
6. Introduza a palavra-passe do administrador local e, em seguida, clique em **alterar**.

#### Resultados

Se o usuário estiver conetado no momento, a alteração da senha fará com que a sessão ativa do usuário seja encerrada.

#### Altere as definições de palavra-passe do utilizador local

Você pode definir o comprimento mínimo necessário para todas as senhas de usuário locais novas ou atualizadas na matriz de armazenamento. Você também pode permitir que os usuários locais acessem o storage array sem inserir uma senha.

**Antes de começar**

Você deve estar logado como administrador local, o que inclui permissões de administrador raiz.

**Sobre esta tarefa**

Tenha estas diretrizes em mente ao definir o comprimento mínimo para senhas de usuário local:

- A definição de alterações não afetará as palavras-passe de utilizador locais existentes.
- A definição de comprimento mínimo necessário para palavras-passe de utilizador local tem de ter entre 0 e 30 carateres.
- Quaisquer novas senhas de usuário local devem atender ou exceder a configuração de comprimento mínimo atual.
- Não defina um tamanho mínimo para a senha se você quiser que os usuários locais acessem o storage array sem digitar uma senha.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **funções de usuário local**.
3. Selecione o botão **View/Edit Settings** (Ver/Editar definições).

   A caixa de diálogo Configurações de senha do usuário local é aberta.

4. Execute um dos seguintes procedimentos:
   - Para permitir que os usuários locais acessem o storage array *sem* inserir uma senha, desmarque a caixa de seleção "exigir que todas as senhas de usuário local sejam pelo menos".
   - Para definir um comprimento mínimo de palavra-passe para todas as palavras-passe de utilizador local, marque a caixa de verificação "exigir que todas as palavras-passe de utilizador local sejam pelo menos" e, em seguida, utilize a caixa de seleção para definir o comprimento mínimo necessário para todas as palavras-passe de utilizador local.

     Todas as novas senhas de usuário local devem atender ou exceder a configuração atual.

5. Clique em **Salvar**.

## Use os serviços de diretório

#### Adicione um servidor de diretório LDAP

Para configurar a autenticação para o Gerenciamento de Acesso, você pode estabelecer comunicações entre o storage array e um servidor LDAP e mapear os grupos de usuários LDAP para as funções predefinidas do array.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança.

Caso contrário, as funções de Gerenciamento de Acesso não aparecem.

- Os grupos de usuários devem ser definidos em seu serviço de diretório.
- As credenciais do servidor LDAP devem estar disponíveis, incluindo o nome de domínio, o URL do servidor e, opcionalmente, o nome de usuário e a senha da conta BIND.
- Para servidores LDAPS que usam um protocolo seguro, a cadeia de certificados do servidor LDAP deve ser instalada na sua máquina local.

**Sobre esta tarefa**

Adicionar um servidor de diretório é um processo de duas etapas. Primeiro você insere o nome de domínio e URL. Se o servidor usar um protocolo seguro, você também deve carregar um certificado de CA para autenticação se ele for assinado por uma autoridade de assinatura não padrão. Se tiver credenciais para uma conta BIND, também poderá introduzir o nome da conta de utilizador e a palavra-passe. Em seguida, você mapeia os grupos de usuários do servidor LDAP para as funções predefinidas do storage array.

> Durante o procedimento para adicionar um servidor LDAP, a interface de gerenciamento herdada será desativada. A interface de gerenciamento legada (símbolo) é um método de comunicação entre o storage array e o cliente de gerenciamento. Quando desabilitado, o storage array e o cliente de gerenciamento usam um método de comunicação mais seguro (API REST sobre https).

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Na guia Serviços de diretório, selecione **Adicionar servidor de diretório**.

   A caixa de diálogo Adicionar servidor de diretório é aberta.

3. Na guia Configurações do servidor , insira as credenciais do servidor LDAP.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| **Configurações de configuração** | Domínio(s) |
| Introduza o nome de domínio do servidor LDAP. Para vários domínios, insira os domínios em uma lista separada por vírgulas. O nome de domínio é usado no login (*username__domain*) para especificar em qual servidor de diretório se autenticar. | URL do servidor |
| Insira o URL para acessar o servidor LDAP na forma `ldap[s]://**host**:*port*` de . | Carregar certificado (opcional) |
| Este campo aparece apenas se um protocolo LDAPS for especificado no campo URL do servidor acima.<br><br>Clique em **Procurar** e selecione um certificado de CA para carregar. Este é o certificado confiável ou cadeia de certificados usada para autenticar o servidor LDAP. | Vincular conta (opcional) |

| Definição | Descrição |
| --- | --- |
| Insira uma conta de usuário somente leitura para consultas de pesquisa no servidor LDAP e para pesquisar nos grupos. Introduza o nome da conta num formato de tipo LDAP. Por exemplo, se o usuário bind é chamado de "bindacct", então você pode digitar um valor como "bindacct,cpoc,DC_local". | Vincular senha (opcional) |
| Este campo é exibido quando você insere uma conta BIND acima.<br><br>Introduza a palavra-passe para a conta vincular. | Teste a conexão do servidor antes de adicionar |

| Definição | Descrição |
| --- | --- |
| Selecione esta caixa de verificação se pretender certificar-se de que a matriz de armazenamento pode comunicar com a configuração do servidor LDAP introduzida. O teste ocorre depois de clicar em **Add** na parte inferior da caixa de diálogo. Se esta caixa de verificação estiver selecionada e o teste falhar, a configuração não será adicionada. Você deve resolver o erro ou desmarcar a caixa de seleção para ignorar o teste e adicionar a configuração. | **Configurações de privilégio** |
| Pesquisar DN base | Introduza o contexto LDAP para procurar utilizadores, normalmente na forma `CN=Users, DC=cpoc, DC=local` de . |
| Atributo de nome de usuário | Insira o atributo que está vinculado ao ID do usuário para autenticação. Por exemplo `sAMAccountName`: . |
| Atributo(s) de grupo | Insira uma lista de atributos de grupo no usuário, que é usada para mapeamento de grupo para função. Por exemplo `memberOf, managedObjects`: . |

4. Clique na guia **Mapeamento de função**.
5. Atribua grupos LDAP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| **Mapeamentos** | DN do grupo |
| Especifique o nome distinto do grupo (DN) para o grupo de usuários LDAP a ser mapeado. Expressões regulares são suportadas. Esses carateres especiais de expressão regular devem ser escapados com uma barra invertida (\) se eles não forem parte de um padrão de expressão regular | Funções |

A função Monitor é necessária para todos os usuários, incluindo o administrador. O System Manager não funcionará corretamente para nenhum usuário sem a função Monitor presente.

6. Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.
7. Quando terminar com os mapeamentos, clique em **Add**.

   O sistema executa uma validação, certificando-se de que a matriz de armazenamento e o servidor LDAP possam se comunicar. Se for apresentada uma mensagem de erro, assinale as credenciais introduzidas na caixa de diálogo e volte a introduzir as informações, se necessário.

### Edite as configurações do servidor de diretório e mapeamentos de função

Se você configurou anteriormente um servidor de diretório em Gerenciamento de Acesso, poderá alterar suas configurações a qualquer momento. As configurações incluem as informações de conexão do servidor e os mapeamentos de grupo para função.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- Um servidor de diretório deve ser definido.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.

2. Selecione a guia **Serviços de diretório**.
3. Se mais de um servidor estiver definido, selecione o servidor que deseja editar na tabela.
4. Selecione **Exibir/Editar configurações**.

   A caixa de diálogo Configurações do servidor de diretório é aberta.

5. Na guia Configurações do servidor, altere as configurações desejadas.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| **Configurações de configuração** | Domínio(s) |
| O(s) nome(s) de domínio do(s) servidor(es) LDAP. Para vários domínios, insira os domínios em uma lista separada por vírgulas. O nome de domínio é usado no login (*username__domain*) para especificar em qual servidor de diretório se autenticar. | URL do servidor |
| O URL para acessar o servidor LDAP na forma `ldap[s]://host:port` de . | Vincular conta (opcional) |
| A conta de usuário somente leitura para consultas de pesquisa no servidor LDAP e para pesquisa dentro dos grupos. | Vincular senha (opcional) |
| A senha para a conta vincular. (Este campo é exibido quando uma conta BIND é inserida.) | Teste a conexão do servidor antes de salvar |

| Definição | Descrição |
| --- | --- |
| Verifica se a matriz de armazenamento pode comunicar com a configuração do servidor LDAP. O teste ocorre depois de clicar em **Salvar** na parte inferior da caixa de diálogo. Se esta caixa de verificação estiver selecionada e o teste falhar, a configuração não será alterada. Você deve resolver o erro ou desmarcar a caixa de seleção para ignorar o teste e reeditar a configuração. | • Configurações de privilégio* |
| Pesquisar DN base | O contexto LDAP para procurar usuários, normalmente na forma `CN=Users, DC=cpoc, DC=local` de . |
| Atributo de nome de usuário | O atributo que está vinculado ao ID do usuário para autenticação. Por exemplo `sAMAccountName`: . |
| Atributo(s) de grupo | Uma lista de atributos de grupo no usuário, que é usada para mapeamento de grupo para função. Por exemplo `memberOf`, `managedObjects`: . |

6. Na guia Mapeamento de funções, altere o mapeamento desejado.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| **Mapeamentos** | DN do grupo |
| O nome de domínio para o grupo de utilizadores LDAP a ser mapeado. Expressões regulares são suportadas. Esses carateres especiais de expressão regular devem ser escapados com uma barra invertida (\) se eles não forem parte de um padrão de expressão regular | Funções |

A função Monitor é necessária para todos os usuários, incluindo o administrador. O System Manager não funcionará corretamente para nenhum usuário sem a função Monitor presente.

7. Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.
8. Clique em **Salvar**.

**Resultados**

Depois de concluir esta tarefa, todas as sessões ativas do utilizador são encerradas. Apenas a sessão de utilizador atual é mantida.

### Remova o servidor de diretório

Para interromper a conexão entre um servidor de diretório e o storage array, você pode remover as informações do servidor da página Gerenciamento de acesso. Talvez você queira executar essa tarefa se tiver configurado um novo servidor e, em seguida, desejar remover o antigo.

**Antes de começar**

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.

**Sobre esta tarefa**

Depois de concluir esta tarefa, todas as sessões ativas do utilizador são encerradas. Apenas a sessão de utilizador atual é mantida.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **Serviços de diretório**.
3. Na lista, selecione o servidor de diretório que deseja excluir.
4. Clique em **Remover**.

   A caixa de diálogo Remover servidor de diretório é aberta.

5. Digite `remove` o campo e clique em **Remover**.

   As configurações do servidor de diretório, as configurações de privilégio e os mapeamentos de função são removidos. Os usuários não podem mais fazer login com credenciais deste servidor.

## Use SAML

### Configurar SAML

Para configurar a autenticação para o Access Management, você pode usar os recursos de Security Assertion Markup Language (SAML) incorporados no storage array. Esta configuração estabelece uma conexão entre um Provedor de identidade e o Provedor de armazenamento.

#### Antes de começar

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- Você deve saber o endereço IP ou o nome de domínio de cada controlador na matriz de armazenamento.
- Um administrador de IDP configurou um sistema de IDP.
- Um administrador de IDP garantiu que o IDP suporta a capacidade de retornar um ID de nome na autenticação.
- Um administrador garantiu que o servidor IDP e os relógios do controlador são sincronizados (através de um servidor NTP ou ajustando as definições do relógio do controlador).
- Um arquivo de metadados IDP é baixado do sistema IDP e está disponível no sistema local usado para acessar o System Manager.

#### Sobre esta tarefa

Um Provedor de identidade (IDP) é um sistema externo usado para solicitar credenciais de um usuário e para determinar se esse usuário foi autenticado com êxito. O IDP pode ser configurado para fornecer autenticação multifator e usar qualquer banco de dados de usuários, como o ative Directory. Sua equipe de segurança é responsável por manter o IDP. Um provedor de serviços (SP) é um sistema que controla a autenticação e o acesso do usuário. Quando o Gerenciamento de Acesso é configurado com SAML, o storage array atua como o provedor de serviços para solicitar autenticação do provedor de identidade. Para estabelecer uma conexão entre o IDP e o storage array, você compartilha arquivos de metadados entre essas duas entidades. Em seguida, você mapeia as entidades de usuário IDP para as funções de storage array. E, finalmente, você testa os logins de conexão e SSO antes de ativar o SAML.

> **SAML e Serviços de diretório**. Se você ativar o SAML quando os Serviços de diretório estiverem configurados como o método de autenticação, o SAML substituirá os Serviços de diretório no System Manager. Se você desabilitar o SAML mais tarde, a configuração dos Serviços de diretório retornará à configuração anterior.

**Edição e desativação.** Uma vez que o SAML está ativado, você *não pode* desabilitá-lo através da interface do usuário, nem pode editar as configurações de IDP. Se você precisar desativar ou editar a configuração SAML, entre em Contato com o suporte técnico para obter assistência.

Configurar a autenticação SAML é um procedimento de várias etapas.

#### Passo 1: Faça o upload do arquivo de metadados IDP

Para fornecer ao storage array informações de conexão IDP, você importa metadados IDP para o System Manager. O sistema de IDP precisa desses metadados para redirecionar as solicitações de autenticação para o URL correto e para validar as respostas recebidas. Você só precisa fazer o upload de um arquivo de metadados para o storage array, mesmo que haja dois controladores.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **SAML**.

   A página exibe uma visão geral das etapas de configuração.

3. Clique no link **Import Identity Provider (IDP) file**.

   A caixa de diálogo Importar arquivo do provedor de identidade será aberta.

4. Clique em **Procurar** para selecionar e carregar o ficheiro de metadados IDP copiado para o sistema local.

   Depois de selecionar o ficheiro, é apresentado o ID da entidade IDP.

5. Clique em **Importar**.

#### Passo 2: Exportar arquivos do provedor de serviços

Para estabelecer uma relação de confiança entre o IDP e o storage array, você importa os metadados do provedor de serviços para o IDP. O IDP precisa desses metadados para estabelecer uma relação de confiança com os controladores e processar solicitações de autorização. O arquivo inclui informações como o nome de domínio do controlador ou endereço IP, para que o IDP possa se comunicar com os provedores de serviços.

**Passos**

1. Clique no link **Exportar arquivos do provedor de serviços**.

   A caixa de diálogo Exportar ficheiros do fornecedor de serviços abre-se.

2. Introduza o endereço IP do controlador ou o nome DNS no campo **Controller A** e, em seguida, clique em **Export** para guardar o ficheiro de metadados no sistema local. Se a matriz de armazenamento incluir dois controladores, repita esta etapa para o segundo controlador no campo **Controller B**.

   Depois de clicar em **Exportar**, os metadados do fornecedor de serviços são transferidos para o seu sistema local. Anote onde o arquivo é armazenado.

3. No sistema local, localize o(s) arquivo(s) de metadados do provedor de serviços que você exportou.

   Há um arquivo formatado em XML para cada controlador.

4. A partir do servidor IDP, importe o(s) arquivo(s) de metadados do provedor de serviços para estabelecer a relação de confiança. Pode importar os ficheiros diretamente ou pode introduzir manualmente as

informações do controlador a partir dos ficheiros.

#### Passo 3: Mapear funções

Para fornecer aos usuários autorização e acesso ao System Manager, é necessário mapear os atributos de usuário e associações a grupos de IDP para as funções predefinidas do storage array.

**Antes de começar**

- Um administrador de IDP configurou atributos de usuário e associação de grupo no sistema de IDP.
- O arquivo de metadados IDP é importado para o System Manager.
- Um arquivo de metadados do provedor de serviços para cada controlador é importado para o sistema IDP para a relação de confiança.

**Passos**

1. Clique no link para **Mapping System Manager** Roles.

   A caixa de diálogo Mapeamento de função é aberta.

2. Atribua atributos de usuário e grupos IDP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

   **Detalhes do campo**

| Definição | Descrição |
|---|---|
| **Mapeamentos** | Atributo do utilizador |
| Especifique o atributo (por exemplo, "membro de") para o grupo SAML a ser mapeado. | Valor do atributo |
| Especifique o valor do atributo para o grupo a ser mapeado. Expressões regulares são suportadas. Esses carateres especiais de expressão regular devem ser escapados com uma barra invertida (\) se eles não forem parte de um padrão de expressão regular | Funções |

> A função Monitor é necessária para todos os usuários, incluindo o administrador. O System Manager não funcionará corretamente para nenhum usuário sem a função Monitor presente.

3. Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.

   Mapeamentos de função podem ser modificados depois que o SAML estiver habilitado.

4. Quando terminar com os mapeamentos, clique em **Salvar**.

#### Passo 4: Teste o login SSO

Para garantir que o sistema IDP e o storage array possam se comunicar, você pode testar opcionalmente um login SSO. Este teste também é realizado durante a etapa final para ativar o SAML.

**Antes de começar**

- O arquivo de metadados IDP é importado para o System Manager.
- Um arquivo de metadados do provedor de serviços para cada controlador é importado para o sistema IDP para a relação de confiança.

**Passos**

1. Selecione o link **Test SSO Login**.

   Abre-se uma caixa de diálogo para introduzir credenciais SSO.

2. Insira credenciais de login para um usuário com permissões de Administrador de Segurança e permissões de Monitor.

   Abre-se uma caixa de diálogo enquanto o sistema testa o início de sessão.

3. Procure uma mensagem Teste bem-sucedida. Se o teste for concluído com êxito, vá para a próxima etapa para ativar o SAML.

   Se o teste não for concluído com êxito, é apresentada uma mensagem de erro com mais informações. Certifique-se de que:

   - O usuário pertence a um grupo com permissões para Administrador de Segurança e Monitor.
   - Os metadados carregados para o servidor IDP estão corretos.
   - Os endereços do controlador nos arquivos de metadados do SP estão corretos.

#### Passo 5: Ative o SAML

Sua etapa final é concluir a configuração SAML para autenticação de usuário. Durante esse processo, o sistema também solicita que você teste um login SSO. O processo de teste SSO Login é descrito na etapa anterior.

**Antes de começar**

- O arquivo de metadados IDP é importado para o System Manager.
- Um arquivo de metadados do provedor de serviços para cada controlador é importado para o sistema IDP para a relação de confiança.
- Pelo menos um mapeamento de função Monitor e um Admin de segurança está configurado.

**Edição e desativação.** Uma vez que o SAML está ativado, você *não pode* desabilitá-lo através da interface do usuário, nem pode editar as configurações de IDP. Se você precisar desativar ou editar a configuração SAML, entre em Contato com o suporte técnico para obter assistência.

**Passos**

1. Na guia **SAML**, selecione o link **Ativar SAML**.

   A caixa de diálogo confirmar ativação SAML é aberta.

2. Digite `enable`e clique em **Ativar**.
3. Insira as credenciais do usuário para um teste de login SSO.

**Resultados**

Depois que o sistema ativa o SAML, ele termina todas as sessões ativas e começa a autenticar usuários por meio do SAML.

### Alterar mapeamentos de função SAML

Se você configurou o SAML para Gerenciamento de Acesso anteriormente, poderá alterar os mapeamentos de função entre os grupos de IDP e as funções predefinidas do storage array.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- Um administrador de IDP configurou atributos de usuário e associação de grupo no sistema de IDP.
- O SAML está configurado e ativado.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **SAML**.
3. Selecione **Mapeamento de função**.

   A caixa de diálogo Mapeamento de função é aberta.

4. Atribua atributos de usuário e grupos IDP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

   Tenha cuidado para não remover suas permissões enquanto o SAML estiver habilitado, ou você perderá o acesso ao System Manager.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| **Mapeamentos** | Atributo do utilizador |
| Especifique o atributo (por exemplo, "membro de") para o grupo SAML a ser mapeado. | Valor do atributo |
| Especifique o valor do atributo para o grupo a ser mapeado. | Funções |

A função Monitor é necessária para todos os usuários, incluindo o administrador. O System Manager não funcionará corretamente para nenhum usuário sem a função Monitor presente.

5. Opcionalmente, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.
6. Clique em **Salvar**.

**Resultados**

Depois de concluir esta tarefa, todas as sessões ativas do utilizador são encerradas. Apenas a sessão de utilizador atual é mantida.

### Exporte arquivos do provedor de serviços SAML

Se necessário, você pode exportar metadados do provedor de serviços para o storage array e importar novamente o(s) arquivo(s) para o sistema de provedor de identidade (IDP).

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- O SAML está configurado e ativado.

**Sobre esta tarefa**

Nessa tarefa, você exporta metadados dos controladores (um arquivo para cada controlador). O IDP precisa desses metadados para estabelecer uma relação de confiança com os controladores e processar solicitações de autenticação. O arquivo inclui informações como o nome de domínio do controlador ou endereço IP que o IDP pode usar para enviar solicitações.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **SAML**.

3. Selecione **Exportar**.

   A caixa de diálogo Exportar ficheiros do fornecedor de serviços abre-se.

4. Para cada controlador, clique em **Exportar** para guardar o ficheiro de metadados no sistema local.

   Os campos de nome de domínio para cada controlador são somente leitura.

   Anote onde o arquivo é armazenado.

5. No sistema local, localize o(s) arquivo(s) de metadados do provedor de serviços que você exportou.

   Há um arquivo formatado em XML para cada controlador.

6. No servidor IDP, importe o(s) arquivo(s) de metadados do provedor de serviços. Você pode importar os arquivos diretamente ou inserir manualmente as informações do controlador a partir deles.
7. Clique em **Fechar**.

## Use tokens de acesso

### Crie tokens de acesso

Você pode criar um token de acesso para autenticar com a API REST ou a interface de linha de comando (CLI) no lugar de um nome de usuário e senha.

Os tokens não têm senhas, então você deve gerenciá-los com cuidado.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **Access tokens**.
3. Selecione **Exibir/Editar Configurações do token de acesso**. Na caixa de diálogo, certifique-se de que a caixa de verificação **Ativar tokens de acesso** está selecionada. Clique em **Salvar** para fechar a caixa de diálogo.
4. Selecione **Create Access Token**.
5. Na caixa de diálogo, selecione a duração para o token ser válido.

   Depois que o token expirar, as tentativas de autenticação do usuário falharão.

6. Clique em **criar.**
7. Na caixa de diálogo, selecione uma das seguintes opções:
   - **Copiar** para salvar o texto do token na área de transferência.
   - **Download** para salvar o texto do token em um arquivo.

     Certifique-se de salvar o texto do token. Esta é a sua única oportunidade de ver o texto antes de fechar o diálogo.

8. Clique em **Fechar**.

9. Use o token da seguinte forma:
   - **API REST**: Para usar um token em uma solicitação de API REST, adicione um cabeçalho HTTP às suas solicitações. Por exemplo:
     `Authorization: Bearer <access-token-value>`
   - **CLI segura**: Para usar um token na CLI, adicione o valor do token na linha de comando ou use o caminho para um arquivo contendo o valor do token. Por exemplo:
     - Valor do token na linha de comando: `-t access-token-value`
     - Caminho para um arquivo contendo o valor do token: `-T access-token-file`

     > A CLI solicita ao usuário um valor de token de acesso na linha de comando se nenhum nome de usuário, senha ou token for especificado.

#### Editar as configurações do token de acesso

Você pode editar configurações para tokens de acesso, que incluem os tempos de expiração e a capacidade de criar novos tokens.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **Access tokens**.
3. Selecione **Exibir/Editar Configurações do token de acesso**.
4. Na caixa de diálogo, você pode executar uma ou ambas as tarefas:
   - Ativar ou desativar a criação de token.
   - Altere a expiração dos tokens existentes.

   > Quando você desseleciona a configuração **Ativar tokens de acesso**, ela impede a criação de tokens e a autenticação de token. Se você reativar essa configuração mais tarde, tokens não expirados podem ser reutilizados. Se você quiser revogar permanentemente todos os tokens existentes, "Revogar tokens de acesso"consulte .
5. Clique em **Salvar**.

#### Revogar tokens de acesso

Você pode revogar todos os tokens de acesso se determinar que um token foi comprometido ou se deseja executar uma rotação manual de chaves para as chaves criptográficas usadas para assinar e validar os tokens de acesso.

Esta operação regenera as chaves usadas para assinar os tokens. Uma vez que as chaves são redefinidas, *todos* tokens emitidos são imediatamente invalidados. Como o storage array não rastreia tokens, tokens individuais não podem ser revogados.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **Access tokens**.

3. Selecione **revogar todos os tokens de acesso**.
4. Na caixa de diálogo, clique em **Yes**.

Depois de revogar todos os tokens, você pode criar novos tokens e usá-los imediatamente.

## Gerenciar syslog

### Exibir atividade do log de auditoria

Ao visualizar logs de auditoria, os usuários com permissões de administrador de segurança podem monitorar as ações do usuário, falhas de autenticação, tentativas de login inválidas e a vida útil da sessão do usuário.

#### Antes de começar

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.

#### Passos

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **Audit Log**.

   A atividade do log de auditoria aparece em formato tabular, que inclui as seguintes colunas de informações:

   - **Date/time** — Timestamp de quando a matriz de armazenamento detetou o evento (em GMT).
   - **Nome de usuário** — o nome de usuário associado ao evento. Para quaisquer ações não autenticadas na matriz de armazenamento, "N/A" aparece como o nome de usuário. Ações não autenticadas podem ser acionadas pelo proxy interno ou por algum outro mecanismo.
   - **Status Code** — Código de status HTTP da operação (200, 400, etc.) e texto descritivo associado ao evento.
   - **URL acessado** — URL completa (incluindo host) e string de consulta.
   - **Endereço IP do cliente** — Endereço IP do cliente associado ao evento.
   - **Source** — fonte de Registro associada ao evento, que pode ser System Manager, CLI, Web Services ou Support Shell.
   - **Descrição** — informações adicionais sobre o evento, se aplicável.
3. Utilize as seleções na página Registo de auditoria para ver e gerir eventos.

**Detalhes da seleção**

| Seleção | Descrição |
| --- | --- |
| Mostrar eventos do… | Limite eventos mostrados por intervalo de datas (últimas 24 horas, últimos 7 dias, últimos 30 dias ou um intervalo de datas personalizado). |
| Filtro | Limite eventos mostrados pelos carateres inseridos no campo. Use aspas (""") para uma correspondência exata de palavras, digite `OR` para retornar uma ou mais palavras ou insira um traço ( — ) para omitir palavras. |
| Atualizar | Selecione **Atualizar** para atualizar a página para os eventos mais atuais. |
| Ver/Editar definições | Selecione **Exibir/Editar configurações** para abrir uma caixa de diálogo que permite especificar uma política de log completa e o nível de ações a serem registradas. |
| Eliminar eventos | Selecione **Excluir** para abrir uma caixa de diálogo que permite remover eventos antigos da página. |
| Mostrar/ocultar colunas | Clique no ícone da coluna **Mostrar/Ocultar** para selecionar colunas adicionais para exibição na tabela. Colunas adicionais incluem:<br>• **Método** — o método HTTP (por exemplo, POST, GET, DELETE, etc.).<br>• * Comando CLI executado* — o comando CLI (gramática) executado para solicitações de CLI segura.<br>• **CLI Return Status** — Um código de status CLI ou uma solicitação de arquivos de entrada do cliente.<br>• **Procedimento de símbolo** — procedimento de símbolo executado.<br>• * Tipo de evento SSH* — tipo de eventos Secure Shell (SSH), como login, logout e login_fail.<br>• **SSH Session PID** — número de ID do processo da sessão SSH.<br>• **Duração(s) da sessão SSH** — o número de segundos em que o usuário foi conetado.<br>• **Tipo de autenticação** — os tipos podem incluir usuário local, LDAP, SAML e token de acesso.<br>• **ID de autenticação** — ID da sessão autenticada. |
| Alternar filtros de coluna | Clique no ícone **alternar** para abrir campos de filtragem para cada coluna. Insira carateres dentro de um campo de coluna para limitar eventos mostrados por esses carateres. Clique novamente no ícone para fechar os campos de filtragem. |
| Anular alterações | Clique no ícone **Desfazer** para retornar a tabela à configuração padrão. |

| Seleção | Descrição |
| --- | --- |
| Exportação | Clique em **Export** para salvar os dados da tabela em um arquivo CSV (Comma Separated Value). |

### Definir políticas de log de auditoria

Pode alterar a política de substituição e os tipos de eventos registados no registo de auditoria.

#### Antes de começar

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.

#### Sobre esta tarefa

Esta tarefa descreve como alterar as definições do registo de auditoria, que incluem a política de substituição de eventos antigos e a política de gravação de tipos de eventos.

#### Passos

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione o separador **Registo de auditoria**.
3. Selecione **Exibir/Editar configurações**.

   A caixa de diálogo Configurações do Registro de auditoria é aberta.

4. Altere a política de substituição ou os tipos de eventos gravados.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| Substituir a política | Determina a política de substituição de eventos antigos quando a capacidade máxima é atingida:<br>• **Permitir que os eventos mais antigos do log de auditoria sejam sobrescritos quando o log de auditoria estiver cheio** — sobrescreve os eventos antigos quando o log de auditoria atinge 50.000 Registros.<br>• **Exigir que os eventos de log de auditoria sejam excluídos manualmente** — especifica que os eventos não serão excluídos automaticamente; em vez disso, um aviso de limite aparece na porcentagem definida. Os eventos devem ser excluídos manualmente.<br>Se a política de substituição estiver desativada e as entradas do log de auditoria atingirem o limite máximo, o acesso ao System Manager será negado aos usuários sem permissões de Administrador de Segurança. Para restaurar o acesso do sistema a usuários sem permissões de Administrador de Segurança, um usuário atribuído à função Administrador de Segurança deve excluir os Registros de eventos antigos.<br>As diretivas de substituição não se aplicam se um servidor syslog estiver configurado para arquivar logs de auditoria. |
| Nível de ações a registar | Determina os tipos de eventos a serem registrados:<br>• **Gravar eventos de modificação somente** — mostra apenas os eventos em que uma ação do usuário envolve fazer uma alteração no sistema.<br>• **Grave todos os eventos de modificação e somente leitura** — mostra todos os eventos, incluindo uma ação do usuário que envolve a leitura ou download de informações. |

5. Clique em **Salvar**.

### Excluir eventos do log de auditoria

Você pode limpar o log de auditoria de eventos antigos, o que torna a pesquisa através de eventos mais gerenciável. Você tem a opção de salvar eventos antigos em um arquivo CSV (valores separados por vírgulas) após a exclusão.

**Antes de começar**

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione o separador **Registo de auditoria**.
3. Selecione **Eliminar**.

   A caixa de diálogo Excluir Registro de auditoria é aberta.

4. Selecione ou introduza o número de eventos mais antigos que pretende eliminar.
5. Se pretender exportar os eventos eliminados para um ficheiro CSV (recomendado), mantenha a caixa de verificação selecionada. Você será solicitado a inserir um nome de arquivo e um local quando clicar em **Excluir** na próxima etapa. Caso contrário, se você não quiser salvar eventos em um arquivo CSV, clique na caixa de seleção para desmarcá-lo.
6. Clique em **Excluir**.

   Abre-se uma caixa de diálogo de confirmação.

7. Digite `delete` o campo e clique em **Excluir**.

   Os eventos mais antigos são removidos da página Registo de Auditoria.

### Configure o servidor syslog para logs de auditoria

Se você quiser arquivar logs de auditoria em um servidor syslog externo, você pode configurar as comunicações entre esse servidor e o storage array. Depois que a conexão é estabelecida, os logs de auditoria são salvos automaticamente no servidor syslog.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- O endereço do servidor syslog, o protocolo e o número da porta devem estar disponíveis. O endereço do servidor pode ser um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- Se o servidor usar um protocolo seguro (por exemplo, TLS), um certificado de autoridade de certificação (CA) deve estar disponível no sistema local. Os certificados CA identificam os proprietários de sites para conexões seguras entre servidores e clientes.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Na guia Registro de auditoria, selecione **Configurar servidores Syslog**.

   A caixa de diálogo Configurar servidores Syslog é aberta.

3. Clique em **Add**.

   A caixa de diálogo Add Syslog Server (Adicionar servidor Syslog) é aberta.

4. Insira as informações do servidor e clique em **Adicionar**.
   - **Endereço do servidor** — Digite um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.

- **Protocol** — Selecione um protocolo na lista suspensa (por exemplo, TLS, UDP ou TCP).
- **Upload certificate (opcional)** — se você selecionou o protocolo TLS e ainda não carregou um certificado CA assinado, clique em **Browse** para carregar um arquivo de certificado. Os logs de auditoria não são arquivados em um servidor syslog sem um certificado confiável.

> Se o certificado se tornar inválido mais tarde, o handshake TLS falhará. Como resultado, uma mensagem de erro é postada no log de auditoria e as mensagens não são mais enviadas para o servidor syslog. Para resolver este problema, tem de corrigir o certificado no servidor syslog e, em seguida, aceder ao **Definições › Registo de auditoria › Configurar servidores Syslog › testar tudo**.

- **Port** — Digite o número da porta para o recetor syslog. Depois de clicar em **Add**, a caixa de diálogo Configurar servidores Syslog abre e exibe o servidor syslog configurado na página.

5. Para testar a conexão do servidor com a matriz de armazenamento, selecione **Test All**.

**Resultados**

Após a configuração, todos os novos logs de auditoria são enviados para o servidor syslog. Os registos anteriores não são transferidos. Para configurar ainda mais as configurações do syslog para alertas, "Configure o servidor syslog para alertas" consulte .

```
NOTE: If multiple syslog servers are configured, all configured syslog
servers will receive an audit log.
```

### Edite as configurações do servidor syslog para Registros de log de auditoria

Você pode alterar as configurações do servidor syslog usado para arquivar logs de auditoria e também carregar um novo certificado de autoridade de certificação (CA) para o servidor.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- O endereço do servidor syslog, o protocolo e o número da porta devem estar disponíveis. O endereço do servidor pode ser um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- Se você estiver carregando um novo certificado de CA, o certificado deve estar disponível no sistema local.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Na guia Registro de auditoria, selecione **Configurar servidores Syslog**.

   Os servidores syslog configurados são exibidos na página.

3. Para editar as informações do servidor, selecione o ícone **Edit** (lápis) à direita do nome do servidor e, em seguida, faça as alterações desejadas nos seguintes campos:
   - **Endereço do servidor** — Digite um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.

- **Protocol** — Selecione um protocolo na lista suspensa (por exemplo, TLS, UDP ou TCP).
- **Port** — Digite o número da porta para o recetor syslog.

4. Se você alterou o protocolo para o protocolo TLS seguro (de UDP ou TCP), clique em **Importar certificado confiável** para carregar um certificado CA.
5. Para testar a nova conexão com a matriz de armazenamento, selecione **Test All**.

**Resultados**

Após a configuração, todos os novos logs de auditoria são enviados para o servidor syslog. Os registos anteriores não são transferidos.

## FAQs

**Por que não consigo fazer login?**

Se receber um erro ao tentar iniciar sessão no System Manager, reveja estas possíveis causas.

Erros de login no System Manager podem ocorrer por um destes motivos:

- Introduziu um nome de utilizador ou palavra-passe incorreto.
- Você não tem Privileges suficiente.
- O servidor de diretório (se configurado) pode estar indisponível. Se for esse o caso, tente fazer login com uma função de usuário local.
- Tentou iniciar sessão sem sucesso várias vezes, o que acionou o modo de bloqueio. Aguarde 10 minutos para voltar a iniciar sessão.
- Uma condição de bloqueio foi acionada e seu log de auditoria pode estar cheio. Aceda a Gestão de Acesso e elimine eventos antigos do registo de auditoria.
- A autenticação SAML está ativada. Atualize seu navegador para fazer login.

Erros de login em um storage array remoto para tarefas de espelhamento podem ocorrer por um destes motivos:

- Introduziu uma palavra-passe incorreta.
- Tentou iniciar sessão sem sucesso várias vezes, o que acionou o modo de bloqueio. Aguarde 10 minutos para iniciar sessão novamente.
- O número máximo de conexões de cliente usadas no controlador foi atingido. Verifique se há vários usuários ou clientes.

**O que eu preciso saber antes de adicionar um servidor de diretório?**

Antes de adicionar um servidor de diretório no Gerenciamento de Acesso, certifique-se de atender aos seguintes requisitos.

- Os grupos de usuários devem ser definidos em seu serviço de diretório.
- As credenciais do servidor LDAP devem estar disponíveis, incluindo o nome de domínio, o URL do servidor e, opcionalmente, o nome de usuário e a senha da conta BIND.
- Para servidores LDAPS que usam um protocolo seguro, a cadeia de certificados do servidor LDAP deve ser instalada na sua máquina local.

**O que eu preciso saber sobre mapeamento para funções de storage array?**

## Antes de mapear grupos para funções, revise as diretrizes a seguir.

As funcionalidades de RBAC (controle de acesso baseado em funções) do storage array incluem as seguintes funções:

- **Storage admin** — Acesso completo de leitura/gravação aos objetos de armazenamento (por exemplo, volumes e pools de discos), mas sem acesso à configuração de segurança.
- **Admin de segurança** — Acesso à configuração de segurança em Gerenciamento de acesso, gerenciamento de certificados, gerenciamento de log de auditoria e a capacidade de ativar ou desativar a interface de gerenciamento legada (símbolo).
- **Support admin** — Acesso a todos os recursos de hardware na matriz de armazenamento, dados de falha, eventos mel e atualizações de firmware do controlador. Sem acesso a objetos de armazenamento ou à configuração de segurança.
- **Monitor** — Acesso somente leitura a todos os objetos de armazenamento, mas sem acesso à configuração de segurança.

#### Serviços de diretório

Se estiver a utilizar um servidor LDAP (Lightweight Directory Access Protocol) e Serviços de diretório, certifique-se de que:

- Um administrador definiu grupos de usuários no serviço de diretório.
- Você conhece os nomes de domínio de grupo para os grupos de usuários LDAP. Expressões regulares são suportadas. Esses carateres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular:

```
\.[]{}()<>*+-=!?^$|
```

- A função Monitor é necessária para todos os usuários, incluindo o administrador. O System Manager não funcionará corretamente para nenhum usuário sem a função Monitor presente.

#### SAML

Se você estiver usando os recursos de Security Assertion Markup Language (SAML) incorporados ao storage array, verifique se:

- Um administrador do Provedor de identidade (IDP) configurou atributos de usuário e associação de grupo no sistema IDP.
- Você conhece os nomes dos membros do grupo.
- Você sabe o valor do atributo para o grupo a ser mapeado. Expressões regulares são suportadas. Esses carateres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular:

```
\.[]{}()<>*+-=!?^$|
```

- A função Monitor é necessária para todos os usuários, incluindo o administrador. O System Manager não

funcionará corretamente para nenhum usuário sem a função Monitor presente.

**Que ferramentas de gestão externas podem ser afetadas por esta alteração?**

Quando você faz certas alterações no System Manager, como alternar a interface de gerenciamento ou usar o SAML para um método de autenticação, algumas ferramentas e recursos externos podem ser restritos ao uso.

#### Interface de gerenciamento

As ferramentas que se comunicam diretamente com a interface de gerenciamento legada (símbolo), como o provedor SMI-S do SANtricity ou o OnCommand Insight (OCI), não funcionam a menos que a configuração Interface de Gerenciamento legado esteja ativada. Além disso, você não pode usar comandos CLI legados ou executar operações de espelhamento se essa configuração estiver desativada.

Entre em Contato com o suporte técnico para obter mais informações.

#### Autenticação SAML

Quando o SAML está habilitado, os seguintes clientes não podem acessar os serviços e recursos do storage array:

- Janela de gerenciamento empresarial (EMW)
- Interface de linha de comando (CLI)
- Clientes de Software Developer Kits (SDK)
- Clientes na banda
- Clientes API REST de Autenticação básica HTTP
- Faça login usando o endpoint padrão da API REST

Entre em Contato com o suporte técnico para obter mais informações.

**O que eu preciso saber antes de configurar e ativar o SAML?**

Antes de configurar e habilitar os recursos de Security Assertion Markup Language (SAML) para autenticação, certifique-se de atender aos requisitos a seguir e entender as restrições SAML.

#### Requisitos

Antes de começar, certifique-se de que:

- Um Provedor de identidade (IDP) está configurado na sua rede. Um IDP é um sistema externo usado para solicitar credenciais de um usuário e determinar se o usuário foi autenticado com êxito. Sua equipe de segurança é responsável por manter o IDP.
- Um administrador de IDP configurou atributos de usuário e grupos no sistema de IDP.
- Um administrador de IDP garantiu que o IDP suporta a capacidade de retornar um ID de nome na autenticação.
- Um administrador garantiu que o servidor IDP e os relógios do controlador são sincronizados (através de um servidor NTP ou ajustando as definições do relógio do controlador).

- Um arquivo de metadados IDP é baixado do sistema IDP e está disponível no sistema local usado para acessar o System Manager.
- Você sabe o endereço IP ou o nome de domínio de cada controlador na matriz de armazenamento.

#### Restrições

Além dos requisitos acima, certifique-se de que compreende as seguintes restrições:

- Uma vez que o SAML está ativado, você *não pode* desabilitá-lo através da interface do usuário, nem pode editar as configurações de IDP. Se você precisar desativar ou editar a configuração SAML, entre em Contato com o suporte técnico para obter assistência. Recomendamos que você teste os logins SSO antes de ativar o SAML na etapa final de configuração. (O sistema também executa um teste de login SSO antes de ativar o SAML.)
- Se você desabilitar o SAML no futuro, o sistema restaurará automaticamente a configuração anterior (funções de usuário local e/ou Serviços de diretório).
- Se os Serviços de diretório estiverem configurados atualmente para autenticação de usuário, o SAML substituirá essa configuração.
- Quando o SAML é configurado, os seguintes clientes não podem acessar os recursos do storage array:
  - Janela de gerenciamento empresarial (EMW)
  - Interface de linha de comando (CLI)
  - Clientes de Software Developer Kits (SDK)
  - Clientes na banda
  - Clientes API REST de Autenticação básica HTTP
  - Faça login usando o endpoint padrão da API REST

### Que tipos de eventos são registrados no log de auditoria?

O log de auditoria pode gravar eventos de modificação ou eventos de modificação e somente leitura.

Dependendo das definições da política, são apresentados os seguintes tipos de eventos:

- **Eventos de modificação** — ações do usuário de dentro do System Manager que envolvem alterações no sistema, como provisionamento de armazenamento.
- **Modificação e eventos somente leitura** — ações do usuário que envolvem alterações no sistema, bem como eventos que envolvem visualização ou download de informações, como visualização de atribuições de volume.

### O que eu preciso saber antes de configurar um servidor syslog?

Você pode arquivar logs de auditoria em um servidor syslog externo.

Antes de configurar um servidor syslog, tenha em mente as seguintes diretrizes.

- Certifique-se de que conhece o endereço do servidor, o protocolo e o número da porta. O endereço do servidor pode ser um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- Se o servidor usar um protocolo seguro (por exemplo, TLS), um certificado de autoridade de certificação (CA) deve estar disponível no sistema local. Os certificados CA identificam os proprietários de sites para

conexões seguras entre servidores e clientes.

- Após a configuração, todos os novos logs de auditoria são enviados para o servidor syslog. Os registos anteriores não são transferidos.
- As configurações de política de substituição (disponíveis em **Exibir/Editar configurações**) não afetam a forma como os logs são gerenciados com uma configuração de servidor syslog.
- Os logs de auditoria seguem o formato de mensagens RFC 5424.

#### O servidor syslog não está mais recebendo logs de auditoria. O que faço?

Se você configurou um servidor syslog com um protocolo TLS, o servidor não poderá receber mensagens se o certificado se tornar inválido por qualquer motivo. Uma mensagem de erro sobre o certificado inválido é publicada no log de auditoria.

Para resolver esse problema, primeiro você deve corrigir o certificado para o servidor syslog. Quando uma cadeia de certificados válida estiver em vigor, aceda ao **Definições › Registo de auditoria › Configurar servidores Syslog › testar tudo**.

# Certificados

## Descrição geral dos certificados

Você pode usar o System Manager para criar solicitações de assinatura de certificado (CSRs), importar certificados e gerenciar certificados existentes.

#### O que são certificados?

*Certificados* são arquivos digitais que identificam entidades online, como sites e servidores, para comunicações seguras na internet. Existem dois tipos de certificados: Um certificado *assinado* é validado por uma autoridade de certificação (CA) e um certificado *autoassinado* é validado pelo proprietário da entidade em vez de um terceiro.

Saiba mais:

- "Como os certificados funcionam"
- "Terminologia do certificado"

#### Como configuro certificados assinados?

Primeiro, você gera uma solicitação de assinatura do System Manager e, em seguida, envia o arquivo para uma CA. Quando a CA retornar os arquivos de certificado, você os importará usando o System Manager.

Saiba mais:

- "Use certificados assinados pela CA para controladores"
- "Use certificados assinados pela CA para autenticação com um servidor de gerenciamento de chaves"

#### Informações relacionadas

Saiba mais sobre tarefas relacionadas a certificados:

- "Exibir informações de certificado importadas"
- "Ativar verificação de revogação de certificado"

## Conceitos

### Como os certificados funcionam

Certificados são arquivos digitais que identificam entidades online, como sites e servidores, para comunicações seguras na internet.

Os certificados garantem que as comunicações da Web sejam transmitidas de forma encriptada, privada e inalterada, apenas entre o servidor e o cliente especificados. Usando o System Manager, você pode gerenciar certificados entre o navegador em um sistema de gerenciamento de host (atuando como cliente) e os controladores em um sistema de storage (atuando como servidores).

Um certificado pode ser assinado por uma autoridade confiável ou pode ser autoassinado. "Assinatura" significa simplesmente que alguém validou a identidade do proprietário e determinou que seus dispositivos podem ser confiáveis. As matrizes de armazenamento são fornecidas com um certificado auto-assinado gerado automaticamente em cada controlador. Você pode continuar usando os certificados autoassinados ou obter certificados assinados pela CA para uma conexão mais segura entre os controladores e os sistemas host.

> Embora os certificados assinados pela CA forneçam melhor proteção de segurança (por exemplo, evitando ataques man-in-the-middle), eles também exigem taxas que podem ser caras se você tiver uma rede grande. Em contraste, os certificados autoassinados são menos seguros, mas são gratuitos. Portanto, os certificados autoassinados são mais usados para ambientes de teste internos, não em ambientes de produção.

#### Certificados assinados

Um certificado assinado é validado por uma autoridade de certificação (CA), que é uma organização de terceiros confiável. Os certificados assinados incluem detalhes sobre o proprietário da entidade (normalmente, um servidor ou site), data de emissão e expiração do certificado, domínios válidos para a entidade e uma assinatura digital composta por letras e números.

Quando você abre um navegador e insere um endereço da Web, o sistema executa um processo de verificação de certificados em segundo plano para determinar se você está se conetando a um site que inclui um certificado válido assinado pela CA. Geralmente, um site protegido com um certificado assinado inclui um ícone de cadeado e uma designação https no endereço. Se você tentar se conetar a um site que não contenha um certificado assinado pela CA, o navegador exibirá um aviso de que o site não está seguro.

A CA toma medidas para verificar sua identidade durante o processo de inscrição. Eles podem enviar um e-mail para sua empresa registrada, verificar seu endereço comercial e executar uma verificação HTTP ou DNS. Quando o processo de aplicação estiver concluído, a CA envia arquivos digitais para serem carregados em um sistema de gerenciamento de host. Normalmente, esses arquivos incluem uma cadeia de confiança, como segue:

- **Root** — na parte superior da hierarquia está o certificado raiz, que contém uma chave privada usada para assinar outros certificados. A raiz identifica uma organização de CA específica. Se você usar a mesma CA para todos os dispositivos de rede, precisará de apenas um certificado raiz.
- **Intermediate** — ramificação fora da raiz são os certificados intermediários. A CA emite um ou mais certificados intermediários para atuar como intermediários entre uma raiz protegida e certificados de servidor.

- **Servidor** — na parte inferior da cadeia está o certificado do servidor, que identifica sua entidade específica, como um site ou outro dispositivo. Cada controlador em um storage array requer um certificado de servidor separado.

#### Certificados autoassinados

Cada controladora no storage inclui um certificado pré-instalado e autoassinado. Um certificado autoassinado é semelhante a um certificado assinado pela CA, exceto que ele é validado pelo proprietário da entidade em vez de um terceiro. Como um certificado assinado pela CA, um certificado autoassinado contém sua própria chave privada e também garante que os dados sejam criptografados e enviados por uma conexão HTTPS entre um servidor e um cliente. No entanto, um certificado autoassinado não usa a mesma cadeia de confiança que um certificado assinado pela CA.

Os certificados autoassinados não são "confiáveis" pelos navegadores. Cada vez que você tenta se conetar a um site que contém apenas um certificado autoassinado, o navegador exibe uma mensagem de aviso. Você deve clicar em um link na mensagem de aviso que permite que você prossiga para o site; ao fazê-lo, você está essencialmente aceitando o certificado auto-assinado.

#### Certificados usados para o servidor de gerenciamento de chaves

Se você estiver usando um servidor de gerenciamento de chaves externo com o recurso Segurança da unidade, também poderá gerenciar certificados para autenticação entre esse servidor e os controladores.

### Terminologia do certificado

Os termos a seguir se aplicam ao gerenciamento de certificados.

| Prazo | Descrição |
|---|---|
| CA | Uma autoridade de certificação (CA) é uma entidade confiável que emite documentos eletrônicos, chamados certificados digitais, para segurança na Internet. Esses certificados identificam proprietários de sites, o que permite conexões seguras entre clientes e servidores. |
| CSR | Uma solicitação de assinatura de certificado (CSR) é uma mensagem enviada de um requerente para uma autoridade de certificação (CA). O CSR valida as informações que a CA precisa para emitir um certificado. |
| Certificado | Um certificado identifica o proprietário de um site para fins de segurança, o que impede que atacantes personificem o site. O certificado contém informações sobre o proprietário do site e a identidade da entidade confiável que certifica (assina) essas informações. |
| Cadeia de certificados | Uma hierarquia de arquivos que adiciona uma camada de segurança aos certificados. Normalmente, a cadeia inclui um certificado raiz na parte superior da hierarquia, um ou mais certificados intermediários e os certificados de servidor que identificam as entidades. |
| Certificado de cliente | Para o gerenciamento de chaves de segurança, um certificado de cliente valida os controladores da matriz de armazenamento, para que o servidor de gerenciamento de chaves possa confiar em seus endereços IP. |

| Prazo | Descrição |
| --- | --- |
| Certificado intermédio | Um ou mais certificados intermediários ramificam da raiz na cadeia de certificados. A CA emite um ou mais certificados intermediários para atuar como intermediários entre uma raiz protegida e certificados de servidor. |
| Certificado do servidor de gerenciamento de chaves | Para o gerenciamento de chaves de segurança, um certificado do servidor de gerenciamento de chaves valida o servidor, para que o storage array possa confiar em seu endereço IP. |
| Armazenamento de chaves | Um keystore é um repositório no seu sistema de gerenciamento de host que contém chaves privadas, juntamente com suas chaves públicas e certificados correspondentes. Essas chaves e certificados identificam suas próprias entidades, como os controladores. |
| Servidor OCSP | O servidor OCSP (Online Certificate Status Protocol) determina se a autoridade de certificação (CA) revogou quaisquer certificados antes da data de expiração agendada e, em seguida, bloqueia o usuário de acessar um servidor se o certificado for revogado. |
| Certificado raiz | O certificado raiz está no topo da hierarquia na cadeia de certificados e contém uma chave privada usada para assinar outros certificados. A raiz identifica uma organização de CA específica. Se você usar a mesma CA para todos os dispositivos de rede, precisará de apenas um certificado raiz. |
| Certificado assinado | Um certificado validado por uma autoridade de certificação (CA). Este arquivo de dados contém uma chave privada e garante que os dados sejam enviados de forma criptografada entre um servidor e um cliente através de uma conexão HTTPS. Além disso, um certificado assinado inclui detalhes sobre o proprietário da entidade (normalmente, um servidor ou site) e uma assinatura digital composta por letras e números. Um certificado assinado usa uma cadeia de confiança e, portanto, é mais frequentemente usado em ambientes de produção. Também referido como um "certificado assinado pela CA" ou um "certificado de gestão". |
| Certificado auto-assinado | Um certificado autoassinado é validado pelo proprietário da entidade. Este arquivo de dados contém uma chave privada e garante que os dados sejam enviados de forma criptografada entre um servidor e um cliente através de uma conexão HTTPS. Também inclui uma assinatura digital composta por letras e números. Um certificado autoassinado não usa a mesma cadeia de confiança que um certificado assinado pela CA e, portanto, é mais frequentemente usado em ambientes de teste. Também referido como um certificado "pré-instalado". |
| Certificado do servidor | O certificado do servidor está na parte inferior da cadeia de certificados. Ele identifica sua entidade específica, como um site ou outro dispositivo. Cada controlador em um sistema de storage requer um certificado de servidor separado. |

# Use certificados

## Use certificados assinados pela CA para controladores

Você pode obter certificados assinados pela CA para comunicações seguras entre os controladores e o navegador usado para acessar o System Manager.

### Antes de começar

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Você deve saber o endereço IP ou os nomes DNS de cada controlador.

### Sobre esta tarefa

O uso de certificados assinados pela CA é um procedimento de três etapas.

#### Etapa 1: Conclua CSRs para os controladores

Primeiro, você deve gerar um arquivo de solicitação de assinatura de certificado (CSR) para cada controlador no storage de armazenamento.

### Sobre esta tarefa

Esta tarefa descreve como gerar um ficheiro CSR a partir do System Manager. O CSR fornece informações sobre a sua organização e o endereço IP ou o nome DNS do controlador. Durante esta tarefa, um arquivo CSR é gerado se o storage array tiver um controlador e dois arquivos CSR se tiver dois controladores.

> Alternativamente, você pode gerar um arquivo CSR usando uma ferramenta como OpenSSL e pode pular para Passo 2: Envie os arquivos CSR.

### Passos

1. Selecione **Definições › certificados**.
2. Na guia Gerenciamento de matrizes, selecione **Complete CSR**.

> Se você vir uma caixa de diálogo solicitando que você aceite um certificado autoassinado para o segundo controlador, clique em **aceitar certificado autoassinado** para continuar.

3. Insira as seguintes informações e clique em **Next**:
   - **Organização** — o nome completo e legal de sua empresa ou organização. Inclua sufixos, como Inc. Ou Corp.
   - * Unidade organizacional (opcional) * — a divisão da sua organização que está a lidar com o certificado.
   - **Cidade/localidade** — a cidade onde seu storage array ou negócio está localizado.
   - **Estado/região (opcional)** — o estado ou a região onde o storage ou a empresa está localizado.
   - **Código ISO do país** — o código ISO de dois dígitos do seu país (Organização Internacional para Padronização), como os EUA.

Alguns campos podem ser pré-preenchidos com as informações apropriadas, como o endereço IP do controlador. Não altere valores pré-preenchidos a menos que você tenha certeza de que eles estão incorretos. Por exemplo, se você ainda não concluiu um CSR, o endereço IP do controlador é definido como ""localhost". Neste caso, você deve alterar ""localhost"" para o nome DNS ou endereço IP do controlador.

4. Verifique ou insira as seguintes informações sobre o controlador A no storage array:
   - **Controller Um nome comum** — o endereço IP ou o nome DNS do controlador A é exibido por padrão. Certifique-se de que este endereço está correto; ele deve corresponder exatamente ao que você digita para acessar o System Manager no navegador. O nome DNS não pode começar com um curinga.
   - **Controller Um endereço IP alternativo** — se o nome comum for um endereço IP, você pode opcionalmente inserir quaisquer endereços IP adicionais ou aliases para o controlador A. para várias entradas, use um formato delimitado por vírgulas.
   - **Controller (controlador) De nomes DNS alternativos** — se o nome comum for um nome DNS, insira quaisquer nomes DNS adicionais para o controlador A. para várias entradas, use um formato delimitado por vírgulas. Se não houver nomes DNS alternativos, mas você inseriu um nome DNS no primeiro campo, copie esse nome aqui. O nome DNS não pode começar com um curinga. Se a matriz de armazenamento tiver apenas um controlador, o botão **Finish** estará disponível.

     Se a matriz de armazenamento tiver dois controladores, o botão **Next** estará disponível.

Não clique no link **Ignorar esta etapa** quando você estiver criando inicialmente uma solicitação CSR. Este link é fornecido em situações de recuperação de erros. Em casos raros, uma solicitação CSR pode falhar em um controlador, mas não no outro. Este link permite que você ignore a etapa para criar uma solicitação CSR no controlador A, se já estiver definida, e continue para a próxima etapa para recriar uma solicitação CSR no controlador B.

5. Se houver apenas um controlador, clique em **Finish**. Se houver dois controladores, clique em **Next** para inserir informações para o controlador B (o mesmo que acima) e, em seguida, clique em **Finish**.

   Para um único controlador, um ficheiro CSR é transferido para o seu sistema local. Para controladores duplos, são transferidos dois ficheiros CSR. A localização da pasta do download depende do seu navegador.

6. Vá para Passo 2: Envie os arquivos CSR.

#### Passo 2: Envie os arquivos CSR

Depois de criar os arquivos de solicitação de assinatura de certificado (CSR), envie os arquivos para uma autoridade de certificação (CA). Os sistemas e-Series exigem o formato PEM (codificação ASCII Base64) para certificados assinados, que inclui os seguintes tipos de arquivo: pem, .crt, .cer ou .key.

**Passos**

1. Localize os ficheiros CSR transferidos.
2. Envie os arquivos CSR para uma CA (por exemplo, VeriSign ou DigiCert) e solicite certificados assinados no formato PEM.

**Depois de enviar um arquivo CSR para a CA, NÃO regenere outro arquivo CSR.** Sempre que você gera um CSR, o sistema cria um par de chaves privadas e públicas. A chave pública faz parte da CSR, enquanto a chave privada é mantida no keystore do sistema. Quando você recebe os certificados assinados e os importa, o sistema garante que as chaves privadas e públicas sejam o par original. Se as chaves não corresponderem, os certificados assinados não funcionarão e você deverá solicitar novos certificados à CA.

3. Quando a CA retornar os certificados assinados, vá para Etapa 3: Importar certificados assinados para controladores.

#### Etapa 3: Importar certificados assinados para controladores

Depois de receber certificados assinados da Autoridade de Certificação (CA), importe os arquivos para os controladores.

**Antes de começar**

- A CA retornou arquivos de certificado assinados. Esses arquivos incluem o certificado raiz, um ou mais certificados intermediários e os certificados do servidor.
- Se a CA forneceu um arquivo de certificado encadeado (por exemplo, um arquivo .p7b), você deve descompactar o arquivo encadeado em arquivos individuais: O certificado raiz, um ou mais certificados intermediários e os certificados de servidor que identificam os controladores. Você pode usar o utilitário Windows `certmgr` para descompactar os arquivos (clique com o botão direito do Mouse e selecione **todas as tarefas › Exportar**). A codificação base-64 é recomendada. Quando as exportações estiverem concluídas, um arquivo CER é exibido para cada arquivo de certificado na cadeia.
- Você copiou os arquivos de certificado para o sistema host onde você acessa o System Manager.

**Passos**

1. Selecione o **Configurações › certificados**
2. Na guia Gerenciamento de matrizes, selecione **Importar**.

   Abre-se uma caixa de diálogo para importar o(s) ficheiro(s) de certificado.

3. Clique nos botões **Browse** para selecionar primeiro os arquivos de certificado raiz e intermediário e, em seguida, selecione cada certificado de servidor para os controladores. Os arquivos raiz e intermediário são os mesmos para ambos os controladores. Apenas os certificados de servidor são exclusivos para cada controlador. Se você gerou o CSR a partir de uma ferramenta externa, você também deve importar o arquivo de chave privada que foi criado juntamente com o CSR.

   Os nomes dos arquivos são exibidos na caixa de diálogo.

4. Clique em **Importar**.

   Os arquivos são carregados e validados.

**Resultado**

A sessão é terminada automaticamente. Você deve fazer login novamente para que os certificados entrem em vigor. Quando você faz login novamente, os novos certificados assinados pela CA são usados para sua sessão.

### Repor certificados de gestão

Você pode reverter os certificados nos controladores de usar certificados assinados pela CA de volta para os certificados autoassinados definidos de fábrica.

#### Antes de começar

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Os certificados assinados pela CA devem ser importados anteriormente.

#### Sobre esta tarefa

A função Redefinir exclui os arquivos de certificado assinados pela CA atuais de cada controlador. Em seguida, os controladores reverterão para o uso de certificados autoassinados.

#### Passos

1. Selecione **Definições › certificados**.
2. Na guia Gerenciamento de matrizes, selecione **Redefinir**.

   Uma caixa de diálogo confirmar certificados de Gerenciamento é aberta.

3. Digite `reset` o campo e clique em **Reset**.

   Após a atualização do navegador, o navegador pode bloquear o acesso ao site de destino e informar que o site está usando HTTP Strict Transport Security. Essa condição surge quando você volta para certificados autoassinados. Para limpar a condição que está bloqueando o acesso ao destino, você deve limpar os dados de navegação do navegador.

#### Resultados

Os controladores revertem para o uso de certificados autoassinados. Como resultado, o sistema solicita aos usuários que aceitem manualmente o certificado autoassinado para suas sessões.

### Exibir informações de certificado importadas

Na página certificados, você pode exibir o tipo de certificado, a autoridade emissora e o intervalo de datas válido de certificados para o storage array.

#### Antes de começar

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.

#### Passos

1. Selecione **Definições › certificados**.
2. Selecione uma das guias para exibir informações sobre os certificados.

| Separador | Descrição |
| --- | --- |
| Gerenciamento de array | Exibir informações sobre os certificados assinados pela CA importados para cada controlador, incluindo o arquivo raiz, o(s) arquivo(s) intermediário(s) e o(s) arquivo(s) do servidor. |

| Separador | Descrição |
| --- | --- |
| Confiável | Exibir informações sobre todos os outros tipos de certificados importados para os controladores. Use o campo de filtro em **Mostrar certificados que são…** para exibir certificados instalados pelo usuário ou pré-instalados.<br>• **User-Installed** — certificados que um usuário carregou no storage array, que podem incluir certificados confiáveis quando o controlador atua como cliente (em vez de um servidor), certificados LDAPS e certificados de Federação de identidade.<br>• **Pré-instalado** — certificados autoassinados incluídos com a matriz de armazenamento. |
| Gerenciamento de chaves | Exibir informações sobre os certificados assinados pela CA importados para um servidor de gerenciamento de chaves externo. |

#### Importar certificados para controladores quando atua como clientes

Se o controlador rejeitar uma ligação porque não pode validar a cadeia de confiança de um servidor de rede, pode importar um certificado a partir do separador fidedigno que permite ao controlador (agindo como cliente) aceitar comunicações desse servidor.

##### Antes de começar

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Os ficheiros de certificado estão instalados no sistema local.

##### Sobre esta tarefa

A importação de certificados da guia confiável pode ser necessária se você quiser permitir que outro servidor entre em Contato com os controladores (por exemplo, um servidor LDAP ou um servidor syslog que usa TLS).

##### Passos

1. Selecione **Definições › certificados**.
2. Na guia confiável, selecione **Importar**.

   Abre-se uma caixa de diálogo para importar os ficheiros de certificado fidedignos.
3. Clique em **Procurar** para selecionar os arquivos de certificado para os controladores.

   Os nomes dos arquivos são exibidos na caixa de diálogo.
4. Clique em **Importar**.

##### Resultados

Os arquivos são carregados e validados.

#### Ativar verificação de revogação de certificado

Você pode habilitar verificações automáticas para certificados revogados, de modo que

um servidor OCSP (Online Certificate Status Protocol) bloqueie os usuários de fazer conexões não seguras.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Um servidor DNS é configurado em ambos os controladores, o que permite o uso de um nome de domínio totalmente qualificado para o servidor OCSP. Esta tarefa está disponível na página hardware.
- Se você quiser especificar seu próprio servidor OCSP, você deve saber a URL desse servidor.

**Sobre esta tarefa**

A verificação automática de revogação é útil nos casos em que a autoridade de certificação emitiu incorretamente um certificado ou uma chave privada é comprometida.

Durante essa tarefa, você pode configurar um servidor OCSP ou usar o servidor especificado no arquivo de certificado. O servidor OCSP determina se a CA revogou quaisquer certificados antes da data de expiração agendada e, em seguida, bloqueia o usuário de acessar um site se o certificado for revogado.

**Passos**

1. Selecione **Definições › certificados**.
2. Selecione a guia **Trusted**.

   Você também pode ativar a verificação de revogação na guia **Key Management**.

3. Clique em **tarefas incomuns** e selecione **Ativar Verificação de revogação** no menu suspenso.
4. Selecione **quero ativar a verificação de revogação** para que uma marca de seleção apareça na caixa de seleção e campos adicionais apareçam na caixa de diálogo.
5. No campo **OCSP respondedor address**, você pode opcionalmente inserir um URL para um servidor de resposta OCSP. Se não introduzir um endereço, o sistema utiliza a URL do servidor OCSP a partir do ficheiro de certificado.
6. Clique em **Endereço de teste** para garantir que o sistema possa abrir uma conexão com o URL especificado.
7. Clique em **Salvar**.

**Resultados**

Se o storage de armazenamento tentar se conetar a um servidor com um certificado revogado, a conexão será negada e um evento será registrado.

### Excluir certificados confiáveis

Você pode excluir os certificados instalados pelo usuário importados anteriormente da guia confiável.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Se você estiver atualizando um certificado confiável com uma nova versão, o certificado atualizado deve ser importado antes de excluir o certificado antigo.

Poderá perder o acesso a um sistema se eliminar um certificado utilizado para autenticar os controladores e outro servidor, como um servidor LDAP, antes de importar um certificado de substituição.

**Sobre esta tarefa**

Esta tarefa descreve como eliminar certificados instalados pelo utilizador. Os certificados pré-instalados e auto-assinados não podem ser eliminados.

**Passos**

1. Selecione **Definições › certificados**.
2. Selecione a guia **Trusted**.

   A tabela mostra os certificados confiáveis do storage array.

3. Na tabela, selecione o certificado que deseja remover.
4. Clique em **tarefas incomuns › Delete**.

   Uma caixa de diálogo confirmar Excluir certificado confiável é aberta.

5. Digite `delete` o campo e clique em **Excluir**.

### Use certificados assinados pela CA para autenticação com um servidor de gerenciamento de chaves

Para comunicações seguras entre um servidor de gerenciamento de chaves e os controladores de storage array, você deve configurar os conjuntos apropriados de certificados.

**Antes de começar**

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.

**Sobre esta tarefa**

A autenticação entre os controladores e um servidor de gerenciamento de chaves é um procedimento de duas etapas.

#### Etapa 1: Conclua e envie CSR para autenticação com um servidor de gerenciamento de chaves

Primeiro, você deve gerar um arquivo de solicitação de assinatura de certificado (CSR) e usar o CSR para solicitar um certificado de cliente assinado de uma autoridade de certificação (CA) confiável pelo servidor de gerenciamento de chaves. Você também pode criar e baixar um certificado de cliente a partir do servidor de gerenciamento de chaves usando o arquivo CSR baixado. Um certificado de cliente valida os controladores do storage array, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP (Key Management Interoperability Protocol).

**Passos**

1. Selecione **Definições › certificados**.
2. Na guia Gerenciamento de chaves, selecione **Complete CSR**.
3. Introduza as seguintes informações:
   - * Nome comum* — um nome que identifica este CSR, como o nome da matriz de armazenamento, que será exibido nos arquivos de certificado.

- **Organização** — o nome completo e legal de sua empresa ou organização. Inclua sufixos, como Inc. Ou Corp.
- * Unidade organizacional (opcional) * — a divisão da sua organização que está a lidar com o certificado.
- **Cidade/localidade** — a cidade ou localidade onde sua organização está localizada.
- **Estado/região (opcional)** — o estado ou a região onde sua organização está localizada.
- **Código ISO do país** — o código ISO de dois dígitos (Organização Internacional para Padronização), como EUA, onde sua organização está localizada.

4. Clique em **Download**.

   Um ficheiro CSR é guardado no seu sistema local.

5. Solicite um certificado de cliente assinado a partir de uma CA confiável pelo servidor de gerenciamento de chaves.
6. Quando tiver um certificado de cliente, vá para Etapa 2: Importar certificados para o servidor de gerenciamento de chaves.

#### Etapa 2: Importar certificados para o servidor de gerenciamento de chaves

Como próxima etapa, você importa certificados para autenticação entre o storage array e o servidor de gerenciamento de chaves. Existem dois tipos de certificados: O certificado do cliente valida os controladores da matriz de armazenamento, enquanto o certificado do servidor de gestão de chaves valida o servidor. Você deve carregar o arquivo de certificado do cliente para os controladores e o arquivo de certificado do servidor para o servidor de gerenciamento de chaves.

**Antes de começar**

- Você tem um arquivo de certificado de cliente assinado (Etapa 1: Conclua e envie CSR para autenticação com um servidor de gerenciamento de chavesconsulte ) e copiou esse arquivo para o host onde está acessando o System Manager. Um certificado de cliente valida os controladores do storage array, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP (Key Management Interoperability Protocol).
- Você deve recuperar um arquivo de certificado do servidor de gerenciamento de chaves e, em seguida, copiar esse arquivo para o host onde você está acessando o System Manager. Um certificado do servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, de modo que o storage array possa confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou servidor para o servidor de gerenciamento de chaves.

> Para obter mais informações sobre o certificado do servidor, consulte a documentação do servidor de gerenciamento de chaves.

**Passos**

1. Selecione **Definições › certificados**.
2. Na guia Gerenciamento de chaves, selecione **Importar**.

   Abre-se uma caixa de diálogo para importar os ficheiros de certificado.

3. Ao lado de **Selecionar certificado de cliente**, clique no botão **Procurar** para selecionar o arquivo de certificado de cliente para os controladores da matriz de armazenamento.

   O nome do arquivo é exibido na caixa de diálogo.

4. Ao lado de **Selecione o certificado do servidor de gerenciamento de chaves**, clique no botão **Procurar** para selecionar o arquivo de certificado do servidor para o servidor de gerenciamento de chaves. Você pode escolher um certificado de raiz, intermediário ou servidor para o servidor de gerenciamento de chaves.

   O nome do arquivo é exibido na caixa de diálogo.

5. Clique em **Importar**.

   Os arquivos são carregados e validados.

#### Exportar certificados do servidor de gerenciamento de chaves

Pode guardar um certificado para um servidor de gestão de chaves na sua máquina local.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Os certificados devem ser importados anteriormente.

**Passos**

1. Selecione **Definições › certificados**.
2. Selecione a guia **Key Management**.
3. Na tabela, selecione o certificado que deseja exportar e clique em **Exportar**.

   Abre-se uma caixa de diálogo Guardar.

4. Digite um nome de arquivo e clique em **Salvar**.

## FAQs

#### Por que a caixa de diálogo não é possível acessar outro controlador aparece?

Quando você executa determinadas operações relacionadas a certificados de CA (por exemplo, importando um certificado), você pode ver uma caixa de diálogo solicitando que você aceite um certificado autoassinado para o segundo controlador.

Em matrizes de armazenamento com dois controladores (configurações duplex), esta caixa de diálogo às vezes aparece se o Gerenciador de sistema SANtricity não puder se comunicar com o segundo controlador ou se o navegador não puder aceitar o certificado durante um determinado ponto de uma operação.

Se esta caixa de diálogo abrir, clique em **aceitar certificado autoassinado** para continuar. Se outra caixa de diálogo solicitar uma senha, digite a senha do administrador usada para acessar o System Manager.

Se esta caixa de diálogo aparecer novamente e não for possível concluir uma tarefa de certificado, tente um dos seguintes procedimentos:

- Use um tipo de navegador diferente para acessar esse controlador, aceitar o certificado e continuar.
- Acesse o segundo controlador comSystem Manager, aceite o certificado autoassinado e, em seguida, retorne ao primeiro controlador e continue.

**Como sei quais certificados precisam ser carregados no System Manager para gerenciamento de chaves externas?**

Para o gerenciamento de chaves externas, você importa dois tipos de certificados para autenticação entre o storage array e o servidor de gerenciamento de chaves para que as duas entidades possam confiar umas nas outras.

Um certificado de cliente valida os controladores do storage array, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP (Key Management Interoperability Protocol). Para obter um certificado de cliente, use o System Manager para concluir um CSR para a matriz de armazenamento. Em seguida, você pode fazer o upload do CSR para um servidor de gerenciamento de chaves e gerar um certificado de cliente a partir daí. Depois de ter um certificado de cliente, copie esse arquivo para o host onde você está acessando o System Manager.

Um certificado do servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, de modo que o storage array possa confiar em seu endereço IP. Recupere o arquivo de certificado do servidor do servidor de gerenciamento de chaves e copie esse arquivo para o host onde você está acessando o System Manager.

**O que eu preciso saber sobre a verificação de revogação de certificados?**

O System Manager permite verificar se há certificados revogados usando um servidor OCSP (Online Certificate Status Protocol), em vez de carregar listas de revogação de certificados (CRLs).

Os certificados revogados não devem mais ser confiáveis. Um certificado pode ser revogado por vários motivos; por exemplo, se a Autoridade de Certificação (CA) emitiu incorretamente o certificado, uma chave privada foi comprometida ou a entidade identificada não aderiu aos requisitos da política.

Depois de estabelecer uma conexão com um servidor OCSP no Gerenciador de sistema, o storage array executa a verificação de revogação sempre que se coneta a um servidor AutoSupport, servidor de gerenciamento de chave externa (EKMS), servidor Lightweight Directory Access Protocol over SSL (LDAPS) ou a um servidor Syslog. O storage array tenta validar os certificados desses servidores para garantir que eles não foram revogados. O servidor então retorna um valor de "bom", "revogado" ou "desconhecido" para esse certificado. Se o certificado for revogado ou o array não puder entrar em Contato com o servidor OCSP, a conexão será recusada.

Especificar um endereço de resposta OCSP no System Manager ou na interface de linha de comando (CLI) substitui o endereço OCSP encontrado no arquivo de certificado.

**Para que tipos de servidores a verificação de revogação será ativada?**

A matriz de armazenamento executa a verificação de revogação sempre que se coneta a um servidor AutoSupport, servidor de gerenciamento de chaves externas (EKMS), servidor Lightweight Directory Access Protocol over SSL (LDAPS) ou a um servidor Syslog.

# Suporte

## Visão geral do suporte

A página de suporte fornece acesso a recursos de suporte técnico.

### Quais tarefas de suporte estão disponíveis?

No suporte, você pode visualizar Contatos de suporte técnico, executar diagnósticos, configurar o AutoSupport, exibir o log de eventos e executar atualizações de software.

Saiba mais:

- "Visão geral do recurso AutoSupport"
- "Visão geral do log de eventos"
- "Visão geral do Centro de atualizações"

### Como posso entrar em Contato com o suporte técnico?

Na página principal, clique no **suporte › Centro de suporte › separador recursos de suporte**. As informações de Contato do suporte técnico estão listadas no canto superior direito da interface.

## Exibir informações e diagnósticos

### Ver o perfil da matriz de armazenamento

O perfil do storage array fornece uma descrição de todos os componentes e propriedades do storage array.

#### Sobre esta tarefa

Você pode usar o perfil do storage array como auxiliar durante a recuperação ou como uma visão geral da configuração atual do storage array. Talvez você queira salvar uma cópia do perfil do storage array no cliente de gerenciamento e manter uma cópia impressa do perfil do storage array com o storage array. Crie uma nova cópia do perfil de storage array se a configuração mudar.

#### Passos

1. Selecione o menu:guia Support [Support Center > Support Resources] (suporte > recursos de suporte).
2. Role para baixo até **Launch detailed storage array information** e selecione **Storage Array Profile**.

   O relatório é apresentado no ecrã.

**Detalhes do campo**

| Secção | Descrição |
| --- | --- |
| Storage array | Mostra todas as opções que você pode configurar e as opções estáticas do sistema para sua matriz de armazenamento. Essas opções incluem o número de controladores, compartimentos de unidades, unidades, pools de discos, grupos de volumes, volumes e unidades hot spare; o número máximo de compartimentos de unidades, unidades, discos de estado sólido (SSDs) e volumes permitidos; o número de grupos de snapshot, imagens de snapshot, volumes de snapshot e grupos de consistência; AutoSupport informações sobre recursos AutoSupport |
| Armazenamento | Mostra uma lista de todos os dispositivos de armazenamento na matriz de armazenamento. Dependendo da configuração do storage array, a seção armazenamento pode mostrar essas subseções.<br>• **Disk Pools** — mostra uma lista de todos os pools de discos na matriz de armazenamento.<br>• **Grupos de volume** — mostra uma lista de todos os grupos de volume na matriz de armazenamento. Volumes e capacidade livre são listados na ordem em que foram criados.<br>• **Volumes** — mostra uma lista de todos os volumes na matriz de armazenamento. As informações listadas incluem o nome do volume, o status do volume, a capacidade, o nível RAID, o grupo de volumes ou o pool de discos, o tipo de unidade e detalhes adicionais.<br>• **Volumes ausentes** — mostra uma lista de todos os volumes na matriz de armazenamento que atualmente têm um status ausente. As informações listadas incluem o World Wide Identifier (WWID) para cada volume em falta. |

| Secção | Descrição |
| --- | --- |
| Serviços de cópia | Mostra uma lista de todos os serviços de cópia usados para o storage array. Dependendo da configuração do storage array, a seção Serviços de cópia pode mostrar estas subseções:<br>• **Cópias de volume** — mostra uma lista de todos os pares de cópias na matriz de armazenamento. As informações listadas incluem o número de cópias, os nomes dos pares de cópias, o status, o carimbo de data/hora inicial e detalhes adicionais.<br>• **Grupos de instantâneos** — mostra uma lista de todos os grupos de instantâneos na matriz de armazenamento.<br>• **Snapshot Images** — mostra uma lista de todos os instantâneos no storage array.<br>• **Volumes instantâneos** — mostra uma lista de todos os volumes instantâneos no storage array.<br>• **Grupos de consistência** — mostra uma lista de todos os grupos de consistência na matriz de armazenamento.<br>• **Volumes de membros** — mostra uma lista de todos os volumes de membros do grupo de consistência na matriz de armazenamento.<br>• **Grupos de espelho** — mostra uma lista de todos os volumes espelhados.<br>• **Capacidade reservada** — mostra uma lista de todos os volumes de capacidade reservada na matriz de armazenamento. |
| Atribuições do host | Mostra uma lista de atribuições de host no storage array. As informações listadas incluem o nome do volume, o número de unidade lógica (LUN), o ID do controlador, o nome do host ou o nome do cluster do host e o status do volume. As informações adicionais listadas incluem definições de topologia e definições de tipo de host. |

| Secção | Descrição |
| --- | --- |
| Hardware | Mostra uma lista de todo o hardware na matriz de armazenamento. Dependendo da configuração da matriz de armazenamento, a seção hardware pode mostrar essas subseções.<br><br>• **Controllers** — mostra uma lista de todos os controladores na matriz de armazenamento e inclui a localização, o estado e a configuração do controlador. Além disso, ele inclui informações do canal da unidade, informações do canal do host e informações da porta Ethernet.<br>• **Drives** — mostra uma lista de todas as unidades no storage de armazenamento. As unidades são listadas em ID do compartimento, ID da gaveta, ordem de ID do slot. As informações listadas incluem o ID do compartimento, o ID da gaveta, o ID do slot, o status, a capacidade bruta, o tipo de Mídia, o tipo de interface, a taxa de dados atual, o ID do produto e a versão do firmware para cada unidade. A seção Drive também inclui informações sobre o canal da unidade, informações sobre a cobertura hot spare e informações sobre a vida útil (somente para unidades SSD). As informações de vida útil incluem a porcentagem de resistência usada, que é a quantidade de dados gravados nas unidades SSD até o momento, dividida pelo limite teórico total de gravação para as unidades.<br>• **Canais de unidade** — mostra informações para todos os canais de unidade na matriz de armazenamento. As informações listadas incluem o status do canal, o status do link (se aplicável), contagens de unidades e contagens de erros cumulativos.<br>• * Prateleiras* — mostra informações para todas as prateleiras no storage array. As informações listadas incluem tipos de unidade e informações de status para cada componente do compartimento. Os componentes da gaveta podem incluir pacotes de bateria, transcetores SFP (Small Form-factor Pluggable), coletores de ventilador de energia ou latas de IOM (módulo de entrada/saída). A seção hardware também mostra o identificador da chave de segurança se uma chave de segurança for usada pelo storage array. |
| Caraterísticas | Mostra uma lista dos pacotes de recursos instalados e o número máximo permitido de grupos de snapshots, snapshots (legados) e volumes por host ou cluster de host. As informações na seção recursos também incluem Segurança da unidade; ou seja, se a matriz de armazenamento está habilitada para segurança ou a segurança está desativada. |

3. Para pesquisar o perfil do storage array, digite um termo de pesquisa na caixa de texto **Localizar** e clique em **Localizar**.

   Todos os termos correspondentes são realçados. Para percorrer todos os resultados um de cada vez, continue a clicar em **Localizar**.

4. Para salvar o perfil da matriz de armazenamento, clique em **Salvar**.

   O arquivo é salvo na pasta Downloads do navegador com o nome `storage-array-profile.txt`.

### Veja o inventário de software e firmware

O inventário de software e firmware lista as versões de firmware para cada componente em sua matriz de armazenamento.

#### Sobre esta tarefa

Um storage array é composto por muitos componentes, que podem incluir controladores, unidades, gavetas e módulos de entrada/saída (IOMs). Cada um destes componentes contém firmware. Algumas versões do firmware dependem de outras versões do firmware. Para capturar informações sobre todas as versões de firmware em sua matriz de armazenamento, consulte o inventário de software e firmware. O suporte técnico pode analisar o inventário de software e firmware para detetar quaisquer problemas de firmware.

#### Passos

1. Selecione o menu:guia Support [Support Center > Support Resources] (suporte > recursos de suporte).
2. Role para baixo até **Launch detailed storage array information** e selecione **Software and firmware Inventory**.

   O relatório de inventário de software e firmware é apresentado no ecrã.

3. Para salvar o inventário de software e firmware, clique em **Salvar**.

   O arquivo é salvo na pasta Downloads do navegador com o nome do `firmware-inventory.txt`arquivo .

4. Siga as instruções fornecidas pelo suporte técnico para enviar o arquivo para eles.

## Recolher dados de diagnóstico

### Colete dados de suporte manualmente

Você pode reunir vários tipos de inventário, status e dados de desempenho sobre seu storage array em um único arquivo. O suporte técnico pode usar o arquivo para solução de problemas e análises adicionais.

#### Sobre esta tarefa

Mais uma vez

> Se o recurso AutoSupport estiver ativado, você também poderá coletar esses dados acessando a guia **AutoSupport** e selecionando **Enviar Envio AutoSupport**.

Você pode executar apenas uma operação de coleta de cada vez. Se tentar iniciar outra operação, receberá uma mensagem de erro.

> Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

#### Passos

1. Selecione menu:guia Support [Support Center > Diagnostics] (suporte > Centro de suporte > Diagnóstico).
2. Selecione **coletar dados de suporte**.
3. Clique em **Collect**.

   O arquivo é salvo na pasta Downloads do navegador com o nome `support-data.7z`. Se a prateleira

contiver gavetas, os dados de diagnóstico dessa prateleira serão arquivados em um arquivo separado com zíper chamado `tray-component-state-capture.7z`.

4. Siga as instruções fornecidas pelo suporte técnico para enviar o arquivo para eles.

### Coletar dados de configuração

Você pode salvar os dados de configuração RAID do controlador, que inclui todos os dados para grupos de volumes e pools de discos. Em seguida, você pode entrar em Contato com o suporte técnico para obter assistência com a restauração dos dados.

#### Sobre esta tarefa

Esta tarefa descreve como salvar o estado atual do banco de dados de configuração RAID. Estes dados são recuperados a partir da localização da memória RPA do controlador.

> O recurso coletar dados de configuração salva as mesmas informações do comando CLI do `save storageArray dbmDatabase`.

Você só deve executar esta tarefa quando instruído por uma operação Recovery Guru ou por suporte técnico.

#### Passos

1. Selecione menu:guia Support [Support Center > Diagnostics] (suporte > Centro de suporte > Diagnóstico).
2. Selecione **Collect Configuration Data**.
3. Na caixa de diálogo, clique em **Collect**.

   O arquivo , `configurationData-<arrayName>-<dateTime>.7z` é salvo na pasta Downloads do navegador.

4. Entre em Contato com o suporte técnico para obter mais informações sobre como enviar o arquivo para eles e para carregar os dados de volta para o sistema.

### Recuperar arquivos de suporte de recuperação

O suporte técnico pode usar arquivos de suporte de recuperação para solucionar problemas. O System Manager salva automaticamente esses arquivos.

#### Antes de começar

O suporte técnico solicitou que você lhes enviasse arquivos adicionais para solução de problemas.

#### Sobre esta tarefa

Os arquivos de suporte de recuperação incluem estes tipos de arquivos:

- Suporta arquivos de dados
- História da AutoSupport
- Log do AutoSupport
- Arquivos de diagnóstico SAS/RLS
- Dados do perfil de recuperação
- Arquivos de captura de banco de dados

**Passos**

1. Selecione menu:guia Support [Support Center > Diagnostics] (suporte > Centro de suporte > Diagnóstico).
2. Selecione **recuperar arquivos de suporte de recuperação**.

   Uma caixa de diálogo lista todos os arquivos de suporte de recuperação que seu storage array coletou. Para encontrar arquivos específicos, você pode classificar qualquer uma das colunas ou digitar carateres na caixa **filtro**.

3. Selecione um arquivo e clique em **Download**.

   O arquivo é salvo na pasta Downloads do navegador.

4. Se você precisar salvar arquivos adicionais, repita a etapa anterior.
5. Clique em **Fechar**.
6. Siga as instruções fornecidas pelo suporte técnico para enviar o arquivo para eles.

### Recupere buffers de rastreamento

Você pode recuperar os buffers de rastreamento dos controladores e enviar o arquivo para suporte técnico para análise.

**Sobre esta tarefa**

O firmware usa os buffers de rastreamento para gravar o processamento, especialmente as condições de exceção, que podem ser úteis para depuração. Você pode recuperar buffers de rastreamento sem interromper a operação do storage array e com efeito mínimo no desempenho.

Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

**Passos**

1. Selecione menu:guia Support [Support Center > Diagnostics] (suporte > Centro de suporte > Diagnóstico).
2. Selecione **Retrieve Trace Buffers**.
3. Marque a caixa de seleção ao lado de cada controlador para o qual você deseja recuperar buffers de rastreamento.

   Pode selecionar um ou ambos os controladores. Se a mensagem de status do controlador à direita de uma caixa de seleção for Falha ou Desativado, a caixa de seleção será desativada.

4. Clique em **Sim**.

   O arquivo é salvo na pasta Downloads do navegador com o nome do `trace-buffers.7z`arquivo .

5. Siga as instruções fornecidas pelo suporte técnico para enviar o arquivo para eles.

### Colete estatísticas de caminho de e/S.

Você pode salvar o arquivo de estatísticas de caminho de e/S e enviá-lo para o suporte técnico para análise.

**Sobre esta tarefa**

O suporte técnico usa as estatísticas de caminho de e/S para ajudar a diagnosticar problemas de

desempenho. Os problemas de desempenho do aplicativo podem ser causados pela utilização de memória, utilização de CPU, latência de rede, latência de e/S ou outros problemas. As estatísticas de caminho de e/S são coletadas automaticamente durante a coleta de dados de suporte ou você pode coletá-las manualmente. Além disso, se você tiver o AutoSupport ativado, as estatísticas de caminho de e/S serão coletadas automaticamente e enviadas para o suporte técnico.

Os contadores para as estatísticas do caminho de e/S são repostos depois de confirmar que pretende recolher as estatísticas do caminho de e/S. Os contadores são repostos mesmo que cancele a operação posteriormente. Os contadores também são repostos quando o controlador é reposto (reinicializa).

Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

**Passos**

1. Selecione menu:guia Support [Support Center > Diagnostics] (suporte > Centro de suporte > Diagnóstico).
2. Selecione **Collect I/o Path Statistics**.
3. Confirme se deseja executar a operação digitando `collect`e clique em **Collect**.

   O arquivo é salvo na pasta Downloads do navegador com o nome do `io-path-statistics.7z`arquivo .

4. Siga as instruções fornecidas pelo suporte técnico para enviar o arquivo para eles.

### Recupere a imagem de integridade

Pode rever uma imagem de estado do controlador. Uma imagem de integridade é um despejo de dados brutos da memória do processador do controlador que o suporte técnico pode usar para diagnosticar um problema com um controlador.

**Sobre esta tarefa**

O firmware gera automaticamente uma imagem de integridade quando deteta determinados erros. Depois que uma imagem de integridade é gerada, o controlador que teve o erro reinicializa e um evento é registrado no log de eventos.

Se você tiver o AutoSupport ativado, a imagem de integridade será enviada automaticamente para o suporte técnico. Se você não tiver o AutoSupport ativado, entre em Contato com o suporte técnico para obter instruções sobre como recuperar a imagem de integridade e enviá-la para eles para análise.

Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

**Passos**

1. Selecione menu:guia Support [Support Center > Diagnostics] (suporte > Centro de suporte > Diagnóstico).
2. Selecione **Retrieve Health Image**.

   Você pode olhar para a seção de detalhes para ver o tamanho da imagem de integridade antes de baixar o arquivo.

3. Clique em **Collect**.

   O arquivo é salvo na pasta Downloads do navegador com o nome `health-image.7z`.

4. Siga as instruções fornecidas pelo suporte técnico para enviar o arquivo para eles.

# Tome ações de recuperação

## Exibir log de setores ilegíveis

Você pode salvar o log de setores ilegíveis e enviar o arquivo para o suporte técnico para análise.

### Sobre esta tarefa

O log de setores ilegíveis contém Registros detalhados de setores ilegíveis causados por unidades que relatam erros de Mídia irrecuperáveis. Setores ilegíveis são detetados durante e/S normais e durante operações de modificação, como reconstruções. Quando setores ilegíveis são detetados em um storage array, um alerta precisa de atenção aparece para o storage array. O Recovery Guru distingue qual condição de setor ilegível precisa de atenção. Quaisquer dados contidos em um setor ilegível não podem ser recuperados e devem ser considerados perdidos.

O log de setores ilegíveis pode armazenar até 1.000 setores ilegíveis. Quando o log de setores ilegíveis atinge 1.000 entradas, as seguintes condições se aplicam:

- Se forem detetados novos setores ilegíveis durante a reconstrução, a reconstrução falhará e não será registada qualquer entrada.
- Para novos setores ilegíveis detetados durante a e/S, a e/S falha e nenhuma entrada é registrada.

> Essas ações incluem gravações RAID 5 e gravações RAID 6 que teriam sido bem-sucedidas antes do estouro.

> • Possível perda de dados * - recuperação de setores ilegíveis é um procedimento complicado que pode envolver vários métodos diferentes. Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

### Passos

1. Selecione menu:guia Support [Support Center > Diagnostics] (suporte > Centro de suporte > Diagnóstico).
2. Selecione **Exibir/Limpar setores ilegíveis**.
3. Para salvar o log de setores ilegíveis:

   a. Na primeira coluna da tabela, você pode selecionar volumes individuais para os quais deseja salvar o log de setores ilegíveis (clique na caixa de seleção ao lado de cada volume) ou selecionar todos os volumes (marque a caixa de seleção no cabeçalho da tabela).

      Para encontrar volumes específicos, você pode classificar qualquer uma das colunas ou digitar carateres na caixa **filtro**.

   b. Clique em **Salvar**.

   O arquivo é salvo na pasta Downloads do navegador com o nome `unreadable-sectors.txt`.

4. Se o suporte técnico lhe der instruções para limpar o log de setores ilegíveis, execute as seguintes etapas:

   a. Na primeira coluna da tabela, você pode selecionar volumes individuais para os quais deseja limpar o log de setores ilegíveis (clique na caixa de seleção ao lado de cada volume) ou selecionar todos os volumes (marque a caixa de seleção no cabeçalho da tabela).

   b. Clique em **Clear** e confirme que deseja executar a operação.

### Reative as portas da unidade

Pode indicar ao controlador que foi tomada uma ação corretiva para recuperar de uma condição de fio incorreto.

#### Passos

1. Selecione menu:guia Support [Support Center > Diagnostics] (suporte > Centro de suporte > Diagnóstico).
2. Selecione **reativar portas de unidade** e confirme se deseja executar a operação.

   Esta opção aparece apenas quando a matriz de armazenamento tiver desativado as portas da unidade.

   O controlador rehabilita todas as portas SAS que foram desativadas quando um fio incorreto foi detetado.

### Limpar o modo de recuperação

Depois de restaurar uma configuração de storage array, use a operação Clear Recovery Mode para retomar a e/S no storage array e retornar às operações normais.

#### Antes de começar

- Se você quiser retornar a matriz de armazenamento para uma configuração anterior, você deve restaurar a configuração do backup antes de limpar o modo de recuperação.
- Você deve executar verificações de validação ou verificar com o suporte técnico para garantir que a restauração foi bem-sucedida. Depois de determinar que a restauração foi bem-sucedida, o modo de recuperação pode ser limpo.

#### Sobre esta tarefa

O storage array contém um banco de dados de configuração que inclui um Registro de sua configuração lógica (pools, grupos de volumes, volumes, etc.). Se você limpar intencionalmente a configuração do storage array ou se o banco de dados de configuração for corrompido, o storage array entrará no modo de recuperação. O modo de recuperação pára e/S e congela o banco de dados de configuração, o que lhe dá tempo para fazer um dos seguintes procedimentos:

- Restaure a configuração a partir do backup automático armazenado nos dispositivos flash do controlador. Você deve entrar em Contato com o suporte técnico para fazer isso.
- Restaure a configuração a partir de uma operação anterior Guardar base de dados de configuração. As operações do banco de dados de configuração são realizadas através da interface de linha de comando (CLI).
- Reconfigure a matriz de armazenamento do zero.

Depois que a configuração do storage array for restaurada ou redefinida e você tiver verificado que tudo está bem, você deve limpar manualmente o modo de recuperação.

> Não é possível cancelar a operação Clear Recovery Mode (Limpar modo de recuperação) depois de iniciada. Limpar o modo de recuperação pode demorar muito tempo. Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

#### Passos

1. Selecione menu:guia Support [Support Center > Diagnostics] (suporte > Centro de suporte > Diagnóstico).
2. Selecione **Clear Recovery Mode** (Limpar modo de recuperação) e confirme que pretende executar esta operação.

Esta opção aparece apenas se a matriz de armazenamento estiver no modo de recuperação.

## Gerenciar o AutoSupport

### Visão geral do recurso AutoSupport

O recurso AutoSupport monitora a integridade de um storage array e envia patches automáticos para o suporte técnico.

O suporte técnico usa os dados do AutoSupport de forma reativa para acelerar o diagnóstico e a resolução de problemas do cliente, além de detectar e evitar problemas em potencial proativamente.

Os dados do AutoSupport incluem informações sobre a configuração, o status, o desempenho e os eventos do sistema de um storage array. Os dados do AutoSupport não contêm nenhum dado de usuário. Os envios podem ser enviados imediatamente ou de acordo com um horário (diário e semanal).

#### Principais benefícios

Alguns dos principais benefícios do recurso AutoSupport incluem:

- Tempos acelerados de resolução de casos
- Monitoramento sofisticado para gerenciamento mais rápido de incidentes
- Relatórios automatizados de acordo com um cronograma, bem como relatórios automatizados sobre eventos críticos
- Solicitações automatizadas de substituição de hardware para componentes selecionados, como unidades
- Alerta não intrusivo para notificá-lo de um problema e fornecer informações para suporte técnico para tomar medidas corretivas
- Ferramentas de análise do AutoSupport que monitoram despachos para problemas de configuração conhecidos

#### Recursos individuais do AutoSupport

O recurso AutoSupport é composto por três recursos individuais que você ativa separadamente.

- **Basic AutoSupport** — permite que sua matriz de armazenamento colete e envie dados automaticamente para o suporte técnico.
- **AutoSupport OnDemand** — permite que o suporte técnico solicite a retransmissão de um despacho AutoSupport anterior quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir da matriz de armazenamento, não do servidor AutoSupport. A matriz de armazenamento verifica periodicamente com o servidor AutoSupport para determinar se existem solicitações de retransmissão pendentes e responde de acordo.
- **Diagnóstico remoto** — permite que o suporte técnico solicite um novo e atualizado despacho do AutoSupport quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir da matriz de armazenamento, não do servidor AutoSupport. O storage array verifica periodicamente com o servidor AutoSupport para determinar se há novas solicitações pendentes e responde de acordo.

#### Diferença entre AutoSupport e coletar dados de suporte

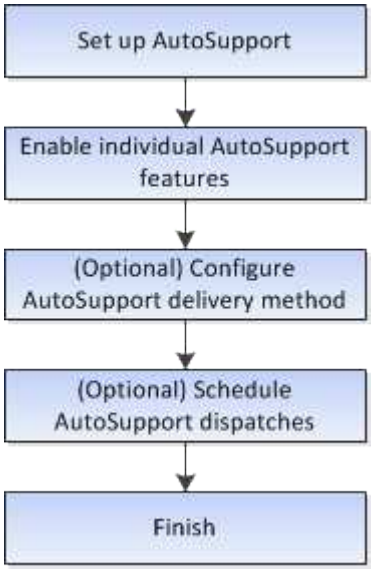
Existem dois métodos de coleta de dados de suporte na matriz de armazenamento:

- **Recurso AutoSupport** — os dados são coletados automaticamente.
- **Opção coletar dados de suporte** — os dados devem ser coletados e enviados manualmente.

O recurso AutoSupport é mais fácil de usar porque os dados são coletados e enviados automaticamente. Os dados do AutoSupport podem ser usados proativamente para evitar problemas antes que eles ocorram. O recurso AutoSupport acelera a solução de problemas porque o suporte técnico já tem acesso aos dados. Por esses motivos, o recurso AutoSupport é o método de coleta de dados preferido a ser usado.

#### Fluxo de trabalho para o recurso AutoSupport

No Gerenciador de sistema, você configura o recurso AutoSupport seguindo estas etapas.




#### Ative ou desative os recursos do AutoSupport

Você ativa o recurso AutoSupport e os recursos individuais do AutoSupport durante a configuração inicial ou pode ativá-los ou desativá-los posteriormente.

##### Antes de começar

Se você quiser ativar o AutoSupport OnDemand ou o Diagnóstico remoto, o método de entrega do AutoSupport deve ser definido como HTTPS.

##### Sobre esta tarefa

Você pode desativar o recurso AutoSupport a qualquer momento, mas é altamente recomendável que o deixe habilitado. A ativação do recurso AutoSupport pode acelerar significativamente a determinação e a resolução de problemas caso ocorra um problema no storage array.

O recurso AutoSupport é composto por três recursos individuais que você ativa separadamente.

- **Basic AutoSupport** — permite que sua matriz de armazenamento colete e envie dados automaticamente para o suporte técnico.
- **AutoSupport OnDemand** — permite que o suporte técnico solicite a retransmissão de um despacho AutoSupport anterior quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir da matriz de armazenamento, não do servidor AutoSupport. A matriz de armazenamento verifica periodicamente com o servidor AutoSupport para determinar se existem solicitações de

retransmissão pendentes e responde de acordo.

- **Diagnóstico remoto** — permite que o suporte técnico solicite um novo e atualizado despacho do AutoSupport quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir da matriz de armazenamento, não do servidor AutoSupport. O storage array verifica periodicamente com o servidor AutoSupport para determinar se há novas solicitações pendentes e responde de acordo.

**Passos**

1. Selecione **suporte › Centro de suporte › AutoSupport**.
2. Selecione **Ativar/Desativar recursos do AutoSupport**.
3. Marque as caixas de seleção ao lado dos recursos do AutoSupport que você deseja habilitar.

   As funcionalidades dependem umas das outras, conforme indicado pela indentação dos itens na caixa de diálogo. Por exemplo, você deve habilitar o OnDemand do AutoSupport antes de ativar o Diagnóstico remoto.

4. Clique em **Salvar**.

   Se desativar o AutoSupport, é apresentada uma notificação na página inicial. Você pode ignorar a notificação clicando em **Ignorar**.

### Configurar o método de entrega do AutoSupport

O recurso AutoSupport oferece suporte aos protocolos HTTPS, HTTP e SMTP para entrega de despachos para suporte técnico.

**Antes de começar**

- O recurso AutoSupport deve estar ativado. Você pode ver se ele está habilitado na página AutoSupport.
- Um servidor DNS deve ser instalado e configurado na rede. O endereço do servidor DNS deve ser configurado no System Manager (esta tarefa está disponível na página hardware).

**Sobre esta tarefa**

Reveja os diferentes protocolos:

- **HTTPS** — permite que você se conete diretamente ao servidor de suporte técnico de destino usando HTTPS. Se você quiser ativar o AutoSupport OnDemand ou o Diagnóstico remoto, o método de entrega do AutoSupport deve ser definido como HTTPS.
- **HTTP** — permite que você se conete diretamente ao servidor de suporte técnico de destino usando HTTP.
- **Email** — permite que você use um servidor de e-mail como o método de entrega para enviar despachos AutoSupport.

> **Diferenças entre os métodos HTTPS/HTTP e Email**. O método de entrega de e-mail, que usa SMTP, tem algumas diferenças importantes em relação aos métodos de entrega HTTPS e HTTP. Primeiro, o tamanho dos envios para o método Email está limitado a 5MB, o que significa que algumas coleções de dados ASUP não serão enviadas. Em segundo lugar, o recurso AutoSupport OnDemand está disponível somente nos métodos HTPP e HTTPS.

**Passos**

1. Selecione **suporte › Centro de suporte › AutoSupport**.
2. Selecione **Configurar método de entrega AutoSupport**.

Uma caixa de diálogo é exibida, que lista os métodos de entrega de despacho.

3. Selecione o método de entrega desejado e, em seguida, selecione os parâmetros para esse método de entrega. Execute um dos seguintes procedimentos:
   - Se você selecionou HTTPS ou HTTP, selecione um dos seguintes parâmetros de entrega:
     - **Directly** — este parâmetro de entrega é a seleção padrão. Escolher esta opção permite que você se conete diretamente ao sistema de suporte técnico de destino usando o protocolo HTTPS ou HTTP.
     - **Via servidor Proxy** — escolher esta opção permite especificar os detalhes do servidor proxy HTTP necessários para estabelecer conexão com o sistema de suporte técnico de destino. Você deve especificar o endereço do host e o número da porta. No entanto, você só precisa inserir os detalhes de autenticação do host (nome de usuário e senha), se necessário.
     - **Via Proxy auto-Configuration script (PAC)** — Especifique a localização de um arquivo de script de configuração automática de proxy (PAC). Um arquivo PAC permite que o sistema escolha automaticamente o servidor proxy apropriado para estabelecer uma conexão com o sistema de suporte técnico de destino.
   - Se você selecionou e-mail, insira as seguintes informações:
     - O endereço do servidor de correio como um nome de domínio totalmente qualificado, endereço IPv4 ou endereço IPv6.
     - O endereço de e-mail que aparece no campo de do e-mail de envio do AutoSupport.
     - **Opcional; se você quiser executar um teste de configuração**: O endereço de e-mail onde uma confirmação é enviada quando o sistema AutoSupport recebe o envio do teste.
     - Se você quiser criptografar mensagens, selecione **SMTPS** ou **STARTTLS** para o tipo de criptografia e, em seguida, selecione o número da porta para mensagens criptografadas. Caso contrário, selecione **nenhum**.
     - Se necessário, introduza um nome de utilizador e uma palavra-passe para autenticação com o remetente de saída e o servidor de correio.
4. Se você tiver um firewall que bloqueia a entrega desses envios ASUP, adicione o seguinte URL à sua lista de permissões: `https://support.netapp.com/put/AsupPut/`
5. Clique em **Configuração de teste** para testar a conexão com o servidor de suporte técnico usando os parâmetros de entrega especificados. Se você ativou o recurso AutoSupport On-Demand, o sistema também testará a conexão para entrega de despacho do AutoSupport OnDemand.

   Se o teste de configuração falhar, verifique as configurações e execute o teste novamente. Se o teste continuar falhando, entre em Contato com o suporte técnico.
6. Clique em **Salvar**.

### Agendar envios do AutoSupport

O Gerenciador do sistema cria automaticamente uma programação padrão para envios do AutoSupport. Se preferir, você pode especificar sua própria programação.

#### Antes de começar

O recurso AutoSupport deve estar ativado. Você pode ver se ele está habilitado na página AutoSupport.

#### Sobre esta tarefa

- **Hora diária** — os envios diários são coletados e enviados todos os dias durante o intervalo de tempo que

você especificar. O System Manager seleciona um tempo aleatório durante o intervalo. Todos os tempos estão em tempo Universal coordenado (UTC), que pode ser diferente da hora local do storage array. Você deve converter a hora local do seu storage array em UTC.

- **Dia semanal** — as expedições semanais são coletadas e enviadas uma vez por semana. O System Manager seleciona um dia aleatório a partir dos dias especificados. Desmarque todos os dias em que você não deseja permitir que um envio semanal ocorra. O System Manager seleciona um dia aleatório a partir dos dias permitidos.
- **Horário semanal** — os envios semanais são coletados e enviados uma vez por semana durante o intervalo de tempo que você especificar. O System Manager seleciona um tempo aleatório durante o intervalo. Todos os tempos estão em tempo Universal coordenado (UTC), que pode ser diferente da hora local do storage array. Você deve converter a hora local do seu storage array em UTC.

**Passos**

1. Selecione **suporte › Centro de suporte › AutoSupport**.
2. Selecione **Agendar envios AutoSupport**.

   O assistente Agendar envios AutoSupport é exibido.

3. Siga as etapas do assistente.

### Enviar despachos AutoSupport

O System Manager permite enviar despachos AutoSupport para o suporte técnico, sem esperar por um despacho agendado.

**Antes de começar**

O recurso AutoSupport deve estar ativado. Você pode ver se ele está habilitado na página AutoSupport.

**Sobre esta tarefa**

Essa operação coleta dados de suporte e os envia automaticamente para o suporte técnico, para que eles possam solucionar problemas.

**Passos**

1. Selecione **suporte › Centro de suporte › AutoSupport**.
2. Selecione **Enviar Envio AutoSupport**.

   A caixa de diálogo Enviar Envio AutoSupport é exibida.

3. Confirme a operação selecionando **Enviar**.

### Ver o estado do AutoSupport

A página AutoSupport mostra se o recurso AutoSupport e os recursos individuais do AutoSupport estão ativados no momento.

**Passos**

1. Selecione **suporte › Centro de suporte › AutoSupport**.
2. Olhe para o lado direito da página logo abaixo das guias para ver se o recurso básico do AutoSupport está ativado.

3. Passe o cursor sobre o ponto de interrogação para ver se os recursos individuais do AutoSupport estão ativados.

### Ver log do AutoSupport

O log do AutoSupport fornece informações sobre status, histórico de despacho e erros encontrados durante a entrega de despachos do AutoSupport.

#### Sobre esta tarefa

Podem existir vários ficheiros de registo. Quando o arquivo de log atual atinge 200 KB, ele é arquivado e um novo arquivo de log é criado. O nome do arquivo de log arquivado é `ASUPMessages.n`, onde *n* é um número inteiro de 1 a 9. Se existirem vários ficheiros de registo, pode optar por visualizar o registo mais atual ou um registo anterior.

- * Registro atual* — mostra uma lista dos últimos eventos capturados.
- **Registro arquivado** — mostra uma lista de eventos anteriores.

#### Passos

1. Selecione **suporte › Centro de suporte › AutoSupport**.
2. Selecione **Ver Registo AutoSupport**.

   É apresentada uma caixa de diálogo que lista o registo AutoSupport atual.

3. Se você quiser ver os logs anteriores do AutoSupport, selecione o botão de opção **Arquivado** e selecione um log na lista suspensa **Selecionar log** AutoSupport.

   A opção Arquivado aparece apenas se existirem registos arquivados na matriz de armazenamento.

   O log AutoSupport selecionado é exibido na caixa de diálogo.

4. **Opcional:** para pesquisar o log do AutoSupport, digite um termo na caixa **Localizar** e clique em **Localizar**.

   Clique em **Find** novamente para procurar ocorrências adicionais do termo.

### Ative a janela de manutenção do AutoSupport

Ative a janela de manutenção do AutoSupport para suprimir a criação automática de tickets em eventos de erro. No modo de operação normal, o storage array usa o AutoSupport para abrir um caso com suporte se houver um problema.

#### Passos

1. Selecione **suporte › Centro de suporte › AutoSupport**.
2. Selecione **Ativar janela de manutenção do AutoSupport**.
3. Introduza o endereço de e-mail para receber uma confirmação de que o pedido da janela de manutenção foi processado.

   Dependendo da configuração, você poderá inserir até cinco endereços de e-mail. Se quiser adicionar mais de um endereço, selecione **Adicionar outro email** para abrir outro campo.

4. Especifique a duração (em horas) para ativar a janela de manutenção.

   A duração máxima suportada é de 72 horas.

5. Clique em **Sim**.

   A criação automática de tickets do AutoSupport em eventos de erro é temporariamente suprimida para a janela de duração especificada.

**Depois de terminar**

A janela de manutenção não começa até que a solicitação do storage array seja processada pelos servidores AutoSupport. Aguarde até receber um e-mail de confirmação antes de realizar quaisquer atividades de manutenção no seu storage array.

### Desative a janela de manutenção do AutoSupport

Desative a janela de manutenção do AutoSupport para permitir a criação automática de tickets em eventos de erro. Quando a janela de manutenção do AutoSupport estiver desativada, o storage array usará o AutoSupport para abrir um caso com suporte se houver um problema.

**Passos**

1. Selecione **suporte › Centro de suporte › AutoSupport**.
2. Selecione **Desativar a janela de manutenção do AutoSupport**.
3. Insira o endereço de e-mail para receber uma confirmação de que a solicitação da janela de desativação de manutenção foi processada.

   Dependendo da configuração, você poderá inserir até cinco endereços de e-mail. Se quiser adicionar mais de um endereço, selecione **Adicionar outro email** para abrir outro campo.

4. Clique em **Sim**.

   A criação automática de ticket do AutoSupport em eventos de erro está ativada.

**Depois de terminar**

A janela de manutenção não terminará até que a solicitação do storage array tenha sido processada pelos servidores AutoSupport. Aguarde até receber um e-mail de confirmação antes de prosseguir.

## Ver eventos

### Visão geral do log de eventos

O log de eventos fornece um Registro histórico de eventos que ocorreram no storage array, o que ajuda o suporte técnico na solução de problemas de eventos que levam a falhas.

Você pode usar o log de eventos como uma ferramenta de diagnóstico complementar ao Recovery Guru para rastrear eventos de storage array. Sempre consulte o Recovery Guru primeiro quando você tentar se recuperar de falhas de componentes no storage array.

#### Categorias de eventos

Os eventos no log de eventos são categorizados com status diferentes. Os eventos nos quais você precisa agir têm os seguintes status:

- Crítico
- Aviso

Os eventos que são informativos e não exigem nenhuma ação imediata são os seguintes:

- Informativo

#### Eventos críticos

Eventos críticos indicam um problema com o storage array. Se você resolver o evento crítico imediatamente, poderá evitar a perda de acesso aos dados.

Quando ocorre um evento crítico, ele é registrado no log de eventos. Todos os eventos críticos são enviados para o console de gerenciamento SNMP ou para o destinatário de e-mail que você configurou para receber notificações de alerta. Se o ID do compartimento não for conhecido no momento do evento, o ID do compartimento é listado como "prateleira desconhecida".

Quando receber um evento crítico, consulte o procedimento Recovery Guru para obter uma descrição detalhada do evento crítico. Conclua o procedimento Recovery Guru para corrigir o evento crítico. Para corrigir certos eventos críticos, talvez seja necessário entrar em Contato com o suporte técnico.

### Exibir eventos usando o log de eventos

Você pode exibir o log de eventos, que fornece um Registro histórico de eventos que ocorreram no storage array.

#### Passos

1. Selecione **suporte › Registo de eventos**.

   É apresentada a página Registo de eventos.

**Detalhes da página**

| Item | Descrição |
| --- | --- |
| Exibir todos campo | Alterna entre todos os eventos e apenas os eventos críticos e de aviso. |
| Campo de filtro | Filtra os eventos. Útil para exibir apenas eventos relacionados a um componente específico, um evento específico, etc. |
| Selecione o ícone colunas. | Permite selecionar outras colunas para visualizar. Outras colunas fornecem informações adicionais sobre o evento. |
| Caixas de verificação | Permite-lhe selecionar os eventos a guardar. A caixa de seleção no cabeçalho da tabela seleciona todos os eventos. |
| Coluna Data/hora | O carimbo de data e hora do evento, de acordo com o relógio do controlador.<br><br>O log de eventos inicialmente classifica os eventos com base no número de sequência. Normalmente, esta sequência corresponde à data e hora. No entanto, os dois relógios do controlador no storage de armazenamento podem ser dessincronizados. Nesse caso, algumas inconsistências percebidas podem aparecer no log de eventos em relação aos eventos e à data e hora mostradas. |
| Coluna de prioridade | Estes valores de prioridade existem:<br><br>• **Critical** — existe um problema com a matriz de armazenamento. No entanto, se você tomar medidas imediatas, pode impedir a perda de acesso aos dados. Eventos críticos são usados para notificações de alerta. Todos os eventos críticos são enviados para qualquer cliente de gerenciamento de rede (por meio de traps SNMP) ou para o destinatário de e-mail que você configurou.<br>• **Aviso** — ocorreu um erro que degradou o desempenho e a capacidade do storage de recuperar de outro erro.<br>• **Informational** — informações não críticas relacionadas ao storage array. |
| Coluna tipo componente | O componente que é afetado pelo evento. O componente pode ser hardware, como uma unidade ou um controlador, ou pode ser software, como firmware do controlador. |
| Coluna localização dos componentes | A localização física do componente no storage array. |

| Item | Descrição |
| --- | --- |
| Coluna de descrição | Uma descrição do evento.<br><br>**Exemplo** — `Drive write failure - retries exhausted` |
| Coluna de número de sequência | Um número de 64 bits que identifica exclusivamente uma entrada de log específica para uma matriz de armazenamento. Esse número aumenta em um com cada nova entrada de log de eventos. Para exibir essas informações, clique no ícone **Selecionar colunas**. |
| Coluna tipo evento | Um número de 4 dígitos que identifica cada tipo de evento registrado. Para exibir essas informações, clique no ícone **Selecionar colunas**. |
| Coluna códigos específicos do evento | Esta informação é usada pelo suporte técnico. Para exibir essas informações, clique no ícone **Selecionar colunas**. |
| Coluna Categoria evento | • **Falha** – Um componente no storage de armazenamento falhou; por exemplo, falha na unidade ou falha da bateria.<br>• **Mudança de estado** – um elemento da matriz de armazenamento que mudou de estado; por exemplo, um volume fez a transição para o status ideal ou um controlador fez a transição para o status Offline.<br>• **Interno** – operações internas do controlador que não exigem ação do usuário; por exemplo, o controlador concluiu o início do dia.<br>• **Comando** – Um comando que foi emitido para o storage array; por exemplo, um hot spare foi atribuído.<br>• **Erro** – uma condição de erro foi detetada no storage de armazenamento; por exemplo, um controlador não consegue sincronizar e purgar o cache, ou um erro de redundância é detetado no storage de armazenamento.<br>• **Geral** – qualquer evento que não se encaixe bem em qualquer outra categoria. Para exibir essas informações, clique no ícone **Selecionar colunas**. |
| Registrado por coluna | O nome do controlador que registrou o evento. Para exibir essas informações, clique no ícone **Selecionar colunas**. |

2. Para recuperar novos eventos da matriz de armazenamento, clique em **Atualizar**.

   Pode demorar vários minutos para que um evento seja registrado e fique visível na página Registro de eventos.

3. Para salvar o log de eventos em um arquivo:
   a. Marque a caixa de seleção ao lado de cada evento que você deseja salvar.
   b. Clique em **Salvar**.

      O arquivo é salvo na pasta Downloads do navegador com o nome `major-event-log-`

`timestamp.log`.

4. Para limpar eventos do log de eventos:

   O log de eventos armazena aproximadamente 8.000 eventos antes de substituir um evento por um novo evento. Se você quiser manter os eventos, você pode salvá-los e limpá-los do log de eventos.

   a. Primeiro, salve o log de eventos.
   b. Clique em **Clear All** (Limpar tudo) e confirme que pretende executar a operação.

## Gerenciar atualizações

### Visão geral do Centro de atualizações

Use o Centro de Atualização para baixar o software e o firmware mais recentes e atualizar seus controladores e unidades.

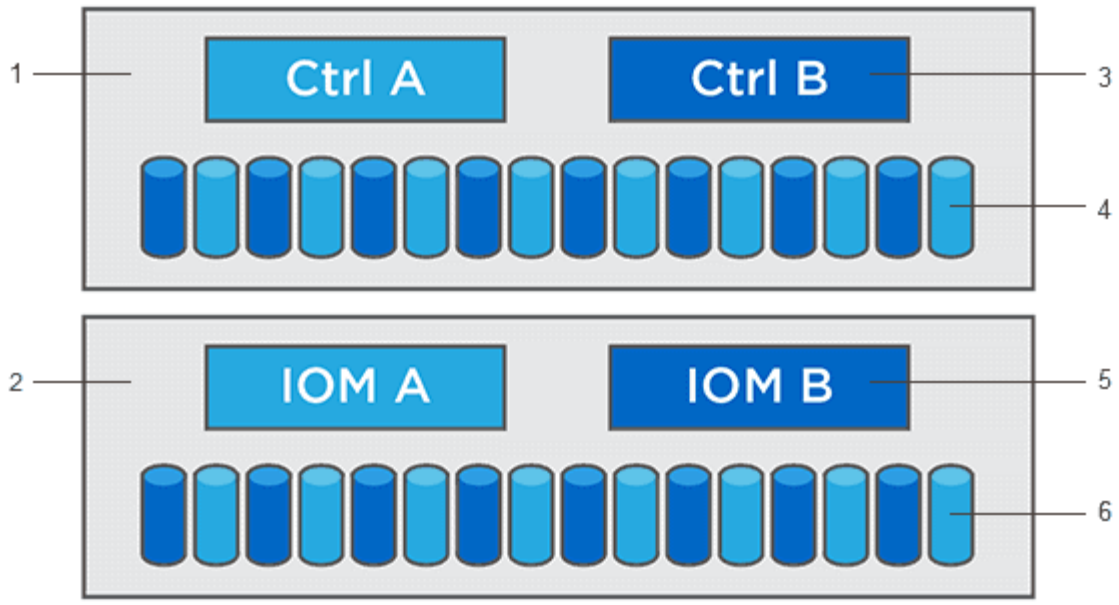
#### Visão geral da atualização do controlador

Você pode atualizar o software e firmware da sua matriz de armazenamento para todos os recursos mais recentes e correções de bugs.

### Componentes incluídos na atualização da controladora do sistema operacional

Vários componentes de storage array contêm software ou hardware que você pode querer atualizar ocasionalmente.

- **Software de gerenciamento** — System Manager é o software que gerencia o storage array.
- **Firmware do controlador** — o firmware do controlador gerencia a e/S entre hosts e volumes.
- **Controller NVSRAM** — Controller NVSRAM é um arquivo de controlador que especifica as configurações padrão para os controladores.
- **Firmware IOM** — o firmware do módulo de e/S (IOM) gerencia a conexão entre uma controladora e um compartimento de unidades. Também monitoriza o estado dos componentes.
- **Software Supervisor** — o software Supervisor é a máquina virtual em um controlador no qual o software é executado.




1 GB, 2 GB, firmware da controladora, software supervisor; 3 GB, firmware da unidade; 4 GB, firmware da unidade; 5 GB, firmware da unidade; 6 GB, firmware da unidade

Você pode exibir as versões atuais de software e firmware na caixa de diálogo Inventário de Software e firmware. Aceda ao **suporte › Centro de Atualização** e, em seguida, clique no link **Inventário de Software e firmware**.

Como parte do processo de atualização, o driver multipath/failover e/ou o driver HBA do host também podem precisar ser atualizados para que o host possa interagir com os controladores corretamente. Para determinar se esse é o caso, consulte "Ferramenta de Matriz de interoperabilidade do NetApp" .

### Quando parar e/S

Se o storage array contiver duas controladoras e você tiver um driver multipath instalado, o storage array poderá continuar processando e/S durante a atualização. Durante a atualização, a controladora A falha em todos os volumes para a controladora B, atualiza, recupera os volumes e todos os volumes da controladora B e, em seguida, atualiza a controladora B.

### Verificação de integridade pré-atualização

Uma verificação de integridade de pré-atualização é executada como parte do processo de atualização. A verificação de integridade da pré-atualização avalia todos os componentes do storage array para garantir que a atualização possa prosseguir. As seguintes condições podem impedir a atualização:

- Unidades atribuídas com falha
- Peças sobressalentes quentes em uso
- Grupos de volumes incompletos
- Operações exclusivas em execução
- Volumes em falta
- Controlador em estado não ótimo
- Número excessivo de eventos de log
- Falha na validação da base de dados de configuração

- Unidades com versões antigas do DACstore

Você também pode executar a verificação de integridade de pré-atualização separadamente sem fazer uma atualização.

#### Visão geral da atualização da unidade

O firmware da unidade controla as caraterísticas operacionais de baixo nível de uma unidade. Periodicamente, os fabricantes de unidades lançam atualizações para o firmware da unidade para adicionar novos recursos, melhorar o desempenho e corrigir defeitos.

### Atualizações de firmware de unidade on-line e off-line

Existem dois tipos de métodos de atualização de firmware de unidade: On-line e off-line.

### Online

Durante uma atualização online, as unidades são atualizadas sequencialmente, uma de cada vez. O storage array continua processando e/S durante a atualização. Você não tem que parar I/O.. Se uma unidade puder fazer uma atualização on-line, o método on-line será usado automaticamente.

As unidades que podem fazer uma atualização online incluem o seguinte:

- Conduz em um pool ideal
- Unidades em um grupo de volume redundante ideal (RAID 1, RAID 5 e RAID 6)
- Unidades não atribuídas
- Unidades de reserva hot spare em espera

Fazer uma atualização de firmware de unidade on-line pode levar várias horas, expondo o storage array a possíveis falhas de volume. A falha de volume pode ocorrer nestes casos:

- Em um grupo de volumes RAID 1 ou RAID 5, uma unidade falha enquanto uma unidade diferente no grupo de volumes está sendo atualizada.
- Em um pool RAID 6 ou grupo de volumes, duas unidades falham enquanto uma unidade diferente no pool ou grupo de volumes está sendo atualizada.

### Offline (paralelo)

Durante uma atualização off-line, todas as unidades do mesmo tipo de unidade são atualizadas ao mesmo tempo. Este método requer a interrupção da atividade de e/S para os volumes associados às unidades selecionadas. Como várias unidades podem ser atualizadas simultaneamente (em paralelo), o tempo de inatividade geral é significativamente reduzido. Se uma unidade puder fazer apenas uma atualização off-line, o método off-line será usado automaticamente.

As seguintes unidades DEVEM usar o método offline:

- Unidades em um grupo de volume não redundante (RAID 0)
- Unidades em um pool ou grupo de volumes não ideais
- Unidades em cache SSD

### Compatibilidade

Cada arquivo de firmware da unidade contém informações sobre o tipo de unidade em que o firmware é executado. Pode transferir o ficheiro de firmware especificado apenas para uma unidade compatível. O System Manager verifica automaticamente a compatibilidade durante o processo de atualização.

### Atualize o software e o firmware do controlador

Você pode atualizar o software do seu storage array e, opcionalmente, o firmware IOM e a memória de acesso aleatório estática não volátil (NVSRAM) para garantir que você tenha todos os recursos e correções de bugs mais recentes.

#### Antes de começar

- Você sabe se deseja atualizar seu firmware IOM.

  Normalmente, você deve atualizar todos os componentes ao mesmo tempo. No entanto, você pode decidir não atualizar o firmware IOM se não quiser atualizá-lo como parte da atualização do software SANtricity os ou se o suporte técnico tiver instruído a fazer o downgrade do firmware IOM (você só pode fazer o downgrade do firmware usando a interface de linha de comando).

- Você sabe se deseja atualizar o arquivo NVSRAM da controladora.

  Normalmente, você deve atualizar todos os componentes ao mesmo tempo. No entanto, você pode decidir não atualizar o arquivo NVSRAM do controlador se o arquivo tiver sido corrigido ou for uma versão personalizada e você não quiser sobrescrevê-lo.

- Você sabe se deseja ativar a atualização do sistema operacional agora ou mais tarde.

  As razões para ativar mais tarde podem incluir:

  - **Hora do dia** — a ativação do software e do firmware pode demorar muito tempo, então você pode querer esperar até que as cargas de e/S sejam mais leves. Os controladores fazem failover durante a ativação, portanto, o desempenho pode ser menor do que o normal até a atualização ser concluída.
  - * Tipo de pacote* — você pode querer testar o novo software e firmware em uma matriz de armazenamento antes de atualizar os arquivos em outras matrizes de armazenamento.

- Você sabe se deseja mudar de unidades não protegidas ou unidades protegidas internamente para usar um servidor de gerenciamento de chaves externo (KMS) para segurança da unidade.
- Você sabe se deseja usar o controle de acesso baseado em funções em seu storage array.

#### Sobre esta tarefa

Você pode optar por atualizar apenas o arquivo de software do sistema operacional ou apenas o arquivo NVSRAM do controlador ou pode optar por atualizar ambos os arquivos.

Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

**Risco de perda de dados ou risco de danos à matriz de armazenamento** — não faça alterações na matriz de armazenamento enquanto a atualização estiver ocorrendo. Mantenha o poder do storage array.

#### Passos

1. Se o storage array contiver apenas uma controladora ou você não tiver um driver multipath instalado, interrompa a atividade de e/S para o storage array para evitar erros de aplicativos. Se o seu storage array

tiver duas controladoras e você tiver um driver multipath instalado, não será necessário interromper a atividade de e/S.

2. Selecione **suporte › Centro de atualizações**.
3. Transfira o novo ficheiro do site de suporte para o seu cliente de gestão.

   a. Clique em **suporte NetApp** para iniciar o site de suporte.

   b. No site de suporte, clique na guia **Downloads** e selecione **Downloads**.

   c. Selecione **Software do controlador SANtricity os da série e**.

   d. Siga as instruções restantes.

   > O firmware assinado digitalmente é necessário na versão 8,42 e superior. Se tentar transferir firmware não assinado, é apresentado um erro e a transferência é cancelada.

4. Se NÃO pretender atualizar o firmware IOM neste momento, clique em **suspender a sincronização automática IOM**.

   Se você tiver um storage array com uma única controladora, o firmware IOM não será atualizado.

5. Em Atualização de software do SANtricity os, clique em **Begin Upgrade**.

   A caixa de diálogo Atualizar software SANtricity os é exibida.

6. Selecione um ou mais arquivos para iniciar o processo de atualização:

   a. Selecione o arquivo de software do sistema operacional SANtricity clicando em **Procurar** e navegando até o arquivo de software do sistema operacional baixado do site de suporte.

   b. Selecione o arquivo NVSRAM da controladora clicando em **Procurar** e navegando até o arquivo NVSRAM baixado do site de suporte. Os arquivos NVSRAM do controlador têm um nome de arquivo semelhante `N2800-830000-000.dlp` ao .

      Estas ações ocorrem:

      - Por padrão, apenas os arquivos compatíveis com a configuração atual da matriz de armazenamento aparecem.
      - Quando você seleciona um arquivo para atualização, o nome e o tamanho do arquivo são exibidos.

7. **Opcional:** se você selecionou um arquivo de software do SANtricity os para atualizar, você pode transferir os arquivos para o controlador sem ativá-los selecionando a caixa de seleção **Transferir arquivos agora, mas não atualizar (ativar atualização mais tarde)**.
8. Clique em **Start** (Iniciar) e confirme que deseja executar a operação.

   Pode cancelar a operação durante a verificação de estado de pré-atualização, mas não durante a transferência ou ativação.

9. **Opcional:** para ver uma lista do que foi atualizado, clique em **Salvar Registro**.

   O arquivo é salvo na pasta Downloads do navegador com o nome `drive_upgrade_log-timestamp.txt`.

**Depois de terminar**

- Verifique se todos os componentes aparecem na página hardware.
- Verifique as novas versões de software e firmware marcando a caixa de diálogo Inventário de Software e firmware (vá para o **suporte › Centro de Atualização** e clique no link **Inventário de Software e firmware**).
- Se você atualizou a NVSRAM da controladora, quaisquer configurações personalizadas aplicadas à NVSRAM existente serão perdidas durante o processo de ativação. Você precisa aplicar as configurações personalizadas à NVSRAM novamente depois que o processo de ativação for concluído.

### Ative o software e o firmware do controlador

Você pode optar por ativar os arquivos de atualização imediatamente ou esperar até um momento mais conveniente.

#### Sobre esta tarefa

Você pode baixar e transferir os arquivos sem ativá-los. Você pode optar por ativar mais tarde por estes motivos:

- **Hora do dia** — a ativação do software e do firmware pode demorar muito tempo, então você pode querer esperar até que as cargas de e/S sejam mais leves. Os controladores fazem failover durante a ativação, portanto, o desempenho pode ser menor do que o normal até a atualização ser concluída.
- * Tipo de pacote* — você pode querer testar o novo software e firmware em uma matriz de armazenamento antes de atualizar os arquivos em outras matrizes de armazenamento.

Quando tiver software ou firmware transferido, mas não ativado, verá uma notificação na área notificações da página inicial do System Manager e também na página Centro de Atualização.

Não é possível parar o processo de ativação depois de iniciado.

#### Passos

1. Selecione **suporte › Centro de atualizações**.
2. Na área rotulada SANtricity os Controller Software upgrade, clique em **Activate** e confirme se deseja executar a operação.

   Pode cancelar a operação durante a verificação de estado de pré-atualização, mas não durante a ativação.

   A verificação de integridade da pré-atualização começa. Se a verificação de integridade da pré-atualização for aprovada, o processo de atualização continuará a ativar os arquivos. Se a verificação de integridade da pré-atualização falhar, use o Recovery Guru ou entre em Contato com o suporte técnico para resolver o problema. Para alguns tipos de condições, o suporte técnico pode aconselhá-lo a continuar com a atualização, apesar dos erros, selecionando uma caixa de verificação **permitir atualização**.

   Após a conclusão bem-sucedida da verificação de integridade da pré-atualização, ocorre a ativação. O tempo de ativação depende da configuração do storage array e dos componentes que você está ativando.

3. **Opcional:** para ver uma lista do que foi atualizado, clique em **Salvar Registro**.

   O arquivo é salvo na pasta Downloads do navegador com o nome `drive_upgrade_log-timestamp.txt`.

**Depois de terminar**

- Verifique se todos os componentes aparecem na página hardware.
- Verifique as novas versões de software e firmware marcando a caixa de diálogo Inventário de Software e firmware (vá para o **suporte › Centro de Atualização** e clique no link **Inventário de Software e firmware**).
- Se você atualizou a NVSRAM da controladora, quaisquer configurações personalizadas aplicadas à NVSRAM existente serão perdidas durante o processo de ativação. Você precisa aplicar as configurações personalizadas à NVSRAM novamente depois que o processo de ativação for concluído.

### Atualize o firmware da unidade

Você pode atualizar o firmware das suas unidades para se certificar de que você tem todos os recursos mais recentes e correções de bugs.

**Antes de começar**

- Você fez backup de seus dados usando backup de disco para disco, cópia de volume (para um grupo de volumes não afetado pela atualização de firmware planejada) ou um espelhamento remoto.
- O storage array tem um status ideal.
- Todas as unidades têm um status ideal.
- Nenhuma alteração de configuração está sendo executada no storage array.
- Se as unidades forem capazes de apenas uma atualização off-line, a atividade de e/S para todos os volumes associados às unidades será interrompida.

**Passos**

1. Selecione **suporte › Centro de atualizações**.
2. Transfira os novos ficheiros do site de suporte para o seu cliente de gestão.
   a. Em Atualização do firmware da unidade, clique em **suporte NetApp**.
   b. No site de suporte da NetApp, clique na guia **Downloads**.
   c. Selecione **Unidade de disco e Matriz de firmware**.
   d. Siga as instruções restantes.
3. Em Drive firmware upgrade, clique em **Begin Upgrade** (Iniciar atualização).

   É apresentada uma caixa de diálogo que lista os ficheiros de firmware da unidade atualmente em utilização.
4. Extraia (descompacte) os arquivos que você baixou do site de suporte.
5. Clique em **Procurar** e selecione os novos arquivos de firmware da unidade que você baixou no site de suporte.

   Os arquivos de firmware da unidade têm um nome de arquivo semelhante ao `D_HUC101212CSS600_30602291_MS01_2800_0002` com a extensão `.dlp` do .

   Você pode selecionar até quatro arquivos de firmware da unidade, um de cada vez. Se mais de um arquivo de firmware de unidade for compatível com a mesma unidade, você receberá um erro de conflito de arquivo. Decida qual arquivo de firmware da unidade você deseja usar para a atualização e remova o outro.

6. Clique em **seguinte**.

   A caixa de diálogo **Selecionar unidades** é exibida, que lista as unidades que você pode atualizar com os arquivos selecionados.

   Apenas as unidades compatíveis aparecem.

   O firmware selecionado para a unidade aparece na área de informações de firmware proposto. Se tiver de alterar o firmware, clique em **Back** (anterior) para regressar à caixa de diálogo anterior.

7. Selecione o tipo de atualização que deseja executar:
   - **Online (padrão)** — mostra as unidades que podem suportar um download de firmware *enquanto o storage array está processando I/o*. Não é necessário interromper a e/S para os volumes associados usando essas unidades quando você selecionar esse método de atualização. Essas unidades são atualizadas uma de cada vez, enquanto o storage array está processando e/S para essas unidades.
   - **Offline (paralelo)** — mostra as unidades que podem suportar um download de firmware *somente enquanto toda a atividade de e/S está parada* em qualquer volume que use as unidades. Você deve parar toda a atividade de e/S em todos os volumes que usam as unidades que você está atualizando ao selecionar esse método de atualização. As unidades que não têm redundância devem ser processadas como uma operação off-line. Esse requisito inclui qualquer unidade associada ao cache SSD, um grupo de volumes RAID 0 ou qualquer pool ou grupo de volumes degradado. A atualização off-line (paralela) é normalmente mais rápida do que o método on-line (padrão).
8. Na primeira coluna da tabela, selecione a unidade ou unidades que deseja atualizar.
9. Clique em **Start** (Iniciar) e confirme que deseja executar a operação.

   Se você precisar parar a atualização, clique em **Parar**. Todas as transferências de firmware atualmente em curso são concluídas. Quaisquer downloads de firmware que não tenham sido iniciados são cancelados.

   > Parar a atualização do firmware da unidade pode resultar em perda de dados ou unidades indisponíveis.

10. **Opcional:** para ver uma lista do que foi atualizado, clique em **Salvar Registro**.

    O arquivo é salvo na pasta Downloads do navegador com o nome `drive_upgrade_log-timestamp.txt`.

11. Se ocorrer algum dos seguintes erros durante o procedimento de atualização, tome a ação recomendada apropriada.

**Erros e ações recomendadas**

| Se encontrar este erro de transferência de firmware… | Em seguida, faça o seguinte… |
|---|---|
| Unidades atribuídas com falha | Um motivo para a falha pode ser que a unidade não tenha a assinatura apropriada. Certifique-se de que a unidade afetada é uma unidade autorizada. Entre em Contato com o suporte técnico para obter mais informações.<br><br>Ao substituir uma unidade, certifique-se de que a unidade de substituição tem uma capacidade igual ou superior à unidade com falha que está a substituir.<br><br>Você pode substituir a unidade com falha enquanto a matriz de armazenamento está recebendo e/S |
| Verifique a matriz de armazenamento | • Certifique-se de que foi atribuído um endereço IP a cada controlador.<br>• Certifique-se de que todos os cabos ligados ao controlador não estão danificados.<br>• Certifique-se de que todos os cabos estão bem ligados. |
| Unidades hot spare integradas | Esta condição de erro tem de ser corrigida antes de poder atualizar o firmware. Inicie o System Manager e use o Recovery Guru para resolver o problema. |
| Grupos de volumes incompletos | Se um ou mais grupos de volumes ou pools de discos estiverem incompletos, você deverá corrigir essa condição de erro antes de atualizar o firmware. Inicie o System Manager e use o Recovery Guru para resolver o problema. |
| Operações exclusivas (exceto Mídia em segundo plano/varredura de paridade) atualmente em execução em qualquer grupo de volume | Se uma ou mais operações exclusivas estiverem em andamento, as operações devem ser concluídas antes que o firmware possa ser atualizado. Use o System Manager para monitorar o andamento das operações. |
| Volumes em falta | Você deve corrigir a condição de volume ausente antes que o firmware possa ser atualizado. Inicie o System Manager e use o Recovery Guru para resolver o problema. |
| Qualquer controlador em um estado diferente do ideal | Um dos controladores de storage array precisa de atenção. Esta condição deve ser corrigida antes que o firmware possa ser atualizado. Inicie o System Manager e use o Recovery Guru para resolver o problema. |
| Informações de partição de armazenamento incompatíveis entre gráficos de objetos do controlador | Ocorreu um erro ao validar os dados nos controladores. Contacte o suporte técnico para resolver este problema. |

| Se encontrar este erro de transferência de firmware… | Em seguida, faça o seguinte… |
| --- | --- |
| Verificação SPM verificar falha na verificação do controlador do banco de dados | Ocorreu um erro de banco de dados de mapeamento de partições de armazenamento em um controlador. Contacte o suporte técnico para resolver este problema. |
| Validação da base de dados de configuração (se suportada pela versão do controlador da matriz de armazenamento) | Ocorreu um erro de banco de dados de configuração em um controlador. Contacte o suporte técnico para resolver este problema. |
| Verificações relacionadas com MEL | Contacte o suporte técnico para resolver este problema. |
| Mais de 10 eventos informativos ou críticos de mel foram relatados nos últimos 7 dias | Contacte o suporte técnico para resolver este problema. |
| Mais de 2 Página 2C Eventos críticos de mel foram relatados nos últimos 7 dias | Contacte o suporte técnico para resolver este problema. |
| Mais de 2 eventos de mel críticos de canal de unidade degradada foram relatados nos últimos 7 dias | Contacte o suporte técnico para resolver este problema. |
| Mais de 4 entradas críticas de mel nos últimos 7 dias | Contacte o suporte técnico para resolver este problema. |

**Depois de terminar**

A atualização do firmware da unidade está concluída. Pode retomar as operações normais.

### Reveja os possíveis erros de atualização de software e firmware

Podem ocorrer erros durante a atualização do software da controladora ou a atualização do firmware da unidade.

| Erro de transferência do firmware | Descrição | Ação recomendada |
| --- | --- | --- |
| Unidades atribuídas com falha | Falha ao atualizar uma unidade atribuída na matriz de armazenamento. | Um motivo para a falha pode ser que a unidade não tenha a assinatura apropriada. Certifique-se de que a unidade afetada é uma unidade autorizada. Entre em Contato com o suporte técnico para obter mais informações.<br><br>Ao substituir uma unidade, certifique-se de que a unidade de substituição tem uma capacidade igual ou superior à unidade com falha que está a substituir.<br><br>Você pode substituir a unidade com falha enquanto a matriz de armazenamento está recebendo e/S |
| Unidades hot spare integradas | Se a unidade estiver marcada como hot spare e estiver em uso para um grupo de volumes, o processo de atualização do firmware falhará. | Esta condição de erro tem de ser corrigida antes de poder atualizar o firmware. Inicie o System Manager e use o Recovery Guru para resolver o problema. |
| Grupos de volumes incompletos | Se qualquer unidade que faça parte de um grupo de volume for ignorada, removida ou não responsiva, será considerada um grupo de volumes incompleto. Um grupo de volumes incompleto impede atualizações de firmware. | Se um ou mais grupos de volumes ou pools de discos estiverem incompletos, você deverá corrigir essa condição de erro antes de atualizar o firmware. Inicie o System Manager e use o Recovery Guru para resolver o problema. |
| Operações exclusivas (exceto Mídia em segundo plano/varredura de paridade) atualmente em execução em qualquer grupo de volume | Não é possível atualizar o firmware se houver operações exclusivas em andamento em um volume. | Se uma ou mais operações exclusivas estiverem em andamento, as operações devem ser concluídas antes que o firmware possa ser atualizado. Use o System Manager para monitorar o andamento das operações. |
| Volumes em falta | Não é possível atualizar o firmware se houver algum volume em falta. | Você deve corrigir a condição de volume ausente antes que o firmware possa ser atualizado. Inicie o System Manager e use o Recovery Guru para resolver o problema. |

| Erro de transferência do firmware | Descrição | Ação recomendada |
| --- | --- | --- |
| Qualquer controlador em um estado diferente do ideal | Não é possível atualizar o firmware se uma das controladoras estiver em um estado diferente do ideal. | Um dos controladores de storage array precisa de atenção. Esta condição deve ser corrigida antes que o firmware possa ser atualizado. Inicie o System Manager e use o Recovery Guru para resolver o problema. |
| Verificação SPM verificar falha na verificação do controlador do banco de dados | Não é possível atualizar o firmware porque o banco de dados de mapeamentos de partições de armazenamento está corrompido. | Ocorreu um erro de banco de dados de mapeamento de partições de armazenamento em um controlador. Contacte o suporte técnico para resolver este problema. |
| Validação da base de dados de configuração (se suportada pela versão do controlador da matriz de armazenamento) | Não é possível atualizar o firmware porque a base de dados de configuração está corrompida. | Ocorreu um erro de banco de dados de configuração em um controlador. Contacte o suporte técnico para resolver este problema. |
| Verificações relacionadas com MEL | Não é possível atualizar o firmware porque o log de eventos contém erros. | Contacte o suporte técnico para resolver este problema. |
| Mais de 10 eventos informativos ou críticos de mel foram relatados nos últimos 7 dias | Não é possível atualizar o firmware porque existem mais de 10 eventos de mel informativos ou críticos DDE comunicados nos últimos sete dias. | Contacte o suporte técnico para resolver este problema. |
| Mais de 2 Página 2C Eventos críticos de mel foram relatados nos últimos 7 dias | Não é possível atualizar o firmware porque há mais de duas páginas 2C Eventos críticos de mel relatados nos últimos sete dias. | Contacte o suporte técnico para resolver este problema. |
| Mais de 2 eventos de mel críticos de canal de unidade degradada foram relatados nos últimos 7 dias | Não é possível atualizar o firmware porque há mais de dois eventos de mel críticos de canal de unidade degradados relatados nos últimos sete dias. | Contacte o suporte técnico para resolver este problema. |
| Mais de 4 entradas críticas de mel nos últimos 7 dias | Não é possível atualizar o firmware porque há mais de quatro entradas de log de eventos críticos relatadas nos últimos sete dias. | Contacte o suporte técnico para resolver este problema. |
| É necessário um endereço IP de gerenciamento válido. | É necessário um endereço IP válido do controlador para executar esta operação. | Contacte o suporte técnico para resolver este problema. |

| Erro de transferência do firmware | Descrição | Ação recomendada |
| --- | --- | --- |
| O comando requer um endereço IP de gerenciamento ativo para cada controlador a ser fornecido. | Um endereço IP do controlador para cada controlador associado à matriz de armazenamento é necessário para esta operação. | Contacte o suporte técnico para resolver este problema. |
| Tipo de ficheiro de transferência não manipulado devolvido. | O ficheiro de transferência especificado não é suportado. | Contacte o suporte técnico para resolver este problema. |
| Ocorreu um erro durante o procedimento de carregamento da transferência do firmware. | A transferência do firmware falhou porque o controlador não consegue processar a solicitação. Verifique se a matriz de armazenamento está ótima e tente novamente a operação. | Se esse erro ocorrer novamente após verificar se a matriz de armazenamento está ótima, entre em Contato com o suporte técnico para resolver esse problema. |
| Ocorreu um erro durante o procedimento de ativação do firmware. | A ativação do firmware falhou porque o controlador não consegue processar a solicitação. Verifique se a matriz de armazenamento está ótima e tente novamente a operação. | Se esse erro ocorrer novamente após verificar se a matriz de armazenamento está ótima, entre em Contato com o suporte técnico para resolver esse problema. |
| O tempo limite foi atingido enquanto aguarda a reinicialização do controlador (0). | O software de gerenciamento não consegue se reconetar ao controlador 0 após uma reinicialização. Validar há um caminho de conexão operacional para o storage array e tentar novamente a operação se ele não foi concluído com êxito. | Se esse erro ocorrer novamente após verificar se a matriz de armazenamento está ótima, entre em Contato com o suporte técnico para resolver esse problema. |

Você pode corrigir algumas dessas condições usando o Recovery Guru no System Manager. No entanto, para algumas das condições, você pode precisar entrar em Contato com o suporte técnico. As informações sobre o download mais recente do firmware do controlador estão disponíveis na matriz de armazenamento. Estas informações ajudam o suporte técnico a compreender as condições de erro que impediram a atualização e o download do firmware.

## FAQs

**Que dados estou coletando?**

O recurso AutoSupport e o recurso manual de coleta de dados de suporte fornecem maneiras de coletar dados em um pacote de suporte ao cliente para solução remota de problemas e análise de problemas por suporte técnico.

O pacote de suporte ao cliente reúne todos os tipos de informações sobre a matriz de armazenamento em um único arquivo compactado. As informações coletadas incluem a configuração física, configuração lógica, informações de versão, eventos, arquivos de log e dados de desempenho. As informações são usadas apenas pelo suporte técnico para resolver problemas com o storage array.

**O que os dados de setores ilegíveis me mostram?**

Você pode exibir dados detalhados sobre setores ilegíveis detetados nas unidades em seu storage array.

O log de setores ilegíveis mostra primeiro o setor ilegível mais recente. O log contém as seguintes informações sobre os volumes que contêm os setores ilegíveis. Os campos são selecionáveis.

| Campo | Descrição |
| --- | --- |
| Volume afetado | Mostra a etiqueta do volume. Se um volume em falta contiver setores ilegíveis, o Identificador mundial será exibido para o volume em falta. |
| Número de unidade lógica (LUN) | Mostra o LUN para o volume. Se o volume não tiver um LUN, a caixa de diálogo mostra na. |
| Atribuído a | Mostra os hosts ou clusters de host que têm acesso ao volume. Se o volume não estiver acessível por um host, cluster de host ou mesmo um cluster padrão, a caixa de diálogo mostrará na. |

Para ver informações adicionais sobre os setores ilegíveis, clique no sinal de mais ao lado de um volume.

| Campo | Descrição |
| --- | --- |
| Data/hora | Mostra a data e a hora em que o setor ilegível foi detetado. |
| Endereço de bloco lógico de volume | Mostra o endereço de bloco lógico (LBA) do volume. |
| Localização da unidade | Mostra o compartimento da unidade, a gaveta (se a prateleira da unidade tiver gavetas) e a localização do compartimento. |
| Endereço do bloco lógico da unidade | Mostra o LBA da unidade. |
| Tipo de avaria | Mostra um dos seguintes tipos de falha:<br>• **Physical** — Um erro de Mídia física.<br>• **Logical** — Um erro de leitura em outro lugar na faixa causando dados ilegíveis. Por exemplo, um setor ilegível devido a erros de Mídia em outro lugar do volume.<br>• **Inconsistente** — dados de redundância inconsistentes.<br>• **Data Assurance** — Um erro de garantia de dados. |

**O que é uma imagem de saúde?**

Uma imagem de integridade é um despejo de dados brutos da memória do processador do controlador que o suporte técnico pode usar para diagnosticar um problema com um

controlador.

O firmware gera automaticamente uma imagem de integridade quando deteta determinados erros. Em certos cenários de solução de problemas, o suporte técnico pode solicitar que você recupere o arquivo de imagem de integridade e envie-o para eles.

#### O que fazem os recursos do AutoSupport?

O recurso AutoSupport é composto por três recursos individuais que você ativa separadamente.

- **Basic AutoSupport** — permite que sua matriz de armazenamento colete e envie dados automaticamente para o suporte técnico.
- **AutoSupport OnDemand** — permite que o suporte técnico solicite a retransmissão de um despacho AutoSupport anterior quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir da matriz de armazenamento, não do servidor AutoSupport. A matriz de armazenamento verifica periodicamente com o servidor AutoSupport para determinar se existem solicitações de retransmissão pendentes e responde de acordo.
- **Diagnóstico remoto** — permite que o suporte técnico solicite um novo e atualizado despacho do AutoSupport quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir da matriz de armazenamento, não do servidor AutoSupport. O storage array verifica periodicamente com o servidor AutoSupport para determinar se há novas solicitações pendentes e responde de acordo.

#### Que tipo de dados são recolhidos através da funcionalidade AutoSupport?

O recurso AutoSupport contém três tipos de despacho padrão: Despachos de eventos, despachos programados e despachos de diagnóstico remoto e sob demanda.

Os dados do AutoSupport não contêm nenhum dado de usuário.

- **Envios de eventos**

  Quando ocorrem eventos no sistema que garantem uma notificação proativa ao suporte técnico, o recurso AutoSupport envia automaticamente um despacho acionado por evento.

  - Enviado quando ocorre um evento de suporte no storage array gerenciado.
  - Inclui um snapshot abrangente do que estava acontecendo com o storage array no momento em que o evento ocorreu.

- **Despachos programados**

  O recurso AutoSupport envia automaticamente vários despachos em um horário regular.

  - **Despachos diários** — enviados uma vez por dia durante um intervalo de tempo configurável pelo usuário. Inclui os registos de eventos e dados de desempenho do sistema atuais.
  - **Expedições semanais** — enviadas uma vez por semana durante um intervalo de tempo e dia configuráveis pelo usuário. Inclui informações de configuração e estado do sistema.

- **AutoSupport OnDemand e despachos de Diagnóstico remoto**
  - **AutoSupport OnDemand** — permite que o suporte técnico solicite a retransmissão de um despacho AutoSupport anterior quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir da matriz de armazenamento, não do servidor AutoSupport. A matriz de armazenamento verifica periodicamente com o servidor AutoSupport para determinar se existem

solicitações de retransmissão pendentes e responde de acordo.

- **Diagnóstico remoto** — permite que o suporte técnico solicite um novo e atualizado despacho do AutoSupport quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir da matriz de armazenamento, não do servidor AutoSupport. O storage array verifica periodicamente com o servidor AutoSupport para determinar se há novas solicitações pendentes e responde de acordo.

### Como configuro o método de entrega para o recurso AutoSupport?

## O recurso AutoSupport oferece suporte aos protocolos HTTPS, HTTP e SMTP para entrega de despachos AutoSupport para suporte técnico.

**Antes de começar**

- O recurso AutoSupport deve estar ativado. Você pode ver se ele está habilitado na página AutoSupport.
- Um servidor DNS deve ser instalado e configurado na rede. O endereço do servidor DNS deve ser configurado no System Manager (esta tarefa está disponível na página hardware).

**Sobre esta tarefa**

Reveja os diferentes protocolos:

- **HTTPS** — permite que você se conete diretamente ao servidor de suporte técnico de destino usando HTTPS. Se você quiser ativar o AutoSupport OnDemand ou o Diagnóstico remoto, o método de entrega do AutoSupport deve ser definido como HTTPS.
- **HTTP** — permite que você se conete diretamente ao servidor de suporte técnico de destino usando HTTP.
- **Email** — permite que você use um servidor de e-mail como o método de entrega para enviar despachos AutoSupport.

> **Diferenças entre os métodos HTTPS/HTTP e Email**. O método de entrega de e-mail, que usa SMTP, tem algumas diferenças importantes em relação aos métodos de entrega HTTPS e HTTP. Primeiro, o tamanho dos envios para o método Email está limitado a 5MB, o que significa que algumas coleções de dados ASUP não serão enviadas. Em segundo lugar, o recurso AutoSupport OnDemand está disponível somente nos métodos HTPP e HTTPS.

**Passos**

1. Selecione **suporte › Centro de suporte › AutoSupport**.
2. Selecione **Configurar método de entrega AutoSupport**.

   Uma caixa de diálogo é exibida, que lista os métodos de entrega de despacho.

3. Selecione o método de entrega desejado e, em seguida, selecione os parâmetros para esse método de entrega. Execute um dos seguintes procedimentos:
   - Se você selecionou HTTPS ou HTTP, selecione um dos seguintes parâmetros de entrega:
     - **Directly** — este parâmetro de entrega é a seleção padrão. Escolher esta opção permite que você se conete diretamente ao sistema de suporte técnico de destino usando o protocolo HTTPS ou HTTP.
     - **Via servidor Proxy** — escolher esta opção permite especificar os detalhes do servidor proxy HTTP necessários para estabelecer conexão com o sistema de suporte técnico de destino. Você deve especificar o endereço do host e o número da porta. No entanto, você só precisa inserir os detalhes de autenticação do host (nome de usuário e senha), se necessário.

        - **Via Proxy auto-Configuration script (PAC)** — Especifique a localização de um arquivo de script de configuração automática de proxy (PAC). Um arquivo PAC permite que o sistema escolha automaticamente o servidor proxy apropriado para estabelecer uma conexão com o sistema de suporte técnico de destino.
    - Se você selecionou e-mail, insira as seguintes informações:
        - O endereço do servidor de correio como um nome de domínio totalmente qualificado, endereço IPv4 ou endereço IPv6.
        - O endereço de e-mail que aparece no campo de do e-mail de envio do AutoSupport.
        - **Opcional; se você quiser executar um teste de configuração.** O endereço de e-mail onde uma confirmação é enviada quando o sistema AutoSupport recebe o envio do teste.
        - Se você quiser criptografar mensagens, selecione **SMTPS** ou **STARTTLS** para o tipo de criptografia e, em seguida, selecione o número da porta para mensagens criptografadas. Caso contrário, selecione **nenhum**.
        - Se necessário, introduza um nome de utilizador e uma palavra-passe para autenticação com o remetente de saída e o servidor de correio.
4. Clique em **Configuração de teste** para testar a conexão com o servidor de suporte técnico usando os parâmetros de entrega especificados. Se você ativou o recurso AutoSupport On-Demand, o sistema também testará a conexão para entrega de despacho do AutoSupport OnDemand.

   Se o teste de configuração falhar, verifique as configurações e execute o teste novamente. Se o teste continuar falhando, entre em Contato com o suporte técnico.

5. Clique em **Salvar**.

#### O que são dados de configuração?

Quando você seleciona coletar dados de configuração, o sistema salva o estado atual do banco de dados de configuração RAID.

O banco de dados de configuração RAID inclui todos os dados para grupos de volumes e pools de discos na controladora. O recurso coletar dados de configuração salva as mesmas informações do comando CLI do `save storageArray dbmDatabase`.

#### O que eu preciso saber antes de atualizar o software SANtricity os?

Antes de atualizar o software e o firmware do controlador, tenha em atenção estes itens.

- Você leu o documento e o `readme.txt` arquivo e determinou que deseja fazer a atualização.
- Você sabe se deseja atualizar seu firmware IOM.

  Normalmente, você deve atualizar todos os componentes ao mesmo tempo. No entanto, você pode decidir não atualizar o firmware IOM se não quiser atualizá-lo como parte da atualização do software da controladora SANtricity os ou se o suporte técnico tiver instruído a fazer o downgrade do firmware IOM (você só pode fazer o downgrade do firmware usando a interface de linha de comando).

- Você sabe se deseja atualizar o arquivo NVSRAM da controladora.

  Normalmente, você deve atualizar todos os componentes ao mesmo tempo. No entanto, você pode decidir não atualizar o arquivo NVSRAM do controlador se o arquivo tiver sido corrigido ou for uma versão personalizada e você não quiser sobrescrevê-lo.

- Você sabe se deseja ativar agora ou mais tarde.

  As razões para ativar mais tarde podem incluir:

  - **Hora do dia** — a ativação do software e do firmware pode demorar muito tempo, então você pode querer esperar até que as cargas de e/S sejam mais leves. Os controladores fazem failover durante a ativação, portanto, o desempenho pode ser menor do que o normal até a atualização ser concluída.
  - * Tipo de pacote* — você pode querer testar o novo software e firmware em uma matriz de armazenamento antes de atualizar os arquivos em outras matrizes de armazenamento.

Esses componentes fazem parte da atualização do software da controladora do SANtricity os:

- **Software de gerenciamento** — System Manager é o software que gerencia o storage array.
- **Firmware do controlador** — o firmware do controlador gerencia a e/S entre hosts e volumes.
- **Controller NVSRAM** — Controller NVSRAM é um arquivo de controlador que especifica as configurações padrão para os controladores.
- **Firmware IOM** — o firmware do módulo de e/S (IOM) gerencia a conexão entre uma controladora e um compartimento de unidades. Também monitoriza o estado dos componentes.
- **Software Supervisor** — o software Supervisor é a máquina virtual em um controlador no qual o software é executado.

Como parte do processo de atualização, o driver multipath/failover e/ou o driver HBA do host também podem precisar ser atualizados para que o host possa interagir com os controladores corretamente.

Para determinar se esse é o caso, consulte "Ferramenta de Matriz de interoperabilidade do NetApp" .

Se o storage array contiver apenas uma controladora ou você não tiver um driver multipath instalado, interrompa a atividade de e/S para o storage array para evitar erros de aplicativos. Se o seu storage array tiver duas controladoras e você tiver um driver multipath instalado, não será necessário interromper a atividade de e/S.

Não faça alterações no storage array enquanto a atualização ocorrer.

**O que eu preciso saber antes de suspender a sincronização automática IOM?**

## A suspensão da sincronização automática IOM impede que o firmware IOM seja atualizado da próxima vez que ocorrer uma atualização do software da controladora SANtricity os.

Normalmente, o software da controladora e o firmware IOM são atualizados como um pacote. Você pode suspender a sincronização automática IOM se tiver uma compilação especial de firmware IOM que deseja preservar em seu gabinete. Caso contrário, você reverterá para o firmware IOM fornecido com o software da controladora da próxima vez que fizer uma atualização do software da controladora.

**Por que minha atualização de firmware está progredindo tão lentamente?**

## O progresso da atualização do firmware depende da carga geral do sistema.

Durante uma atualização online do firmware da unidade, se ocorrer uma transferência de volume durante o processo de reconstrução rápida, o sistema inicia uma reconstrução completa do volume transferido. Esta

operação pode levar uma quantidade considerável de tempo. O tempo real de reconstrução total depende de vários fatores, incluindo a quantidade de atividade de e/S que ocorre durante a operação de reconstrução, o número de unidades no grupo de volumes, a definição de prioridade de reconstrução e o desempenho da unidade.

**O que eu preciso saber antes de atualizar o firmware da unidade?**

Antes de atualizar o firmware da sua unidade, esteja ciente desses itens.

- Como precaução, faça backup de seus dados usando backup de disco para disco, cópia de volume (para um grupo de volumes não afetado pela atualização de firmware planejada) ou um espelho remoto.
- Talvez você queira atualizar apenas algumas unidades para testar o comportamento do novo firmware para garantir que ele esteja funcionando corretamente. Se o novo firmware estiver funcionando corretamente, atualize as unidades restantes.
- Se você tiver alguma unidade com falha, corrija-a antes de iniciar a atualização de firmware.
- Se as unidades puderem fazer uma atualização off-line, interrompa a atividade de e/S para todos os volumes associados às unidades. Quando a atividade de e/S é interrompida, não podem ocorrer operações de configuração associadas a esses volumes.
- Não remova nenhuma unidade durante a atualização do firmware da unidade.
- Não faça alterações de configuração no storage de armazenamento durante a atualização do firmware da unidade.

**Como faço para escolher qual tipo de atualização deve ser executada?**

Você escolhe o tipo de atualização a ser executada na unidade, dependendo do estado do pool ou do grupo de volume.

- **Online**

  Se o pool ou grupo de volumes suportar redundância e for ideal, você pode usar o método on-line para atualizar o firmware da unidade. O método Online faz o download do firmware *enquanto o storage array está processando I/o* para os volumes associados usando essas unidades. Não é necessário interromper a e/S para os volumes associados usando essas unidades. Essas unidades são atualizadas uma de cada vez para os volumes associados às unidades. Se a unidade não estiver atribuída a um pool ou grupo de volumes, o firmware poderá ser atualizado pelo método Online ou Offline. O desempenho do sistema pode ser afetado quando você usa o método on-line para atualizar o firmware da unidade.

- **Offline**

  Se o pool ou grupo de volumes não suportar redundância (RAID 0) ou estiver degradado, você deve usar o método Offline para atualizar o firmware da unidade. O método Offline atualizará o firmware *somente enquanto toda a atividade de e/S estiver parada* para os volumes associados usando essas unidades. Você deve parar todas as e/S para quaisquer volumes associados usando essas unidades. Se a unidade não estiver atribuída a um pool ou grupo de volumes, o firmware poderá ser atualizado pelo método Online ou Offline.

# Gerenciamento de vários arrays com o Unified Manager 6

## Interface principal

### Visão geral da interface do Unified Manager

O Unified Manager é uma interface baseada na Web que permite gerenciar vários storage arrays em uma única visualização.

#### Página principal

Quando você faz login no Unified Manager, a página principal é aberta para **Gerenciar - todos**. Nesta página, você pode rolar por uma lista de matrizes de armazenamento descobertas na sua rede, ver o seu status e executar operações em uma única matriz ou em um grupo de matrizes.

#### Barra lateral de navegação

Você pode acessar os recursos e funções do Unified Manager na barra lateral de navegação.

| Área | Descrição |
| --- | --- |
| Gerenciar | Descubra matrizes de armazenamento na sua rede, inicie o Gestor de sistema SANtricity para uma matriz, importe definições de uma matriz para várias matrizes e gere grupos de matrizes. Marque as caixas de seleção ao lado dos nomes dos arrays para executar operações neles, como importar configurações e criar grupos de matrizes. As elipses no final de cada linha fornecem um menu em linha para operações em um único array, como renomeá-lo. |
| Operações | Visualize o progresso das operações em lote, como importar configurações de um array para outro.<br>Algumas operações não estão disponíveis quando um storage array tem um status não ideal. |
| Gerenciamento de certificados | Gerencie certificados para autenticar entre navegadores e clientes. |
| Gerenciamento de acesso | Estabeleça a autenticação de usuário para a interface do Unified Manager. |
| Suporte | Veja opções de suporte técnico, recursos e Contatos. |

#### Definições de interface e ajuda

No canto superior direito da interface, você pode acessar a Ajuda e outra documentação. Você também pode acessar opções de administração, que estão disponíveis na lista suspensa ao lado do nome de login.

#### Logins de usuário e senhas

O usuário atual conetado ao sistema é mostrado no canto superior direito da interface.

Para obter mais informações sobre usuários e senhas, consulte:

- "Defina a proteção de senha de administrador"
- "Altere a senha de administrador"
- "Alterar senhas para perfis de usuário locais"

## Navegadores suportados

O Unified Manager pode ser acessado de vários tipos de navegadores.

Os seguintes navegadores e versões são suportados.

| Navegador | Versão mínima |
|---|---|
| Google Chrome | 89 |
| Mozilla Firefox | 80 |
| Safari | 14 |
| Microsoft Edge | 90 |

O Proxy de Serviços Web deve estar instalado e disponível para o navegador.

## Defina a proteção de senha de administrador

Você deve configurar o Unified Manager com uma senha de administrador para protegê-lo contra acesso não autorizado.

#### Senha de administrador e perfis de usuário

Ao iniciar o Unified Manager pela primeira vez, você será solicitado a definir uma senha de administrador. Qualquer usuário que tenha a senha de administrador pode fazer alterações de configuração nos storages.

Além da senha de administrador, a interface do Unified Manager inclui perfis de usuário pré-configurados com uma ou mais funções mapeadas para eles. Para obter mais informações, "Como o Gerenciamento de Acesso funciona"consulte .

Os usuários e mapeamentos não podem ser alterados. Apenas as senhas podem ser modificadas. Para alterar senhas, consulte:

- "Altere a senha de administrador"
- "Alterar senhas para perfis de usuário locais"

### Tempos limite da sessão

O software solicita a senha apenas uma vez durante uma única sessão de gerenciamento. Uma sessão expira após 30 minutos de inatividade por padrão, e nesse momento, você deve digitar a senha novamente. Se outro utilizador aceder ao software a partir de outro cliente de gestão e alterar a palavra-passe enquanto a sessão estiver em curso, ser-lhe-á pedida uma palavra-passe da próxima vez que tentar uma operação de configuração ou uma operação de visualização.

Por razões de segurança, você pode tentar inserir uma senha apenas cinco vezes antes que o software entre em um estado de "bloqueio". Neste estado, o software rejeita tentativas subsequentes de senha. Tem de esperar 10 minutos para repor o estado "normal" antes de tentar introduzir novamente uma palavra-passe.

Você pode ajustar os tempos limite da sessão ou desativar completamente os tempos limite da sessão. Para obter mais informações, "Gerenciar tempos limite de sessão"consulte .

## Altere a senha de administrador

Você pode alterar a senha de administrador usada para acessar o Unified Manager.

### Antes de começar

- Você deve estar logado como administrador local, o que inclui permissões de administrador raiz.
- Você deve saber a senha de administrador atual.

### Sobre esta tarefa

Tenha em mente estas diretrizes ao escolher uma senha:

- As senhas diferenciam maiúsculas de minúsculas.
- Os espaços de saída não são removidos das senhas quando são definidos. Tenha cuidado para incluir espaços se eles foram incluídos na senha.
- Para maior segurança, use pelo menos 15 carateres alfanuméricos e altere a senha com frequência.

### Passos

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **funções de usuário local**.
3. Selecione o usuário **admin** na tabela.

   O botão alterar senha fica disponível.

4. Selecione **alterar palavra-passe**.

   A caixa de diálogo alterar senha será exibida.

5. Se não estiver definido um comprimento mínimo de palavra-passe para palavras-passe de utilizador local, selecione a caixa de verificação para exigir que o utilizador introduza uma palavra-passe para aceder ao sistema.
6. Introduza a nova palavra-passe nos dois campos.
7. Introduza a palavra-passe do administrador local para confirmar esta operação e, em seguida, clique em **alterar**.

## Gerenciar tempos limite de sessão

É possível configurar tempos limite para o Unified Manager para que os usuários de sessões inativas sejam desconetadas após um tempo especificado.

### Sobre esta tarefa

Por padrão, o tempo limite da sessão para o Unified Manager é de 30 minutos. Você pode ajustar esse tempo ou pode desativar os tempos limite da sessão por completo.

> Se o Gerenciamento de Acesso for configurado usando os recursos SAML (Security Assertion Markup Language) incorporados no array, um tempo limite de sessão pode ocorrer quando a sessão SSO do usuário atingir seu limite máximo. Isso pode ocorrer antes do tempo limite da sessão do System Manager.

### Passos

1. Na barra de menus, selecione a seta suspensa ao lado do nome de login do usuário.
2. Selecione **Ativar/Desativar tempo limite da sessão**.

   A caixa de diálogo Ativar/Desativar tempo limite da sessão é aberta.
3. Utilize os controlos giratórios para aumentar ou diminuir o tempo em minutos.

   O tempo limite mínimo que você pode definir é de 15 minutos.

   > Para desativar os tempos limite de sessão, desmarque a caixa de seleção **Definir o período de tempo…**.
4. Clique em **Salvar**.

# Storage arrays

## Descrição geral da descoberta

Para gerenciar recursos de armazenamento, primeiro você deve descobrir os storages de armazenamento na rede.

### Como faço para descobrir arrays?

Use a página Adicionar/descobrir para localizar e adicionar os storages de armazenamento que você deseja gerenciar na rede da sua organização. Você pode descobrir vários arrays ou descobrir um único array. Para fazer isso, você insere endereços IP de rede e, em seguida, o Unified Manager tenta conexões individuais para cada endereço IP nesse intervalo.

Saiba mais:

- "Considerações para descobrir arrays"
- "Descubra vários storages de armazenamento"
- "Descubra um único array"

### Como faço para gerenciar arrays?

Depois de descobrir arrays, vá para a página **Gerenciar - todos**. Nesta página, você pode rolar por uma lista de matrizes de armazenamento descobertas na sua rede, ver o seu status e executar operações em uma única matriz ou em um grupo de matrizes.

Se você quiser gerenciar um único array, selecione-o e abra o System Manager.

Saiba mais:

- "Considerações para acessar o System Manager"
- "Gerenciar um storage array individual"
- "Ver o status do storage array"

## Conceitos

### Considerações para descobrir arrays

Antes que o Unified Manager possa exibir e gerenciar recursos de storage, ele deve descobrir os storages que você deseja gerenciar na rede da organização. Você pode descobrir vários arrays ou descobrir um único array.

#### Descobrindo vários storages de armazenamento

Se você optar por descobrir vários arrays, insira um intervalo de endereços IP de rede e, em seguida, o Unified Manager tentará conexões individuais para cada endereço IP nesse intervalo. Qualquer matriz de armazenamento alcançada com sucesso aparece na página descobrir e pode ser adicionada ao seu domínio de gerenciamento.

#### Descobrindo um único storage array

Se você optar por descobrir um único array, insira o endereço IP único de um dos controladores no storage array e, em seguida, o storage array individual será adicionado.

> O Unified Manager deteta e exibe apenas o único endereço IP ou endereço IP dentro de um intervalo atribuído a um controlador. Se houver controladores alternativos ou endereços IP atribuídos a esses controladores que estejam fora desse único endereço IP ou intervalo de endereços IP, o Unified Manager não os detetará ou exibirá. No entanto, depois de adicionar a matriz de armazenamento, todos os endereços IP associados serão descobertos e exibidos na visualização Gerenciar.

#### Credenciais do usuário

Como parte do processo de descoberta, você deve fornecer a senha de administrador para cada storage que deseja adicionar.

#### Certificados de serviços da Web

Como parte do processo de descoberta, o Unified Manager verifica se os storage arrays descobertos estão usando certificados de uma fonte confiável. O Unified Manager usa dois tipos de autenticação baseada em certificado para todas as conexões que estabelece com o navegador:

- **Certificados confiáveis**

Para storages descobertos pelo Unified Manager, talvez seja necessário instalar certificados confiáveis adicionais fornecidos pela Autoridade de certificação.

Use o botão **Import** para importar esses certificados. Se você já tiver conetado a esse array antes, um ou ambos os certificados do controlador expiram, revogam ou faltam um certificado raiz ou um certificado intermediário em sua cadeia de certificados. Você deve substituir o certificado expirado ou revogado ou adicionar o certificado raiz ou o certificado intermediário em falta antes de gerenciar o storage array.

- **Certificados autoassinados**

  Certificados autoassinados também podem ser usados. Se o administrador tentar descobrir matrizes sem importar certificados assinados, o Unified Manager exibirá uma caixa de diálogo de erro que permite que o administrador aceite o certificado autoassinado. O certificado autoassinado do storage array será marcado como confiável e o storage array será adicionado ao Unified Manager.

  Se você não confiar nas conexões com o storage array, selecione **Cancelar** e valide a estratégia de certificado de segurança do storage antes de adicionar o storage array ao Unified Manager.

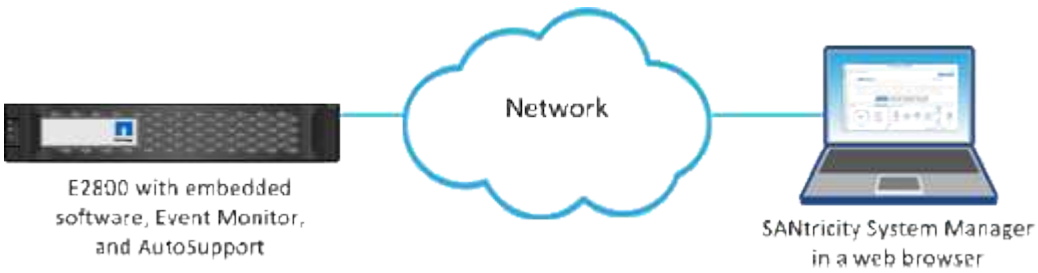
#### Considerações para acessar o System Manager

Selecione um ou mais storages e use a opção Iniciar para abrir o System Manager quando quiser configurar e gerenciar storages.

O System Manager é uma aplicação incorporada nos controladores, que está ligada à rede através de uma porta de gestão Ethernet. Ele inclui todas as funções baseadas em array.

Para acessar o System Manager, você deve ter:

- Um dos modelos de array listados aqui: "Visão geral do hardware e-Series"
- Uma conexão fora da banda a um cliente de gerenciamento de rede com um navegador da Web.




## Descubra arrays

#### Descubra vários storages de armazenamento

Você descobre várias matrizes para detetar todas as matrizes de armazenamento na sub-rede onde reside o servidor de gestão e para adicionar automaticamente as matrizes descobertas ao seu domínio de gestão.

#### Antes de começar

- Você deve estar conetado com um perfil de usuário que inclua permissões de Administrador de Segurança.
- A matriz de armazenamento deve ser corretamente configurada e configurada.

- As senhas do storage array devem ser configuradas usando o bloco Gerenciamento de Acesso do System Manager.
- Para resolver certificados não confiáveis, você deve ter arquivos de certificado confiáveis de uma autoridade de certificação (CA) e os arquivos de certificado estão disponíveis no sistema local.

Descobrir arrays é um procedimento de várias etapas.

#### Etapa 1: Insira o endereço de rede

Introduza um intervalo de endereços de rede para pesquisar na sub-rede local. Qualquer matriz de armazenamento alcançada com sucesso aparece na página descobrir e pode ser adicionada ao seu domínio de gerenciamento.

Se você precisar parar a operação de descoberta por qualquer motivo, clique em **Stop Discovery**.

**Passos**

1. Na página Gerenciar, selecione **Adicionar/descobrir**.

   A caixa de diálogo Adicionar/descobrir é exibida.

2. Selecione o botão de opção **Discover all storage arrays within a network range**.
3. Introduza o endereço de rede inicial e o endereço de rede final para procurar na sub-rede local e, em seguida, clique em **Iniciar descoberta**.

   O processo de descoberta é iniciado. Este processo de descoberta pode levar vários minutos para ser concluído. A tabela na página descobrir é preenchida à medida que os storages são descobertos.

   Se não forem detetados arrays gerenciáveis, verifique se os storages de armazenamento estão conetados corretamente à sua rede e se seus endereços atribuídos estão dentro do alcance. Clique em **New Discovery Parameters** (novos parâmetros de descoberta) para voltar à página Add/Discover (Adicionar/descobrir).

4. Reveja a lista de matrizes de armazenamento descobertas.
5. Marque a caixa de seleção ao lado de qualquer matriz de armazenamento que você deseja adicionar ao seu domínio de gerenciamento e clique em **Avançar**.

   O Unified Manager executa uma verificação de credenciais em cada array que você está adicionando ao domínio de gerenciamento. Talvez seja necessário resolver quaisquer certificados autoassinados e certificados não confiáveis associados a essa matriz.

6. Clique em **Next** (seguinte) para avançar para a próxima etapa do assistente.

#### Etapa 2: Resolva certificados autoassinados durante a descoberta

Como parte do processo de descoberta, o sistema verifica se os storages de armazenamento estão usando certificados por uma fonte confiável.

**Passos**

1. Execute um dos seguintes procedimentos:
   - Se você confiar nas conexões com os storages de armazenamento descobertos, continue para a próxima placa no assistente. Os certificados autoassinados serão marcados como confiáveis e os storages de armazenamento serão adicionados ao Unified Manager.

◦ Se você não confiar nas conexões com os storages de armazenamento, selecione **Cancelar** e valide a estratégia de certificado de segurança de cada storage antes de adicionar qualquer um deles ao Unified Manager.

2. Clique em **Next** (seguinte) para avançar para a próxima etapa do assistente.

#### Etapa 3: Resolva certificados não confiáveis durante a descoberta

Certificados não confiáveis ocorrem quando um storage array tenta estabelecer uma conexão segura com o Unified Manager, mas a conexão não consegue confirmar como segura. Durante o processo de descoberta de matriz, você pode resolver certificados não confiáveis importando um certificado de autoridade de certificação (CA) (ou certificado assinado pela CA) emitido por um terceiro confiável.

Talvez seja necessário instalar certificados de CA confiáveis adicionais se alguma das seguintes opções for verdadeira:

- Recentemente, você adicionou uma matriz de armazenamento.
- Um ou ambos os certificados expiram.
- Um ou ambos os certificados são revogados.
- Um ou ambos os certificados estão faltando um certificado raiz ou intermediário.

**Passos**

1. Marque a caixa de seleção ao lado de qualquer storage para o qual você deseja resolver certificados não confiáveis e selecione o botão **Importar**.

   Abre-se uma caixa de diálogo para importar os ficheiros de certificado fidedignos.

2. Clique em **Procurar** para selecionar os arquivos de certificado para os storages de armazenamento.

   Os nomes dos arquivos são exibidos na caixa de diálogo.

3. Clique em **Importar**.

   Os arquivos são carregados e validados.

   Qualquer storage array com problemas de certificado não confiáveis que não sejam resolvidos não será adicionado ao Unified Manager.

4. Clique em **Next** (seguinte) para avançar para a próxima etapa do assistente.

#### Passo 4: Forneça senhas

Você deve inserir as senhas dos storages de armazenamento que deseja adicionar ao seu domínio de gerenciamento.

**Passos**

1. Introduza a palavra-passe para cada matriz de armazenamento que pretende adicionar ao Unified Manager.
2. **Opcional:** associar matrizes de armazenamento a um grupo: Na lista pendente, selecione o grupo pretendido a associar com as matrizes de armazenamento selecionadas.
3. Clique em **Finish**.

**Depois de terminar**

Os storages de armazenamento são adicionados ao domínio de gerenciamento e associados ao grupo selecionado (se especificado).

Pode levar alguns minutos para que o Unified Manager se conecte aos storage arrays especificados.

**Descubra um único array**

## Use a opção Add/Discover Single Storage Array (Adicionar/descobrir matriz de armazenamento única) para descobrir e adicionar manualmente uma única matriz de armazenamento à rede da sua organização.

**Antes de começar**

- A matriz de armazenamento deve ser corretamente configurada e configurada.
- As senhas do storage array devem ser configuradas usando o bloco Gerenciamento de Acesso do System Manager.

**Passos**

1. Na página Gerenciar, selecione **Adicionar/descobrir**.

   A caixa de diálogo Adicionar/descobrir é exibida.

2. Selecione o botão de opção **Discover a single storage array**.
3. Insira o endereço IP de um dos controladores na matriz de armazenamento e clique em **Start Discovery**.

   Pode levar alguns minutos para que o Unified Manager se conecte ao storage array especificado.

   A mensagem Storage Array Not Accessible (Matriz de armazenamento não acessível) é exibida quando a conexão com o endereço IP do controlador especificado não for bem-sucedida.

4. Se solicitado, resolva quaisquer certificados autoassinados.

   Como parte do processo de descoberta, o sistema verifica se os storages descobertos estão usando certificados por uma fonte confiável. Se não conseguir localizar um certificado digital para uma matriz de armazenamento, ele solicitará que você resolva o certificado que não está assinado por uma autoridade de certificação (CA) reconhecida adicionando uma exceção de segurança.

5. Se solicitado, resolva quaisquer certificados não confiáveis.

   Certificados não confiáveis ocorrem quando um storage array tenta estabelecer uma conexão segura com o Unified Manager, mas a conexão não consegue confirmar como segura. Resolva certificados não confiáveis importando um certificado de autoridade de certificação (CA) emitido por um terceiro confiável.

6. Clique em **seguinte**.
7. **Opcional:** associar a matriz de armazenamento descoberta a um grupo: Na lista suspensa, selecione o grupo desejado a ser associado à matriz de armazenamento.

   O grupo "All" (todos) é selecionado por predefinição.

8. Insira a senha de administrador do storage que você deseja adicionar ao domínio de gerenciamento e

clique em **OK**.

**Depois de terminar**

O storage array é adicionado ao Unified Manager e, se especificado, também é adicionado ao grupo selecionado.

Se a coleta automática de dados de suporte estiver ativada, os dados de suporte serão coletados automaticamente para um storage array que você adicionar.

## Gerenciar arrays

### Ver o status do storage array

O Unified Manager exibe o status de cada storage array descoberto.

Vá para a página **Gerenciar - todos**. Nesta página, você pode visualizar o status da conexão entre o Proxy de Serviços Web e esse storage array.

Os indicadores de status são descritos na tabela a seguir.

| Estado | Indica |
|---|---|
| Ideal | O storage array está em um estado ideal. Não há problemas de certificado e a senha é válida. |
| Palavra-passe inválida | Foi fornecida uma palavra-passe inválida da matriz de armazenamento. |
| Certificado não fidedigno | Uma ou mais conexões com o storage não são confiáveis porque o certificado HTTPS é autoassinado e não foi importado, ou o certificado é assinado pela CA e os certificados raiz e intermediário da CA não foram importados. |
| Precisa de atenção | Há um problema com o storage array que requer a sua intervenção para corrigi-lo. |
| Bloqueio | O storage array está em um estado bloqueado. |
| Desconhecido | O storage array nunca foi contatado. Isso pode acontecer quando o Web Services Proxy está sendo iniciado e ainda não entrou em Contato com o storage array, ou o storage está offline e nunca foi contatado desde que o Web Services Proxy foi iniciado. |
| Offline | O Web Services Proxy já havia contatado o storage array, mas agora perdeu toda a conexão com ele. |

### Gerenciar um storage array individual

Você pode usar a opção Iniciar para abrir o System Manager baseado em navegador para um ou mais arrays de storage quando quiser executar operações de gerenciamento.

**Passos**

1. Na página Gerenciar, selecione um ou mais arrays de armazenamento que você deseja gerenciar.
2. Clique em **Launch**.

   O sistema abre uma nova janela e exibe a página de login do System Manager.

3. Digite seu nome de usuário e senha e clique em **Log in**.

### Altere as senhas do storage array

Você pode atualizar as senhas usadas para visualizar e acessar matrizes de armazenamento no Unified Manager.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de armazenamento.
- Você deve saber a senha atual para a matriz de armazenamento, que é definida no System Manager.

**Sobre esta tarefa**

Nesta tarefa, insira a senha atual de um storage array para que você possa acessá-lo no Unified Manager. Isso pode ser necessário se a senha do array tiver sido alterada no System Manager e, agora, ela também deve ser alterada no Unified Manager.

**Passos**

1. Na página Gerenciar, selecione um ou mais arrays de armazenamento.
2. Selecione **tarefas incomuns › fornecer senhas de storage de armazenamento**.
3. Insira a senha ou as senhas de cada matriz de armazenamento e clique em **Salvar**.

### Remova os storage arrays do SANtricity Unified Manager

Você pode remover um ou mais arrays de storage se não quiser mais gerenciá-lo do Unified Manager.

**Sobre esta tarefa**

Não é possível acessar nenhum dos storages de armazenamento que você remover. Você pode, no entanto, estabelecer uma conexão com qualquer um dos storages removidos apontando um navegador diretamente para seu endereço IP ou nome de host.

A remoção de um storage array não afeta o storage array ou seus dados de forma alguma. Se uma matriz de armazenamento for removida acidentalmente, ela pode ser adicionada novamente.

**Passos**

1. Selecione a página **Gerenciar**.
2. Selecione um ou mais storages que você deseja remover.
3. Selecione **tarefas incomuns › Remove storage array**.

   O storage array é removido de todas as visualizações no Gerenciador Unificado do SANtricity.

# Importação de definições

## Descrição geral das definições de importação

O recurso Importar configurações permite que você execute uma operação em lote para importar as configurações de uma matriz para várias matrizes. Esse recurso economiza tempo quando você precisa configurar vários arrays na rede.

#### Que definições podem ser importadas?

Você pode importar métodos de alerta, configurações do AutoSupport, configurações dos Serviços de diretório, configurações de armazenamento (como grupos de volumes e pools) e configurações do sistema (como balanceamento de carga automático).

Saiba mais:

- "Como as Configurações de importação funcionam"
- "Requisitos para replicação de configurações de storage"

#### Como faço para executar uma importação em lote?

Em uma matriz de armazenamento a ser usada como fonte, abra o System Manager e configure as configurações desejadas. Em seguida, no Unified Manager, vá para a página Gerenciar e importe as configurações para um ou mais arrays.

Saiba mais:

- "Importar definições de alerta"
- "Importar definições do AutoSupport"
- "Importar definições dos serviços de diretório"
- "Importar definições de configuração de armazenamento"
- "Importar definições do sistema"

## Conceitos

#### Como as Configurações de importação funcionam

Você pode usar o Unified Manager para importar configurações de um storage array para vários storage arrays. O recurso Importar configurações é uma operação em lote que economiza tempo quando você precisa configurar vários arrays na rede.

##### Definições disponíveis para importação

As configurações a seguir podem ser importadas para vários storages:

- **Alertas** — métodos de alertas para enviar eventos importantes para administradores, usando e-mail, um servidor syslog ou um servidor SNMP.
- **AutoSupport** — um recurso que monitora a integridade de um storage array e envia envios automáticos para o suporte técnico.

- **Serviços de diretório** — Um método de autenticação de usuário gerenciado por meio de um servidor LDAP (Lightweight Directory Access Protocol) e serviço de diretório, como o ative Directory da Microsoft.
- **Configuração de armazenamento** — Configurações relacionadas ao seguinte:
  - Volumes (somente volumes espessos e não-repositórios)
  - Grupos de volume e pools
  - Atribuições de unidades hot spare
- **Configurações do sistema** — Configurações relacionadas ao seguinte:
  - Definições de digitalização de multimédia para um volume
  - Definições SSD
  - Balanceamento de carga automático (não inclui relatórios de conectividade de host)

#### Fluxo de trabalho de configuração

Para importar configurações, siga este fluxo de trabalho:

1. Em uma matriz de armazenamento a ser usada como origem, configure as configurações usando o System Manager.
2. Nos storages a serem usados como destinos, faça backup de sua configuração usando o System Manager.
3. No Unified Manager, vá para a página **Manage** e importe as configurações.
4. Na página **operações**, revise os resultados da operação Importar configurações.

### Requisitos para replicação de configurações de storage

Antes de importar uma configuração de armazenamento de um storage array para outro, revise os requisitos e as diretrizes.

#### Compartimentos

- Os compartimentos em que os controladores residem devem ser idênticos nos arrays de origem e destino.
- As IDs de gaveta devem ser idênticas nos arrays de origem e destino.
- Os compartimentos de expansão devem ser preenchidos nos mesmos slots com os mesmos tipos de unidade (se a unidade for usada na configuração, o local das unidades não utilizadas não importa).

#### Controladores

- O tipo de controlador pode ser diferente entre os arrays de origem e destino (por exemplo, importando de um E2800 para um E5700), mas o tipo de gabinete RBOD deve ser idêntico.
- As HICs, incluindo os recursos DA DO host, devem ser idênticas entre os arrays de origem e destino.
- A importação de uma configuração duplex para simplex não é suportada; no entanto, a importação de simplex para duplex é permitida.
- As definições FDE não estão incluídas no processo de importação.

#### Estado

- Os arrays de destino devem estar no status ideal.

- O array de origem não precisa estar no status ideal.

#### Armazenamento

- A capacidade da unidade pode variar entre os arrays de origem e destino, desde que a capacidade de volume no destino seja maior do que a origem. (Um array de destino pode ter unidades de capacidade mais novas e maiores que não seriam totalmente configuradas em volumes pela operação de replicação.)
- Volumes de pool de discos de 64 TB ou maiores no array de origem impedirão o processo de importação nos destinos.
- Os volumes finos não estão incluídos no processo de importação.

## Use importações de lote

### Importar definições de alerta

Você pode importar configurações de alerta de um storage array para outros storage arrays. Esta operação em lote economiza tempo quando você precisa configurar vários arrays na rede.

#### Antes de começar

- Os alertas são configurados no System Manager para a matriz de armazenamento que você deseja usar como fonte (**Configurações › Alertas**).
- A configuração existente para os storages de armazenamento de destino é feita com backup no System Manager (**Configurações › sistema › Salvar configuração da matriz de armazenamento**).

#### Sobre esta tarefa

Você pode selecionar alertas de e-mail, SNMP ou syslog para a operação de importação. As definições importadas incluem:

- **Alertas por e-mail** — Um endereço de servidor de e-mail e os endereços de e-mail dos destinatários do alerta.
- **Alertas Syslog** — Um endereço de servidor syslog e uma porta UDP.
- **Alertas SNMP** — Um nome de comunidade e endereço IP para o servidor SNMP.

#### Passos

1. Na página Gerenciar, clique em **Importar configurações**.

   O assistente Importar configurações é aberto.

2. Na caixa de diálogo Selecionar configurações, selecione **Email alerts**, **SNMP alerts** ou **Syslog alerts** e, em seguida, clique em **Next**.

   Abre-se uma caixa de diálogo para selecionar a matriz de origem.

3. Na caixa de diálogo Selecionar fonte, selecione a matriz com as configurações que deseja importar e clique em **Avançar**.
4. Na caixa de diálogo Selecionar destinos, selecione um ou mais arrays para receber as novas configurações.

Matrizes de armazenamento com firmware abaixo de 8,50 não estão disponíveis para seleção. Além disso, uma matriz não aparece nesta caixa de diálogo se o Unified Manager não puder se comunicar com essa matriz (por exemplo, se estiver offline ou se tiver problemas de certificado, senha ou rede).

5. Clique em **Finish**.

   A página operações exibe os resultados da operação de importação. Se a operação falhar, você pode clicar em sua linha para ver mais informações.

**Resultados**

Os storages de armazenamento de destino agora estão configurados para enviar alertas aos administradores por e-mail, SNMP ou syslog.

### Importar definições do AutoSupport

Você pode importar uma configuração do AutoSupport de um storage array para outros storage arrays. Esta operação em lote economiza tempo quando você precisa configurar vários arrays na rede.

**Antes de começar**

- O AutoSupport é configurado no Gerenciador de sistema para o storage array que você deseja usar como origem (**suporte › Centro de suporte**).
- A configuração existente para os storages de armazenamento de destino é feita com backup no System Manager (**Configurações › sistema › Salvar configuração da matriz de armazenamento**).

**Sobre esta tarefa**

As configurações importadas incluem os recursos separados (Basic AutoSupport, AutoSupport OnDemand e Remote Diagnostics), a janela de manutenção, o método de entrega e o agendamento de envio.

**Passos**

1. Na página Gerenciar, clique em **Importar configurações**.

   O assistente Importar configurações é aberto.

2. Na caixa de diálogo Selecionar configurações, selecione **AutoSupport** e clique em **Avançar**.

   Abre-se uma caixa de diálogo para selecionar a matriz de origem.

3. Na caixa de diálogo Selecionar fonte, selecione a matriz com as configurações que deseja importar e clique em **Avançar**.
4. Na caixa de diálogo Selecionar destinos, selecione um ou mais arrays para receber as novas configurações.

   Matrizes de armazenamento com firmware abaixo de 8,50 não estão disponíveis para seleção. Além disso, uma matriz não aparece nesta caixa de diálogo se o Unified Manager não puder se comunicar com essa matriz (por exemplo, se estiver offline ou se tiver problemas de certificado, senha ou rede).

5. Clique em **Finish**.

A página operações exibe os resultados da operação de importação. Se a operação falhar, você pode clicar em sua linha para ver mais informações.

**Resultados**

Os storages de armazenamento de destino agora são configurados com as mesmas configurações de AutoSupport que o array de origem.

### Importar definições dos serviços de diretório

Você pode importar uma configuração de serviços de diretório de um storage array para outros storage arrays. Esta operação em lote economiza tempo quando você precisa configurar vários arrays na rede.

**Antes de começar**

- Os serviços de diretório são configurados no System Manager para a matriz de armazenamento que você deseja usar como fonte (**Configurações › Gerenciamento de Acesso**).
- A configuração existente para os storages de armazenamento de destino é feita com backup no System Manager (**Configurações › sistema › Salvar configuração da matriz de armazenamento**).

**Sobre esta tarefa**

As configurações importadas incluem o nome de domínio e URL de um servidor LDAP (Lightweight Directory Access Protocol), juntamente com os mapeamentos para os grupos de usuários do servidor LDAP para as funções predefinidas do storage array.

**Passos**

1. Na página Gerenciar, clique em **Importar configurações**.

   O assistente Importar configurações é aberto.

2. Na caixa de diálogo Selecionar configurações, selecione **Serviços de diretório** e clique em **Avançar**.

   Abre-se uma caixa de diálogo para selecionar a matriz de origem.

3. Na caixa de diálogo Selecionar fonte, selecione a matriz com as configurações que deseja importar e clique em **Avançar**.
4. Na caixa de diálogo Selecionar destinos, selecione um ou mais arrays para receber as novas configurações.

   > Matrizes de armazenamento com firmware abaixo de 8,50 não estão disponíveis para seleção. Além disso, uma matriz não aparece nesta caixa de diálogo se o Unified Manager não puder se comunicar com essa matriz (por exemplo, se estiver offline ou se tiver problemas de certificado, senha ou rede).

5. Clique em **Finish**.

   A página operações exibe os resultados da operação de importação. Se a operação falhar, você pode clicar em sua linha para ver mais informações.

#### Resultados

Os storages de armazenamento de destino agora são configurados com os mesmos serviços de diretório que o array de origem.

### Importar definições do sistema

Você pode importar a configuração do sistema de um storage array para outros storage arrays. Esta operação em lote economiza tempo quando você precisa configurar vários arrays na rede.

#### Antes de começar

- As configurações do sistema são configuradas no System Manager para a matriz de armazenamento que você deseja usar como origem.
- A configuração existente para os storages de armazenamento de destino é feita com backup no System Manager (**Configurações › sistema › Salvar configuração da matriz de armazenamento**).

#### Sobre esta tarefa

As definições importadas incluem definições de digitalização de multimédia para um volume, definições de SSD para controladores e balanceamento de carga automático (não inclui relatórios de conetividade do anfitrião).

#### Passos

1. Na página Gerenciar, clique em **Importar configurações**.

   O assistente Importar configurações é aberto.

2. Na caixa de diálogo Selecionar configurações, selecione **sistema** e clique em **Avançar**.

   Abre-se uma caixa de diálogo para selecionar a matriz de origem.

3. Na caixa de diálogo Selecionar fonte, selecione a matriz com as configurações que deseja importar e clique em **Avançar**.
4. Na caixa de diálogo Selecionar destinos, selecione um ou mais arrays para receber as novas configurações.

   > Matrizes de armazenamento com firmware abaixo de 8,50 não estão disponíveis para seleção. Além disso, uma matriz não aparece nesta caixa de diálogo se o Unified Manager não puder se comunicar com essa matriz (por exemplo, se estiver offline ou se tiver problemas de certificado, senha ou rede).

5. Clique em **Finish**.

   A página operações exibe os resultados da operação de importação. Se a operação falhar, você pode clicar em sua linha para ver mais informações.

#### Resultados

Os storages de armazenamento de destino agora são configurados com as mesmas configurações do sistema que o array de origem.

### Importar definições de configuração de armazenamento

Você pode importar a configuração de armazenamento de um storage array para outros storage arrays. Esta operação em lote economiza tempo quando você precisa configurar vários arrays na rede.

#### Antes de começar

- O armazenamento é configurado no Gerenciador de sistema do SANtricity para o storage array que você deseja usar como origem.
- A configuração existente para os storages de armazenamento de destino é feita com backup no System Manager (**Configurações › sistema › Salvar configuração da matriz de armazenamento**).
- Os arrays de origem e destino devem atender a estes requisitos:
  - As gavetas em que os controladores residem devem ser idênticas.
  - As IDs de gaveta devem ser idênticas.
  - Os compartimentos de expansão devem ser preenchidos nos mesmos slots com os mesmos tipos de unidades.
  - O tipo de compartimento RBOD deve ser idêntico.
  - As HICs, incluindo os recursos de Garantia de dados do host, devem ser idênticas.
  - Os arrays de destino devem estar no status ideal.
  - A capacidade de volume no array de destino é maior do que a capacidade do array de origem.
- Você entende as seguintes restrições:
  - A importação de uma configuração duplex para simplex não é suportada; no entanto, a importação de simplex para duplex é permitida.
  - Volumes de pool de discos de 64 TB ou maiores no array de origem impedirão o processo de importação nos destinos.
  - Os volumes finos não estão incluídos no processo de importação.

#### Sobre esta tarefa

As configurações importadas incluem volumes configurados (somente volumes espessos e não-repositórios), grupos de volumes, pools e atribuições de unidades hot spare.

#### Passos

1. Na página Gerenciar, clique em **Importar configurações**.

   O assistente Importar configurações é aberto.

2. Na caixa de diálogo Selecionar configurações, selecione **Configuração de armazenamento** e clique em **Avançar**.

   Abre-se uma caixa de diálogo para selecionar a matriz de origem.

3. Na caixa de diálogo Selecionar fonte, selecione a matriz com as configurações que deseja importar e clique em **Avançar**.
4. Na caixa de diálogo Selecionar destinos, selecione um ou mais arrays para receber as novas configurações.

Matrizes de armazenamento com firmware abaixo de 8,50 não estão disponíveis para seleção. Além disso, uma matriz não aparece nesta caixa de diálogo se o Unified Manager não puder se comunicar com essa matriz (por exemplo, se estiver offline ou se tiver problemas de certificado, senha ou rede).

5. Clique em **Finish**.

   A página operações exibe os resultados da operação de importação. Se a operação falhar, você pode clicar em sua linha para ver mais informações.

**Resultados**

Os storage arrays de destino agora são configurados com a mesma configuração de armazenamento que o array de origem.

## FAQs

**Que definições serão importadas?**

O recurso Importar configurações é uma operação em lote que carrega configurações de uma matriz de armazenamento para várias matrizes de armazenamento. As configurações importadas durante essa operação dependem de como o storage de armazenamento de origem é configurado no System Manager.

As seguintes configurações podem ser importadas para vários storages de armazenamento:

- **Alertas por e-mail** — as configurações incluem um endereço de servidor de e-mail e os endereços de e-mail dos destinatários do alerta.
- **Alertas Syslog** — as configurações incluem um endereço de servidor syslog e uma porta UDP.
- **Alertas SNMP** — as configurações incluem um nome de comunidade e endereço IP para o servidor SNMP.
- **AutoSupport** — as configurações incluem os recursos separados (AutoSupport Básico, OnDemand do AutoSupport e Diagnóstico remoto), a janela de manutenção, o método de entrega e o cronograma de envio.
- **Serviços de diretório** — a configuração inclui o nome de domínio e URL de um servidor LDAP (Lightweight Directory Access Protocol), juntamente com os mapeamentos para os grupos de usuários do servidor LDAP para as funções predefinidas do storage array.
- **Configuração de armazenamento** — as configurações incluem volumes (somente volumes espessos e somente não-repositórios), grupos de volumes, pools e atribuições de unidades hot spare.
- * Configurações do sistema* — as configurações incluem configurações de varredura de Mídia para um volume, cache SSD para controladores e balanceamento de carga automático (não inclui relatórios de conetividade do host).

**Por que não vejo todos os meus arrays de armazenamento?**

Durante a operação Importar configurações, alguns dos storages de armazenamento podem não estar disponíveis na caixa de diálogo seleção de destino.

Os storage arrays podem não aparecer pelos seguintes motivos:

- A versão do firmware é inferior a 8,50.
- A matriz de armazenamento está offline.
- O sistema não pode se comunicar com esse array (por exemplo, o array tem problemas de certificado, senha ou rede).

# Grupos de array

## Visão geral dos grupos

Na página Gerenciar grupos, você pode criar um conjunto de grupos de storage para facilitar o gerenciamento.

### O que são grupos de matriz?

Você pode gerenciar sua infraestrutura física e virtualizada agrupando um conjunto de storage arrays. Você pode querer agrupar storages para facilitar a execução de tarefas de monitoramento ou geração de relatórios.

Existem dois tipos de grupos:

- **All group** — o grupo All é o grupo padrão e inclui todos os storages de armazenamento descobertos em sua organização. O grupo todos pode ser acessado a partir da vista principal.
- **Grupo criado pelo usuário** — Um grupo criado pelo usuário inclui os storages que você seleciona manualmente para adicionar a esse grupo. Os grupos criados pelo utilizador podem ser acedidos a partir da vista principal.

### Como configuro grupos?

Na página Gerenciar grupos, você pode criar um grupo e adicionar matrizes a esse grupo.

Saiba mais:

- "Configurar o grupo de storage array"

## Configurar o grupo de storage array

Você cria grupos de armazenamento e adiciona matrizes de armazenamento aos grupos.

A configuração de grupos é um procedimento de duas etapas.

### Passo 1: Criar grupo

Primeiro você cria um grupo. O grupo de armazenamento define quais unidades fornecem o armazenamento que compõe o volume.

#### Passos

1. Na página Gerenciar, selecione **Gerenciar grupos › criar grupo de matriz de armazenamento**.
2. No campo **Nome**, digite um nome para o novo grupo.
3. Selecione as matrizes de armazenamento que pretende adicionar ao novo grupo.
4. Clique em **criar**.

#### Etapa 2: Adicionar storage array ao grupo

Você pode adicionar um ou mais arrays de armazenamento a um grupo criado pelo usuário.

**Passos**

1. Na exibição principal, selecione **Gerenciar** e, em seguida, selecione o grupo ao qual você deseja adicionar matrizes de armazenamento.
2. Selecione **Gerenciar grupos › Adicionar matrizes de armazenamento ao grupo**.
3. Selecione as matrizes de armazenamento que pretende adicionar ao grupo.
4. Clique em **Add.**

## Remova os storages de armazenamento do grupo

Você pode remover um ou mais arrays de armazenamento gerenciados de um grupo se não quiser mais gerenciá-los de um grupo de armazenamento específico.

**Sobre esta tarefa**

A remoção de matrizes de armazenamento de um grupo não afeta a matriz de armazenamento ou os seus dados de forma alguma. Se o storage array for gerenciado pelo System Manager, você ainda poderá gerenciá-lo usando o navegador. Se um storage array for removido acidentalmente de um grupo, ele poderá ser adicionado novamente.

**Passos**

1. Na página Gerenciar, selecione **Gerenciar grupos › Remover matrizes de armazenamento do grupo**.
2. Na lista suspensa, selecione o grupo que contém os storages de armazenamento que deseja remover e clique na caixa de seleção ao lado de cada storage array que você deseja remover do grupo.
3. Clique em **Remover**.

## Eliminar grupo de matrizes de armazenamento

Você pode remover um ou mais grupos de storage que não são mais necessários.

**Sobre esta tarefa**

Esta operação exclui apenas o grupo de matrizes de armazenamento. Os storage arrays associados ao grupo excluído permanecem acessíveis por meio da exibição Gerenciar tudo ou qualquer outro grupo ao qual está associado.

**Passos**

1. Na página Gerenciar, selecione **Gerenciar grupos › Excluir grupo de matrizes de armazenamento**.
2. Selecione um ou mais grupos de matrizes de armazenamento que pretende eliminar.
3. Clique em **Excluir**.

## Renomeie o grupo de storage array

Você pode alterar o nome de um grupo de storage array quando o nome atual não for mais significativo ou aplicável.

**Sobre esta tarefa**

Tenha em mente estas diretrizes.

- Um nome pode consistir em letras, números e os carateres especiais sublinhado (_), hífen (-) e libra ( no). Se você escolher outros carateres, uma mensagem de erro será exibida. Você é solicitado a escolher outro nome.
- Limite o nome para 30 carateres. Todos os espaços à esquerda e à direita no nome são eliminados.
- Use um nome único e significativo que seja fácil de entender e lembrar.
- Evite nomes arbitrários ou nomes que rapidamente perderem seu significado no futuro.

**Passos**

1. Na exibição principal, selecione **Gerenciar** e, em seguida, selecione o grupo de storage que deseja renomear.
2. Selecione **Gerenciar grupos › Renomear storage array group**.
3. No campo **Nome do grupo**, digite um novo nome para o grupo.
4. Clique em **Renomear.**

# Atualizações

## Visão geral do Centro de atualizações

No Centro de Atualização, você pode gerenciar atualizações de software SANtricity os e NVSRAM para vários storages de armazenamento.

### Como funcionam as atualizações?

Transfira o software SO mais recente e, em seguida, atualize um ou mais arrays.

#### Atualizar fluxo de trabalho

As etapas a seguir fornecem um fluxo de trabalho de alto nível para a realização de atualizações de software.

1. Você faz o download do arquivo de software mais recente do SANtricity os no site de suporte (um link está disponível no Unified Manager na página suporte). Salve o arquivo no sistema host de gerenciamento (o host onde você acessa o Unified Manager em um navegador) e, em seguida, descompacte o arquivo.
2. No Gerenciador Unificado, você carrega o arquivo de software do SANtricity os e o arquivo NVSRAM no repositório (uma área do servidor proxy de serviços da Web onde os arquivos são armazenados). Pode adicionar ficheiros a partir do **Centro de Atualização › Atualizar software SANtricity os ou a partir do Centro de Atualização › gerir repositório de software**.
3. Depois que os arquivos são carregados no repositório, você pode selecionar o arquivo a ser usado na atualização. Na página Atualizar o software SANtricity os (**Centro de atualização › Atualizar software SANtricity os**), selecione o ficheiro de software SANtricity os e o ficheiro NVSRAM. Depois de selecionar um ficheiro de software, é apresentada nesta página uma lista de matrizes de armazenamento compatíveis. Em seguida, selecione as matrizes de armazenamento que pretende atualizar com o novo software. (Não é possível selecionar matrizes incompatíveis.)
4. Em seguida, você pode iniciar uma transferência e ativação imediata de software, ou você pode optar por preparar os arquivos para ativação posteriormente. Durante o processo de atualização, o Unified Manager executa as seguintes tarefas:
    a. Executa uma verificação de integridade nos storage arrays para determinar se existem condições que

possam impedir a conclusão da atualização. Se algum array falhar na verificação de integridade, você pode pular esse array específico e continuar a atualização para os outros, ou você pode parar todo o processo e solucionar problemas dos arrays que não passaram.

b. Transfere os arquivos de atualização para cada controlador.

c. Reinicializa os controladores e ativa o novo software SANtricity os, um controlador de cada vez. Durante a ativação, o arquivo SANtricity os existente é substituído pelo novo arquivo.

> Você também pode especificar que o software está ativado posteriormente.

#### Atualização imediata ou faseada

Você pode ativar a atualização imediatamente ou colocá-la em fase posterior. Você pode optar por ativar mais tarde por estes motivos:

- **Hora do dia** — a ativação do software pode demorar muito tempo, então você pode querer esperar até que as cargas de e/S sejam mais leves. Dependendo da carga de e/S e do tamanho do cache, uma atualização da controladora normalmente pode levar entre 15 a 25 minutos para ser concluída. Os controladores reiniciam e fazem failover durante a ativação para que o desempenho possa ser menor do que o normal até que a atualização seja concluída.
- * Tipo de pacote* — você pode querer testar o novo software e firmware em uma matriz de armazenamento antes de atualizar os arquivos em outras matrizes de armazenamento.

Para ativar o software em estágio, vá para o **suporte › Centro de atualização** e clique em **Ativar** na área rotulada SANtricity os Controller Software upgrade.

#### Verificação de integridade

Uma verificação de integridade é executada como parte do processo de atualização, mas você também pode executar uma verificação de integridade separadamente antes de começar (vá para o **Centro de Atualização › Verificação de integridade pré-atualização**).

A verificação de integridade avalia todos os componentes do sistema de storage para garantir que a atualização possa prosseguir. As seguintes condições podem impedir a atualização:

- Unidades atribuídas com falha
- Peças sobressalentes quentes em uso
- Grupos de volumes incompletos
- Operações exclusivas em execução
- Volumes em falta
- Controlador em estado não ótimo
- Número excessivo de eventos de log
- Falha na validação da base de dados de configuração
- Unidades com versões antigas do DACstore

### O que eu preciso saber antes de atualizar?

Antes de atualizar vários storages de armazenamento, revise as principais considerações como parte do Planejamento.

#### Versões atuais

Você pode exibir as versões atuais do software SANtricity os na página Gerenciar do Gerenciador Unificado para cada storage array descoberto. A versão é mostrada na coluna Software do SANtricity os. As informações de firmware e NVSRAM da controladora estão disponíveis em uma caixa de diálogo pop-up quando você clica na versão do SANtricity os em cada linha.

#### Outros componentes que exigem atualização

Como parte do processo de atualização, você também pode precisar atualizar o driver multipath/failover do host ou o driver HBA para que o host possa interagir com os controladores corretamente.

Para obter informações sobre compatibilidade, consulte o "Matriz de interoperabilidade do NetApp". Consulte também os procedimentos nos Guias expressos do seu sistema operativo. Os guias expressos estão disponíveis no "Documentação do e-Series e do SANtricity".

#### Controladores duplos

Se um storage array contiver dois controladores e você tiver um driver multipath instalado, o storage array poderá continuar processando e/S durante a atualização. Durante a atualização, ocorre o seguinte processo:

1. O controlador A faz failover de todos os LUNs para o controlador B.
2. A atualização ocorre no controlador A..
3. O controlador A recupera os LUNs e todos os LUNs do controlador B.
4. A atualização ocorre no controlador B.

Após a conclusão da atualização, talvez seja necessário redistribuir manualmente os volumes entre as controladoras para garantir que os volumes voltem para a controladora proprietária correta.

## Atualizar software e firmware

#### Execute a verificação de integridade pré-atualização

Uma verificação de integridade é executada como parte do processo de atualização, mas você também pode executar uma verificação de integridade separadamente antes de começar. A verificação de integridade avalia os componentes do storage array para garantir que a atualização possa prosseguir.

#### Passos

1. Na visualização principal, selecione **Manage** e, em seguida, selecione menu:Upgrade Center [Pre-Upgrade Health Check] (Verificação de integridade pré-atualização).

   A caixa de diálogo Verificação do estado de pré-atualização abre-se e lista todos os sistemas de armazenamento descobertos.

2. Se necessário, filtre ou classifique os sistemas de storage na lista para que você possa visualizar todos os sistemas que não estão no estado ideal atualmente.
3. Marque as caixas de seleção dos sistemas de armazenamento que você deseja executar na verificação de integridade.
4. Clique em **Iniciar**.

   O progresso é mostrado na caixa de diálogo enquanto a verificação de integridade é executada.

5. Quando a verificação de integridade for concluída, você pode clicar nas elipses (…) à direita de cada linha para exibir mais informações e executar outras tarefas.

> Se algum array falhar na verificação de integridade, você pode pular esse array específico e continuar a atualização para os outros, ou você pode parar todo o processo e solucionar problemas dos arrays que não passaram.

### Atualize o SANtricity os

Atualize um ou mais storages de armazenamento com o software mais recente e NVSRAM para garantir que você tenha todos os recursos e correções de bugs mais recentes. A NVSRAM da controladora é um arquivo de controladora que especifica as configurações padrão para os controladores.

#### Antes de começar

- Os arquivos mais recentes do SANtricity os estão disponíveis no sistema host em que o proxy de serviços da Web do SANtricity e o Gerenciador Unificado estão em execução.
- Você sabe se deseja ativar a atualização de software agora ou mais tarde.

  Você pode optar por ativar mais tarde por estes motivos:

  - **Hora do dia** — a ativação do software pode demorar muito tempo, então você pode querer esperar até que as cargas de e/S sejam mais leves. Os controladores fazem failover durante a ativação, portanto, o desempenho pode ser menor do que o normal até que a atualização seja concluída.
  - * Tipo de pacote* — você pode querer testar o novo software do sistema operacional em uma matriz de armazenamento antes de atualizar os arquivos em outras matrizes de armazenamento.

> Os sistemas devem estar executando o SANtricity os 11.70.5 para atualizar para 11,80.x ou posterior.

#### Sobre esta tarefa

Mais uma vez

> Risco de perda de dados ou risco de danos à matriz de armazenamento - não faça alterações na matriz de armazenamento enquanto a atualização estiver ocorrendo. Mantenha o poder do storage array.

#### Passos

1. Se o storage array contiver apenas uma controladora ou um driver multipath não estiver em uso, interrompa a atividade de e/S no storage array para evitar erros de aplicativos. Se o seu storage array tiver duas controladoras e você tiver um driver multipath instalado, não será necessário interromper a atividade de e/S.
2. Na exibição principal, selecione **Gerenciar** e, em seguida, selecione um ou mais storages que você deseja atualizar.
3. Selecione **Centro de Atualização › Atualizar software SANtricity os**.

   A página Atualizar software SANtricity os é exibida.

4. Transfira o mais recente pacote de software do SANtricity os a partir do site de suporte da NetApp para a

sua máquina local.

a. Clique em **Adicionar novo arquivo ao repositório de software**.
b. Clique no link para encontrar os mais recentes **Downloads do SANtricity os**.
c. Clique no link **Download Latest Release**.
d. Siga as instruções restantes para transferir o ficheiro SANtricity os e o ficheiro NVSRAM para a sua máquina local.

> O firmware assinado digitalmente é necessário na versão 8,42 e superior. Se tentar transferir firmware não assinado, é apresentado um erro e a transferência é cancelada.

5. Selecione o arquivo de software do sistema operacional e o arquivo NVSRAM que você deseja usar para atualizar os controladores:

a. Na lista suspensa **Selecione um arquivo de software do SANtricity os**, selecione o arquivo do sistema operacional que você baixou para sua máquina local.

   Se houver vários arquivos disponíveis, os arquivos serão classificados da data mais recente para a data mais antiga.

> O repositório de software lista todos os arquivos de software associados ao Web Services Proxy. Se você não vir o arquivo que deseja usar, clique no link **Adicionar novo arquivo ao repositório de software**, para navegar até o local onde reside o arquivo do sistema operacional que você deseja adicionar.

a. Na lista suspensa **Selecione um arquivo NVSRAM**, selecione o arquivo do controlador que deseja usar.

   Se houver vários arquivos, os arquivos serão classificados da data mais recente para a data mais antiga.

6. Na tabela Matriz de armazenamento compatível, reveja os storages de armazenamento compatíveis com o arquivo de software do sistema operacional selecionado e selecione os storages que você deseja atualizar.
   - As matrizes de armazenamento selecionadas na vista gerir e compatíveis com o ficheiro de firmware selecionado são selecionadas por predefinição na tabela Matriz de armazenamento compatível.
   - As matrizes de armazenamento que não podem ser atualizadas com o ficheiro de firmware selecionado não são selecionáveis na tabela Matriz de armazenamento compatível, conforme indicado pelo estado **incompatível**.
7. **Opcional:** para transferir o arquivo de software para os storages de armazenamento sem ativá-los, marque a caixa de seleção **Transfira o software do sistema operacional para os storages, marque-o como encenado e ative posteriormente**.
8. Clique em **Iniciar**.
9. Dependendo se você escolheu ativar agora ou mais tarde, execute um dos seguintes procedimentos:
   - Digite **TRANSFER** para confirmar que deseja transferir as versões propostas de software do sistema operacional nos arrays que você selecionou para atualizar e clique em **Transferir**.

     Para ativar o software transferido, selecione **Centro de Atualização › Activate Staged os Software**.

   - Digite **UPGRADE** para confirmar que deseja transferir e ativar as versões propostas de software do

sistema operacional nos arrays que você selecionou para atualizar e clique em **Upgrade**.

O sistema transfere o ficheiro de software para cada matriz de armazenamento selecionada para atualizar e, em seguida, ativa esse ficheiro iniciando uma reinicialização.

As seguintes ações ocorrem durante a operação de atualização:

- Uma verificação de integridade de pré-atualização é executada como parte do processo de atualização. A verificação de integridade da pré-atualização avalia todos os componentes do storage array para garantir que a atualização possa prosseguir.
- Se qualquer verificação de integridade falhar em um storage array, a atualização será interrompida. Você pode clicar nas reticências (…) e selecionar **Salvar Registro** para revisar os erros. Você também pode optar por substituir o erro de verificação de integridade e clicar em **continuar** para continuar com a atualização.
- Você pode cancelar a operação de atualização após a verificação de integridade da pré-atualização.

10. **Opcional:** uma vez concluída a atualização, você pode ver uma lista do que foi atualizado para uma matriz de armazenamento específica clicando nas reticências (…) e selecionando **Salvar Log**.

    O arquivo é salvo na pasta Downloads do navegador com o nome `upgrade_log-<date>.json`.

### Ativar o software SO faseado

Você pode optar por ativar o arquivo de software imediatamente ou esperar até um momento mais conveniente. Este procedimento pressupõe que optou por ativar o ficheiro de software posteriormente.

#### Sobre esta tarefa

Você pode transferir os arquivos de firmware sem ativá-los. Você pode optar por ativar mais tarde por estes motivos:

- **Hora do dia** — a ativação do software pode demorar muito tempo, então você pode querer esperar até que as cargas de e/S sejam mais leves. Os controladores reiniciam e fazem failover durante a ativação para que o desempenho possa ser menor do que o normal até que a atualização seja concluída.
- * Tipo de pacote* — você pode querer testar o novo software e firmware em uma matriz de armazenamento antes de atualizar os arquivos em outras matrizes de armazenamento.

> Não é possível parar o processo de ativação depois de iniciado.

#### Passos

1. Na vista principal, selecione **Manage** (gerir). Se necessário, clique na coluna Status para classificar, na parte superior da página, todos os storages de armazenamento com o status "Atualização do sistema operacional (aguardando ativação)".
2. Selecione uma ou mais matrizes de armazenamento para as quais pretende ativar o software e, em seguida, selecione o **Centro de Atualização › Ativar software de SO faseado**.

   As seguintes ações ocorrem durante a operação de atualização:

   - Uma verificação de integridade pré-atualização é executada como parte do processo de ativação. A verificação de integridade da pré-atualização avalia todos os componentes do storage array para garantir que a ativação possa continuar.

- Se qualquer verificação de integridade falhar em um storage array, a ativação será interrompida. Você pode clicar nas reticências (…) e selecionar **Salvar Registro** para revisar os erros. Você também pode optar por substituir o erro de verificação de integridade e clicar em **continuar** para continuar com a ativação.
- Pode cancelar a operação de ativação após a verificação do estado de pré-atualização. Após a conclusão bem-sucedida da verificação de integridade da pré-atualização, ocorre a ativação. O tempo de ativação depende da configuração do storage array e dos componentes que você está ativando.

3. **Opcional:** após a conclusão da ativação, você pode ver uma lista do que foi ativado para uma matriz de armazenamento específica clicando nas reticências (…) e selecionando **Salvar Log**.

   O arquivo é salvo na pasta Downloads do navegador com o nome `activate_log-<date>.json`.

### Gerenciar o repositório de software

## O repositório de software lista todos os arquivos de software associados ao Web Services Proxy.

Se você não vir o arquivo que deseja usar, use a opção Gerenciar Repositório de software para importar um ou mais arquivos do SANtricity os para o sistema host onde o Proxy de serviços da Web e o Gerenciador Unificado estão sendo executados. Você também pode optar por excluir um ou mais arquivos do SANtricity os disponíveis no repositório de software.

#### Antes de começar

Se você estiver adicionando arquivos do SANtricity os, verifique se os arquivos do sistema operacional estão disponíveis no sistema local.

#### Passos

1. No modo de exibição principal, selecione **Manage** e, em seguida, selecione **Centro de Atualização › Manage Software Repository**.

   A caixa de diálogo Gerenciar Repositório de Software é exibida.

2. Execute uma das seguintes ações:

| Opção | Faça isso |
|---|---|
| Importar | a. Clique em **Importar.**<br>b. Clique em **Procurar** e navegue até o local onde residem os arquivos do sistema operacional que você deseja adicionar.<br>Os arquivos DO SO têm um nome de arquivo semelhante `N2800-830000-000.dlp` ao .<br>c. Selecione um ou mais arquivos do sistema operacional que você deseja adicionar e clique em **Importar**. |
| Eliminar | a. Selecione um ou mais arquivos do SO que você deseja remover do repositório de software.<br>b. Clique em **Excluir**. |

#### Resultados

Se você selecionou importar, o(s) arquivo(s) será(ão) carregado(s) e validado(s). Se você selecionou excluir, os arquivos serão removidos do repositório de software.

#### Limpar o software de SO faseado

Você pode remover o software de sistema operacional em estágios para garantir que uma versão pendente não seja ativada inadvertidamente posteriormente. A remoção do software do SO em estágio não afeta a versão atual que está sendo executada nos storages de armazenamento.

#### Passos

1. Na visualização principal, selecione **Manage** e, em seguida, selecione **Centro de Atualização › Clear Staged os Software**.

   A caixa de diálogo Clear Staged os Software abre e lista todos os sistemas de armazenamento descobertos com software pendente ou NVSRAM.

2. Se necessário, filtre ou classifique os sistemas de storage na lista para que você possa visualizar todos os sistemas que tenham feito o software em estágios.
3. Marque as caixas de seleção dos sistemas de armazenamento com software pendente que você deseja desmarcar.
4. Clique em **Limpar**.

   O estado da operação é apresentado na caixa de diálogo.

# Espelhamento

## Visão geral do espelhamento

Use os recursos de espelhamento para replicar dados entre um storage array local e um storage array remoto, seja de forma assíncrona ou síncrona.

> O espelhamento síncrono não está disponível no sistema de storage EF600 ou EF300.

#### O que é espelhamento?

As aplicações SANtricity incluem dois tipos de espelhamento: Assíncrono e síncrono. O espelhamento assíncrono copia volumes de dados sob demanda ou de acordo com o cronograma, o que minimiza ou evita o tempo de inatividade que pode resultar de corrupção ou perda de dados. O espelhamento síncrono replica volumes de dados em tempo real para garantir disponibilidade contínua.

Saiba mais:

- "Como o espelhamento funciona"
- "Terminologia de espelhamento"

### Como faço para configurar o espelhamento?

Você configura o espelhamento assíncrono ou síncrono no Unified Manager e, em seguida, usa o System Manager para gerenciar sincronizações.

Saiba mais:

- "Fluxo de trabalho de configuração de espelhamento"
- "Requisitos para uso do espelhamento"
- "Crie um par espelhado assíncrono"
- "Crie par espelhado síncrono"

## Conceitos

### Como o espelhamento funciona

O Unified Manager inclui opções de configuração para os recursos de espelhamento do SANtricity, que permitem que os administradores repliquem dados entre dois storage arrays para proteção de dados.

O espelhamento síncrono não está disponível no sistema de storage EF600 ou EF300.

#### Tipos de espelhamento

As aplicações SANtricity incluem dois tipos de espelhamento: Assíncrono e síncrono.

O espelhamento assíncrono copia volumes de dados sob demanda ou de acordo com o cronograma, o que minimiza ou evita o tempo de inatividade que pode resultar de corrupção ou perda de dados. O espelhamento assíncrono captura o estado do volume primário em um determinado momento no tempo e copia apenas os dados que foram alterados desde a última captura de imagem. O site principal pode ser atualizado imediatamente e o site secundário pode ser atualizado como a largura de banda permite. As informações são armazenadas em cache e enviadas posteriormente, à medida que os recursos de rede ficam disponíveis. Esse tipo de espelhamento é ideal para processos periódicos, como backup e arquivamento.

O espelhamento síncrono replica volumes de dados em tempo real para garantir disponibilidade contínua. O objetivo é alcançar um objetivo de ponto de restauração (RPO) sem perda de dados ao ter uma cópia dos dados importantes disponível se um desastre ocorrer em um dos dois storage arrays. A cópia é idêntica aos dados de produção a cada momento, porque cada vez que uma gravação é feita no volume primário, uma gravação é feita no volume secundário. O host não recebe uma confirmação de que a gravação foi bem-sucedida até que o volume secundário seja atualizado com as alterações feitas no volume primário. Esse tipo de espelhamento é ideal para fins de continuidade dos negócios, como recuperação de desastres.

#### Diferenças entre tipos de espelhamento

A tabela a seguir descreve as principais diferenças entre os dois tipos de espelhamento.

| Atributo | Assíncrono | Síncrono |
| --- | --- | --- |
| Método de replicação | Point-in-time — o espelhamento é feito sob demanda ou automaticamente de acordo com uma programação definida pelo usuário. | Contínuo — o espelhamento é executado automaticamente continuamente, copiando dados de cada gravação de host. |
| Distância | Suporta longas distâncias entre arrays. Normalmente, a distância é limitada apenas pelas capacidades da rede e da tecnologia de extensão de canal. | Restrito a distâncias mais curtas entre arrays. Normalmente, a distância deve estar a cerca de 10 km (6,2 milhas) do storage array local para atender aos requisitos de latência e desempenho do aplicativo. |
| Método de comunicação | Uma rede IP ou Fibre Channel padrão. | Apenas rede Fibre Channel. |
| Tipos de volume | Padrão ou fino. | Apenas padrão. |

#### Fluxo de trabalho de configuração de espelhamento

Você configura o espelhamento assíncrono ou síncrono no Unified Manager e, em seguida, usa o System Manager para gerenciar sincronizações.

##### Fluxo de trabalho de espelhamento assíncrono

O espelhamento assíncrono envolve o seguinte fluxo de trabalho:

1. Execute a configuração inicial no Unified Manager:
   a. Selecione a matriz de armazenamento local como a origem para a transferência de dados.
   b. Crie ou selecione um grupo de consistência de espelho existente, que é um contentor para o volume primário no array local e o volume secundário no array remoto. Os volumes primário e secundário são referidos como o "par espelhado". Se você estiver criando o grupo de consistência de espelho pela primeira vez, especifique se deseja executar sincronizações manuais ou agendadas.
   c. Selecione um volume primário no storage array local e, em seguida, determine sua capacidade reservada. A capacidade reservada é a capacidade física alocada a ser usada para a operação de cópia.
   d. Selecione um storage array remoto como o destino da transferência, um volume secundário e, em seguida, determine sua capacidade reservada.
   e. Inicie a transferência de dados inicial do volume primário para o volume secundário. Dependendo do tamanho do volume, esta transferência inicial pode demorar várias horas.
2. Verifique o progresso da sincronização inicial:
   a. No Unified Manager, inicie o System Manager para o array local.
   b. No System Manager, visualize o status da operação de espelhamento. Quando o espelhamento estiver concluído, o status do par espelhado é "ótimo".

3. Opcionalmente, você pode reagendar ou realizar manualmente transferências de dados subsequentes no System Manager. Somente blocos novos e alterados são transferidos do volume primário para o volume secundário.

> Como a replicação assíncrona é periódica, o sistema pode consolidar os blocos alterados e conservar a largura de banda da rede. Há impacto mínimo na taxa de transferência de gravação e na latência de gravação.

#### Fluxo de trabalho de espelhamento síncrono

O espelhamento síncrono envolve o seguinte fluxo de trabalho:

1. Execute a configuração inicial no Unified Manager:
   a. Selecione uma matriz de armazenamento local como a origem para a transferência de dados.
   b. Selecione um volume primário no storage array local.
   c. Selecione uma matriz de armazenamento remota como destino para a transferência de dados e, em seguida, selecione um volume secundário.
   d. Selecione as prioridades de sincronização e ressincronização.
   e. Inicie a transferência de dados inicial do volume primário para o volume secundário. Dependendo do tamanho do volume, esta transferência inicial pode demorar várias horas.
2. Verifique o progresso da sincronização inicial:
   a. No Unified Manager, inicie o System Manager para o array local.
   b. No System Manager, visualize o status da operação de espelhamento. Quando o espelhamento estiver concluído, o status do par espelhado é "ótimo". Os dois arrays tentam permanecer sincronizados através de operações normais. Somente blocos novos e alterados são transferidos do volume primário para o volume secundário.
3. Opcionalmente, você pode alterar as configurações de sincronização no System Manager.

> Como a replicação síncrona é contínua, o link de replicação entre os dois locais precisa fornecer recursos de largura de banda suficientes.

### Terminologia de espelhamento

Saiba como os termos de espelhamento se aplicam ao storage array.

| Prazo | Descrição |
|---|---|
| Storage array local | O storage array local é o storage array em que você está agindo. |
| Grupo de consistência do espelho | Um grupo de consistência de espelho é um recipiente para um ou mais pares espelhados. Para operações de espelhamento assíncrono, você precisa criar um grupo de consistência de espelhamento. Todos os pares espelhados em um grupo são ressincronizados simultaneamente, preservando assim um ponto de recuperação consistente.<br><br>O espelhamento síncrono não usa grupos de consistência de espelho. |

| Prazo | Descrição |
| --- | --- |
| Par espelhado | Um par espelhado é composto por dois volumes, um volume primário e um volume secundário.<br><br>No espelhamento assíncrono, um par espelhado sempre pertence a um grupo de consistência de espelho. As operações de gravação são executadas primeiro no volume primário e, em seguida, replicadas no volume secundário. Cada par espelhado em um grupo de consistência de espelho compartilha as mesmas configurações de sincronização. |
| Volume primário | O volume primário de um par espelhado é o volume de origem a ser espelhado. |
| Storage array remoto | O storage array remoto geralmente é designado como local secundário, que geralmente contém uma réplica dos dados em uma configuração de espelhamento. |
| Capacidade reservada | A capacidade reservada é a capacidade alocada física usada para qualquer operação de serviço de cópia e objeto de storage. Não é diretamente legível pelo host.<br><br>Esses volumes são necessários para que o controlador possa salvar persistentemente as informações necessárias para manter o espelhamento em um estado operacional. Eles contêm informações como Registros delta e dados copy-on-write. |
| Volume secundário | O volume secundário de um par espelhado geralmente está localizado em um local secundário e contém uma réplica dos dados. |
| Sincronização | A sincronização ocorre na sincronização inicial entre o storage array local e o storage array remoto. A sincronização também ocorre quando os volumes primário e secundário ficam não sincronizados após uma interrupção da comunicação. Quando o link de comunicação está funcionando novamente, todos os dados não replicados são sincronizados com o storage array do volume secundário. |

### Requisitos para uso do espelhamento

Se você planeja configurar o espelhamento, tenha em mente os seguintes requisitos.

#### Unified Manager

- O serviço Web Services Proxy deve estar em execução.
- O Unified Manager deve estar em execução em seu host local por meio de uma conexão HTTPS.
- O Unified Manager deve mostrar certificados SSL válidos para a matriz de armazenamento. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando o Unified Manager e navegando para o **certificado › Gerenciamento de certificados**.

#### Storage arrays

O espelhamento síncrono não está disponível no storage array EF600 ou EF300.

- Você precisa ter dois storage arrays.
- Cada storage array deve ter duas controladoras.
- Os dois storage arrays devem ser descobertos no Unified Manager.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conetado à rede.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)
- Você deve saber a senha para os storages de armazenamento local e remoto.
- Você precisa ter capacidade livre suficiente no storage array remoto para criar um volume secundário igual ou maior que o volume principal que deseja espelhar.
- O espelhamento assíncrono é compatível com controladoras com portas de host Fibre Channel (FC) ou iSCSI, enquanto o espelhamento síncrono é compatível somente com controladoras com portas de host FC.

#### Requisitos de conetividade

O espelhamento por meio de uma interface FC (assíncrona ou síncrona) requer o seguinte:

- Cada controladora do storage array dedica sua porta de host FC de maior número às operações de espelhamento.
- Se o controlador tiver portas FC de base e portas FC da placa de interface do host (HIC), a porta numerada mais alta estará em um HIC. Qualquer host conetado à porta dedicada é desconetado e nenhuma solicitação de login do host é aceita. As solicitações de e/S nessa porta são aceitas somente de controladores que participam de operações de espelhamento.
- As portas de espelhamento dedicadas devem ser conectadas a um ambiente de malha FC que suporte as interfaces do serviço de diretório e serviço de nomes. Em particular, FC-AL e ponto a ponto não são compatíveis como opções de conectividade entre as controladoras que estão participando de relacionamentos espelhados.

O espelhamento através de uma interface iSCSI (apenas assíncrona) requer o seguinte:

- Ao contrário do FC, o iSCSI não requer uma porta dedicada. Quando o espelhamento assíncrono é usado em ambientes iSCSI, não é necessário dedicar nenhuma das portas iSCSI de front-end do storage array para uso com espelhamento assíncrono. Essas portas são compartilhadas para tráfego de espelhamento assíncrono e conexões de e/S de host para array.
- O controlador mantém uma lista de sistemas de armazenamento remoto com os quais o iniciador iSCSI tenta estabelecer uma sessão. A primeira porta que estabelece com êxito uma conexão iSCSI é usada para toda a comunicação subsequente com esse storage de armazenamento remoto. Se a comunicação falhar, uma nova sessão é tentada usando todas as portas disponíveis.
- As portas iSCSI são configuradas no nível da matriz, porta a porta. A comunicação entre controladores para mensagens de configuração e transferência de dados usa as configurações globais, incluindo configurações para:
  - VLAN: Os sistemas locais e remotos devem ter a mesma configuração de VLAN para se comunicar
  - Porta de escuta iSCSI

- Jumbo Frames
- Prioridade Ethernet

> A comunicação do intercontrolador iSCSI deve usar uma porta de conexão de host e não a porta Ethernet de gerenciamento.

#### Candidatos a volume espelhado

- O nível RAID, os parâmetros de armazenamento em cache e o tamanho do segmento podem ser diferentes nos volumes primário e secundário de um par espelhado.

> Para controladores EF600 e EF300, os volumes primário e secundário de um par espelhado assíncrono devem corresponder ao mesmo protocolo, nível da bandeja, tamanho do segmento, tipo de segurança e nível RAID. Pares espelhados assíncronos não elegíveis não aparecerão na lista de volumes disponíveis.

- O volume secundário deve ser pelo menos tão grande quanto o volume primário.
- Um volume pode participar de apenas um relacionamento de espelho.
- Para um par espelhado síncrono, os volumes primário e secundário devem ser volumes padrão. Não podem ser volumes finos ou volumes instantâneos.
- Para o espelhamento síncrono, há limites para o número de volumes compatíveis com um determinado storage array. Certifique-se de que o número de volumes configurados na matriz de armazenamento seja inferior ao limite suportado. Quando o espelhamento síncrono está ativo, os dois volumes de capacidade reservada criados contam para o limite de volume.
- Para o espelhamento assíncrono, o volume primário e o volume secundário devem ter os mesmos recursos de Segurança da Unidade.
  - Se o volume primário for compatível com FIPS, o volume secundário deve ser capaz de FIPS.
  - Se o volume principal for compatível com FDE, o volume secundário tem de ser capaz de FDE.
  - Se o volume principal não estiver usando o Drive Security, o volume secundário não deve estar usando o Drive Security.

#### Capacidade reservada

Espelhamento assíncrono:

- Um volume de capacidade reservada é necessário para um volume primário e para um volume secundário em um par espelhado para Registrar informações de gravação para recuperar de reinicializações do controlador e outras interrupções temporárias.
- Como o volume principal e o volume secundário em um par espelhado exigem capacidade reservada adicional, você precisa garantir que tenha capacidade livre disponível em ambos os storage arrays na relação espelhada.

Espelhamento síncrono:

- A capacidade reservada é necessária para um volume primário e para um volume secundário para registar informações de gravação para recuperar de reinicializações do controlador e outras interrupções temporárias.
- Os volumes de capacidade reservada são criados automaticamente quando o espelhamento síncrono é ativado. Como o volume principal e o volume secundário em um par espelhado exigem capacidade

reservada, você precisa garantir que tenha capacidade livre suficiente disponível em ambos os storage arrays que participam do relacionamento de espelhamento síncrono.

#### Recurso de segurança da unidade

- Se você estiver usando unidades com capacidade de segurança, o volume primário e o volume secundário devem ter configurações de segurança compatíveis. Esta restrição não é imposta; portanto, você deve verificá-la por conta própria.
- Se você estiver usando unidades com capacidade segura, o volume primário e o volume secundário deverão usar o mesmo tipo de unidade. Esta restrição não é imposta; portanto, você deve verificá-la por conta própria.
- Se estiver a utilizar o Data Assurance (DA), o volume primário e o volume secundário têm de ter as mesmas definições DE DA.

## Configurar o espelhamento

### Crie um par espelhado assíncrono

Para configurar o espelhamento assíncrono, você cria um par espelhado que inclui um volume primário no array local e um volume secundário no array remoto.

#### Antes de começar

Antes de criar um par espelhado, atenda aos seguintes requisitos do Unified Manager:

- O serviço Web Services Proxy deve estar em execução.
- O Unified Manager deve estar em execução em seu host local por meio de uma conexão HTTPS.
- O Unified Manager deve mostrar certificados SSL válidos para a matriz de armazenamento. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando o Unified Manager e navegando para o **certificado › Gerenciamento de certificados**.

Certifique-se também de atender aos seguintes requisitos para storage arrays e volumes:

- Cada storage array deve ter duas controladoras.
- Os dois storage arrays devem ser descobertos no Unified Manager.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conetado à rede.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)
- Você deve saber a senha para os storages de armazenamento local e remoto.
- Você precisa ter capacidade livre suficiente no storage array remoto para criar um volume secundário igual ou maior que o volume principal que deseja espelhar.
- Seus storage arrays locais e remotos são conectados por meio de uma malha Fibre Channel ou de uma interface iSCSI.
- Você criou os volumes primário e secundário que deseja usar na relação de espelhamento assíncrono.
- O volume secundário deve ser pelo menos tão grande quanto o volume primário.

#### Sobre esta tarefa

O processo para criar um par espelhado assíncrono é um procedimento de várias etapas.

#### Passo 1: Crie ou selecione um grupo de consistência de espelho

Nesta etapa, você cria um novo grupo de consistência de espelho ou seleciona um existente. Um grupo de consistência de espelho é um contentor para os volumes primário e secundário (o par espelhado) e especifica o método de ressincronização desejado (manual ou automático) para todos os pares no grupo.

**Passos**

1. Na página **Gerenciar**, selecione a matriz de armazenamento local que você deseja usar para a origem.
2. Selecione **ações › Create Asynchronous Mirrored Pair** (criar par espelhado assíncrono).

   O assistente criar par espelhado assíncrono é aberto.

3. Selecione um grupo de consistência de espelho existente ou crie um novo.

   Para selecionar um grupo existente, certifique-se de que **um grupo de consistência de espelho existente** está selecionado e selecione o grupo na tabela. Um grupo de consistência pode incluir vários pares espelhados.

   Para criar um novo grupo, faça o seguinte:

   a. Selecione **Um novo grupo de consistência de espelho** e, em seguida, clique em **seguinte**.
   b. Insira um nome exclusivo que melhor descreva os dados nos volumes que serão espelhados entre os dois arrays de armazenamento. Um nome só pode consistir em letras, números e os carateres especiais sublinhado (_), traço (-) e sinal de hash ( no). Um nome não pode exceder 30 carateres e não pode conter espaços.
   c. Selecione a matriz de armazenamento remoto na qual você deseja estabelecer uma relação de espelhamento com a matriz de armazenamento local.

      Se a matriz de armazenamento remota estiver protegida por palavra-passe, o sistema solicitará uma palavra-passe.

   d. Escolha se deseja sincronizar os pares espelhados manualmente ou automaticamente:
      - **Manual** — Selecione essa opção para iniciar manualmente a sincronização de todos os pares espelhados nesse grupo. Observe que quando você deseja executar uma ressincronização mais tarde, você deve iniciar o System Manager para o storage array primário e, em seguida, ir para **armazenamento › Espelhamento assíncrono**, selecione o grupo na guia **Espelhar grupos** e selecione **mais › manualmente ressincronizar**.
      - **Automático** — Selecione o intervalo desejado em **minutos**, **horas** ou **dias**, desde o início da atualização anterior até o início da próxima atualização. Por exemplo, se o intervalo de sincronização for definido em 30 minutos e o processo de sincronização começar às 4:00 horas, o próximo processo será iniciado às 4:30 horas
   e. Selecione as definições de alerta pretendidas:
      - Para sincronizações manuais, especifique o limite (definido pela porcentagem da capacidade restante) para quando receber alertas.
      - Para sincronizações automáticas, você pode definir três métodos de alerta: Quando a sincronização não tiver sido concluída em um período específico de tempo, quando os dados do ponto de recuperação no array remoto forem mais antigos que um limite de tempo específico e quando a capacidade reservada estiver próxima a um limite específico (definido pela porcentagem da capacidade restante).
4. Selecione **seguinte** e vá para Passo 2: Selecione o volume principal.

Se você definiu um novo grupo de consistência de espelho, o Unified Manager criará primeiro o grupo de consistência de espelho no storage array local e, em seguida, criará o grupo de consistência de espelho no storage array remoto. Você pode visualizar e gerenciar o grupo de consistência de espelho iniciando o System Manager para cada array.

> Se o Unified Manager criar com êxito o grupo de consistência de espelho no storage array local, mas não conseguir criá-lo no storage array remoto, ele excluirá automaticamente o grupo de consistência de espelho do storage array local. Se ocorrer um erro enquanto o Unified Manager estiver tentando excluir o grupo de consistência de espelho, você deverá excluí-lo manualmente.

#### Passo 2: Selecione o volume principal

Nesta etapa, você seleciona o volume principal a ser usado na relação de espelhamento e aloca capacidade reservada. Quando você seleciona um volume primário no storage array local, o sistema exibe uma lista de todos os volumes elegíveis para esse par espelhado. Quaisquer volumes que não sejam elegíveis para serem usados não são exibidos nessa lista.

Todos os volumes adicionados ao grupo de consistência de espelho no storage array local terão a função principal na relação de espelhamento.

**Passos**

1. Na lista de volumes elegíveis, selecione um volume que pretende utilizar como volume principal e, em seguida, clique em **seguinte** para atribuir a capacidade reservada.
2. Na lista de candidatos elegíveis, selecione capacidade reservada para o volume primário.

   Tenha em mente as seguintes diretrizes:

   - A configuração padrão para capacidade reservada é de 20% da capacidade do volume base e, geralmente, essa capacidade é suficiente. Se você alterar a porcentagem, clique em **Atualizar candidatos**.
   - A capacidade necessária varia, dependendo da frequência e do tamanho das gravações de e/S no volume principal e por quanto tempo você precisa manter a capacidade.
   - Em geral, escolha uma capacidade maior para a capacidade reservada se uma ou ambas as condições existirem:
     - Você pretende manter o par espelhado por um longo período de tempo.
     - Uma grande porcentagem de blocos de dados mudará no volume primário devido à intensa atividade de e/S. Use dados históricos de desempenho ou outros utilitários do sistema operacional para ajudá-lo a determinar a atividade típica de e/S para o volume principal.
3. Selecione **seguinte** e vá para Passo 3: Selecione o volume secundário.

#### Passo 3: Selecione o volume secundário

Nesta etapa, você seleciona o volume secundário a ser usado na relação de espelhamento e aloca sua capacidade reservada. Quando você seleciona um volume secundário no storage array remoto, o sistema exibe uma lista de todos os volumes elegíveis para esse par espelhado. Quaisquer volumes que não sejam elegíveis para serem usados não são exibidos nessa lista.

Todos os volumes adicionados ao grupo de consistência de espelho no storage array de armazenamento remoto terão a função secundária na relação de espelhamento.

**Passos**

1. Na lista de volumes elegíveis, selecione um volume que você deseja usar como volume secundário no par espelhado e clique em **Next** para alocar a capacidade reservada.
2. Na lista de candidatos elegíveis, selecione capacidade reservada para o volume secundário.

   Tenha em mente as seguintes diretrizes:

   - A configuração padrão para capacidade reservada é de 20% da capacidade do volume base e, geralmente, essa capacidade é suficiente. Se você alterar a porcentagem, clique em **Atualizar candidatos**.
   - A capacidade necessária varia, dependendo da frequência e do tamanho das gravações de e/S no volume principal e por quanto tempo você precisa manter a capacidade.
   - Em geral, escolha uma capacidade maior para a capacidade reservada se uma ou ambas as condições existirem:
     - Você pretende manter o par espelhado por um longo período de tempo.
     - Uma grande porcentagem de blocos de dados mudará no volume primário devido à intensa atividade de e/S. Use dados históricos de desempenho ou outros utilitários do sistema operacional para ajudá-lo a determinar a atividade típica de e/S para o volume principal.
3. Selecione **Finish** para concluir a sequência de espelhamento assíncrono.

**Resultados**

O Unified Manager realiza as seguintes ações:

- Inicia a sincronização inicial entre a matriz de armazenamento local e a matriz de armazenamento remoto.
- Cria a capacidade reservada para o par espelhado no storage array local e no storage array remoto.

> Se o volume espelhado for um volume fino, apenas os blocos provisionados (capacidade alocada em vez de capacidade reportada) serão transferidos para o volume secundário durante a sincronização inicial. Isso reduz a quantidade de dados que devem ser transferidos para concluir a sincronização inicial.

### Crie par espelhado síncrono

Para configurar o espelhamento síncrono, você cria um par espelhado que inclui um volume primário no array local e um volume secundário no array remoto.

> Este recurso não está disponível no sistema de armazenamento EF600 ou EF300.

**Antes de começar**

Antes de criar um par espelhado, atenda aos seguintes requisitos do Unified Manager:

- O serviço Web Services Proxy deve estar em execução.
- O Unified Manager deve estar em execução em seu host local por meio de uma conexão HTTPS.
- O Unified Manager deve mostrar certificados SSL válidos para a matriz de armazenamento. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando o Unified Manager e navegando para o **certificado › Gerenciamento de certificados**.

Certifique-se também de atender aos seguintes requisitos para storage arrays e volumes:

- Os dois storage arrays que você planeja usar para espelhamento são descobertos no Unified Manager.
- Cada storage array deve ter duas controladoras.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conetado à rede.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)
- Você deve saber a senha para os storages de armazenamento local e remoto.
- Seus storage arrays locais e remotos são conectados por meio de uma malha Fibre Channel.
- Você criou os volumes primário e secundário que deseja usar na relação de espelhamento síncrono.
- O volume primário deve ser um volume padrão. Não pode ser um volume fino ou um volume instantâneo.
- O volume secundário deve ser um volume padrão. Não pode ser um volume fino ou um volume instantâneo.
- O volume secundário deve ser pelo menos tão grande quanto o volume primário.

**Sobre esta tarefa**

O processo para criar pares espelhados síncronos é um procedimento de várias etapas.

#### Passo 1: Selecione o volume principal

Nesta etapa, você seleciona o volume primário a ser usado na relação de espelhamento síncrono. Quando você seleciona um volume primário no storage array local, o sistema exibe uma lista de todos os volumes elegíveis para esse par espelhado. Quaisquer volumes que não sejam elegíveis para serem usados não são exibidos nessa lista. O volume selecionado mantém a função principal na relação de espelhamento.

**Passos**

1. Na página **Gerenciar**, selecione a matriz de armazenamento local que você deseja usar para a origem.
2. Selecione **ações › Create Synchronous Mirrored Pair** (criar par espelhado síncrono).

   O assistente criar par espelhado síncrono é aberto.

3. Na lista de volumes elegíveis, selecione um volume que você deseja usar como o volume principal no espelho.
4. Selecione **seguinte** e vá para Passo 2: Selecione o volume secundário.

#### Passo 2: Selecione o volume secundário

Nesta etapa, você seleciona o volume secundário a ser usado na relação de espelhamento. Quando você seleciona um volume secundário no storage array remoto, o sistema exibe uma lista de todos os volumes elegíveis para esse par espelhado. Quaisquer volumes que não sejam elegíveis para serem usados não são exibidos nessa lista. O volume selecionado manterá a função secundária na relação de espelho.

**Passos**

1. Selecione a matriz de armazenamento remoto na qual você deseja estabelecer uma relação de espelhamento com a matriz de armazenamento local.

   Se a matriz de armazenamento remota estiver protegida por palavra-passe, o sistema solicitará uma palavra-passe.

- Os storage arrays são listados pelo nome do storage array. Se você não nomeou um storage array, ele será listado como "sem nome".
- Se o storage array que você deseja usar não estiver na lista, verifique se ele foi descoberto no Unified Manager.

2. Na lista de volumes elegíveis, selecione um volume que pretende utilizar como volume secundário no espelho.

> Se um volume secundário for escolhido com uma capacidade maior que o volume primário, a capacidade utilizável será restrita ao tamanho do volume primário.

3. Clique em **seguinte** e vá para Passo 3: Selecione as configurações de sincronização.

#### Passo 3: Selecione as configurações de sincronização

Nesta etapa, você seleciona as configurações que determinam como os dados são sincronizados após uma interrupção de comunicação. Você pode definir a prioridade na qual o proprietário do controlador do volume primário ressincroniza os dados com o volume secundário após uma interrupção de comunicação. Você também deve selecionar a política de ressincronização, manual ou automática.

**Passos**

1. Utilize a barra deslizante para definir a prioridade de sincronização.

   A prioridade de sincronização determina quanto dos recursos do sistema são usados para concluir a sincronização inicial e a operação de ressincronização após uma interrupção de comunicação em comparação com as solicitações de e/S de serviço.

   A prioridade definida nesta caixa de diálogo aplica-se tanto ao volume primário como ao volume secundário. Você pode modificar a taxa no volume primário posteriormente acessando o System Manager e selecionando **armazenamento › Espelhamento síncrono › mais › Editar configurações**.

   Existem cinco taxas de prioridade de sincronização:

   - Mais baixo
   - Baixo
   - Média
   - Alta
   - Mais alto

     Se a prioridade de sincronização estiver definida para a taxa mais baixa, a atividade de e/S será priorizada e a operação de ressincronização demorará mais tempo. Se a prioridade de sincronização estiver definida para a taxa mais alta, a operação de ressincronização será priorizada, mas a atividade de e/S para o storage array pode ser afetada.

2. Escolha se deseja ressincronizar os pares espelhados na matriz de armazenamento remoto manualmente ou automaticamente.
   - **Manual** (a opção recomendada) — Selecione essa opção para exigir que a sincronização seja reiniciada manualmente após a comunicação ser restaurada para um par espelhado. Essa opção oferece a melhor oportunidade para recuperar dados.
   - **Automático** — Selecione esta opção para iniciar a ressincronização automaticamente após a comunicação ser restaurada para um par espelhado.

Para retomar manualmente a sincronização, vá para System Manager e selecione **armazenamento › Espelhamento síncrono**, realce o par espelhado na tabela e selecione **Resume** em **More**.

3. Clique em **Finish** para concluir a sequência de espelhamento síncrono.

**Resultados**

Quando o espelhamento é ativado, o sistema executa as seguintes ações:

- Inicia a sincronização inicial entre a matriz de armazenamento local e a matriz de armazenamento remoto.
- Define a prioridade de sincronização e a política de ressincronização.
- Reserva a porta com o número mais alto do HIC do controlador para transmissão de dados espelhados.

  As solicitações de e/S recebidas nesta porta são aceitas somente pelo proprietário do controlador preferido remoto do volume secundário no par espelhado. (São permitidas reservas no volume primário.)

- Cria dois volumes de capacidade reservados, um para cada controlador, que são usados para Registrar informações de gravação para recuperar de reinicializações do controlador e outras interrupções temporárias.

  A capacidade de cada volume é de 128 MIB. No entanto, se os volumes forem colocados em um pool, 4 GiB serão reservados para cada volume.

**Depois de terminar**

Vá para System Manager e selecione **Home › View Operations in Progress** (Visualizar operações em andamento) para ver o progresso da operação de espelhamento síncrono. Esta operação pode ser demorada e pode afetar o desempenho do sistema.

## FAQs

**O que eu preciso saber antes de criar um grupo de consistência de espelho?**

Siga estas diretrizes antes de criar um grupo de consistência espelhada.

Atender aos seguintes requisitos do Unified Manager:

- O serviço Web Services Proxy deve estar em execução.
- O Unified Manager deve estar em execução em seu host local por meio de uma conexão HTTPS.
- O Unified Manager deve mostrar certificados SSL válidos para a matriz de armazenamento. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando o Unified Manager e navegando para o **certificado › Gerenciamento de certificados**.

Certifique-se também de atender aos seguintes requisitos para matrizes de armazenamento:

- Os dois storage arrays devem ser descobertos no Unified Manager.
- Cada storage array deve ter duas controladoras.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conetado à rede.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)

- Você deve saber a senha para os storages de armazenamento local e remoto.
- Seus storage arrays locais e remotos são conectados por meio de uma malha Fibre Channel ou de uma interface iSCSI.

O espelhamento síncrono não está disponível no sistema de storage EF600 ou EF300.

**O que eu preciso saber antes de criar um par espelhado?**

Antes de criar um par espelhado, siga estas diretrizes.

- Você precisa ter dois storage arrays.
- Cada storage array deve ter duas controladoras.
- Os dois storage arrays devem ser descobertos no Unified Manager.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conetado à rede.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)
- Você deve saber a senha para os storages de armazenamento local e remoto.
- Você precisa ter capacidade livre suficiente no storage array remoto para criar um volume secundário igual ou maior que o volume principal que deseja espelhar.
- O espelhamento assíncrono é compatível com controladoras com portas de host Fibre Channel (FC) ou iSCSI, enquanto o espelhamento síncrono é compatível somente com controladoras com portas de host FC.

O espelhamento síncrono não está disponível no sistema de storage EF600 ou EF300.

**Por que eu alteraria essa porcentagem?**

A capacidade reservada costuma ser de 20% do volume base para operações de espelhamento assíncrono. Normalmente, essa capacidade é suficiente.

A capacidade necessária varia, dependendo da frequência e tamanho das gravações de e/S no volume base e quanto tempo você pretende usar a operação de serviço de cópia do objeto de armazenamento. Em geral, escolha uma porcentagem maior para a capacidade reservada se uma ou ambas as condições existirem:

- Se a vida útil de uma operação de serviço de cópia de um objeto de armazenamento específico será muito longa.
- Se uma grande porcentagem de blocos de dados mudar no volume base devido à intensa atividade de e/S. Use dados históricos de desempenho ou outros utilitários do sistema operacional para ajudá-lo a determinar a atividade típica de e/S para o volume base.

**Por que vejo mais de um candidato à capacidade reservada?**

Se houver mais de um volume em um pool ou grupo de volumes que atenda ao valor percentual de capacidade selecionado para o objeto de armazenamento, você verá vários candidatos.

Você pode atualizar a lista de candidatos recomendados alterando a porcentagem de espaço físico da

unidade que deseja reservar no volume base para operações de serviço de cópia. Os melhores candidatos são exibidos com base na sua seleção.

**Por que não vejo todos os meus volumes?**

Ao selecionar um volume primário para um par espelhado, uma lista mostra todos os volumes elegíveis.

Quaisquer volumes que não sejam elegíveis para serem usados não são exibidos nessa lista. Os volumes podem não ser elegíveis por qualquer um dos seguintes motivos:

- O volume não é ideal.
- O volume já está participando de uma relação de espelhamento.
- Para o espelhamento síncrono, os volumes primário e secundário em um par espelhado devem ser volumes padrão. Não podem ser volumes finos ou volumes instantâneos.
- Para o espelhamento assíncrono, os thin volumes devem ter a expansão automática ativada.

> Para controladores EF600 e EF300, os volumes primário e secundário de um par espelhado assíncrono devem corresponder ao mesmo protocolo, nível da bandeja, tamanho do segmento, tipo de segurança e nível RAID. Pares espelhados assíncronos não elegíveis não aparecerão na lista de volumes disponíveis.

**Por que não vejo todos os volumes no storage array remoto?**

Quando você está selecionando um volume secundário no storage array remoto, uma lista mostra todos os volumes elegíveis para esse par espelhado.

Quaisquer volumes que não sejam elegíveis para serem usados, não serão exibidos nessa lista. Os volumes não podem ser elegíveis por qualquer um dos seguintes motivos:

- O volume é um volume não padrão, como um volume instantâneo.
- O volume não é ideal.
- O volume já está participando de uma relação de espelhamento.
- Para espelhamento assíncrono, os atributos de volume fino entre o volume primário e o volume secundário não correspondem.
- Se estiver a utilizar o Data Assurance (DA), o volume primário e o volume secundário têm de ter as mesmas definições DE DA.
  - Se o volume primário for DA ativado, o volume secundário tem de ser DA ativado.
  - Se o volume primário não estiver ativado DA, o volume secundário não deve ser ativado DA.
- Para o espelhamento assíncrono, o volume primário e o volume secundário devem ter os mesmos recursos de Segurança da Unidade.
  - Se o volume primário for compatível com FIPS, o volume secundário deve ser capaz de FIPS.
  - Se o volume principal for compatível com FDE, o volume secundário tem de ser capaz de FDE.
  - Se o volume principal não estiver usando o Drive Security, o volume secundário não deve estar usando o Drive Security.

**Qual o impactos que a prioridade de sincronização tem nas taxas de sincronização?**

## A prioridade de sincronização define quanto tempo de processamento é alocado para atividades de sincronização em relação ao desempenho do sistema.

O proprietário do controlador do volume primário executa esta operação em segundo plano. Ao mesmo tempo, o proprietário do controlador processa gravações de e/S locais no volume principal e gravações remotas associadas no volume secundário. Como a ressincronização desvia os recursos de processamento do controlador da atividade de e/S, a ressincronização pode ter um impacto no desempenho do aplicativo host.

Mantenha essas diretrizes em mente para ajudá-lo a determinar quanto tempo uma prioridade de sincronização pode levar e como as prioridades de sincronização podem afetar o desempenho do sistema.

Estas tarifas prioritárias estão disponíveis:

- Mais baixo
- Baixo
- Média
- Alta
- Mais alto

A taxa de prioridade mais baixa suporta o desempenho do sistema, mas a ressincronização leva mais tempo. A taxa de prioridade mais alta é compatível com a ressincronização, mas o desempenho do sistema pode estar comprometido.

Estas orientações aproximam aproximadamente as diferenças entre as prioridades.

| Taxa de prioridade para sincronização completa | Tempo decorrido em comparação com a taxa de sincronização mais elevada |
|---|---|
| Mais baixo | Aproximadamente oito vezes, desde que na taxa de prioridade mais alta. |
| Baixo | Aproximadamente seis vezes, desde que na taxa de prioridade mais alta. |
| Média | Aproximadamente três vezes e meia, desde que com a taxa de prioridade mais alta. |
| Alta | Aproximadamente o dobro do tempo na taxa de prioridade mais alta. |

As cargas de tamanho de volume e taxa de e/S do host afetam as comparações de tempo de sincronização.

**Por que é recomendável usar uma política de sincronização manual?**

## A ressincronização manual é recomendada porque permite gerenciar o processo de ressincronização de uma forma que forneça a melhor oportunidade para recuperar dados.

Se você usar uma política de ressincronização automática e ocorrerem problemas de comunicação intermitente durante a ressincronização, os dados no volume secundário poderão ser corrompidos temporariamente. Quando a ressincronização é concluída, os dados são corrigidos.

# Certificados

## Descrição geral dos certificados

O Gerenciamento de certificados permite criar solicitações de assinatura de certificado (CSRs), importar certificados e gerenciar certificados existentes.

### O que são certificados?

*Certificados* são arquivos digitais que identificam entidades online, como sites e servidores, para comunicações seguras na internet. Existem dois tipos de certificados: Um certificado *assinado* é validado por uma autoridade de certificação (CA) e um certificado *autoassinado* é validado pelo proprietário da entidade em vez de um terceiro.

Saiba mais:

- "Como os certificados funcionam"
- "Terminologia do certificado"

### Como faço para configurar certificados?

No Gerenciamento de certificados, você pode configurar certificados para a estação de gerenciamento que hospeda o Unified Manager e também importar certificados para os controladores nos arrays.

Saiba mais:

- "Use certificados assinados pela CA para o sistema de gerenciamento"
- "Importar certificados para matrizes"

## Conceitos

### Como os certificados funcionam

Certificados são arquivos digitais que identificam entidades online, como sites e servidores, para comunicações seguras na internet.

#### Certificados assinados

Os certificados garantem que as comunicações da Web sejam transmitidas de forma encriptada, privada e inalterada, apenas entre o servidor e o cliente especificados. Com o Unified Manager, você pode gerenciar certificados para o navegador em um sistema de gerenciamento de host e as controladoras nos storage arrays descobertos.

Um certificado pode ser assinado por uma autoridade confiável ou pode ser autoassinado. "Assinatura" significa simplesmente que alguém validou a identidade do proprietário e determinou que seus dispositivos podem ser confiáveis. As matrizes de armazenamento são fornecidas com um certificado auto-assinado gerado automaticamente em cada controlador. Você pode continuar usando os certificados autoassinados ou obter certificados assinados pela CA para uma conexão mais segura entre os controladores e os sistemas

host.

> Embora os certificados assinados pela CA forneçam melhor proteção de segurança (por exemplo, evitando ataques man-in-the-middle), eles também exigem taxas que podem ser caras se você tiver uma rede grande. Em contraste, os certificados autoassinados são menos seguros, mas são gratuitos. Portanto, os certificados autoassinados são mais usados para ambientes de teste internos, não em ambientes de produção.

Um certificado assinado é validado por uma autoridade de certificação (CA), que é uma organização de terceiros confiável. Os certificados assinados incluem detalhes sobre o proprietário da entidade (normalmente, um servidor ou site), data de emissão e expiração do certificado, domínios válidos para a entidade e uma assinatura digital composta por letras e números.

Quando você abre um navegador e insere um endereço da Web, o sistema executa um processo de verificação de certificados em segundo plano para determinar se você está se conetando a um site que inclui um certificado válido assinado pela CA. Geralmente, um site protegido com um certificado assinado inclui um ícone de cadeado e uma designação https no endereço. Se você tentar se conetar a um site que não contenha um certificado assinado pela CA, o navegador exibirá um aviso de que o site não está seguro.

A CA toma medidas para verificar sua identidade durante o processo de inscrição. Eles podem enviar um e-mail para sua empresa registrada, verificar seu endereço comercial e executar uma verificação HTTP ou DNS. Quando o processo de aplicação estiver concluído, a CA envia arquivos digitais para serem carregados em um sistema de gerenciamento de host. Normalmente, esses arquivos incluem uma cadeia de confiança, como segue:

- **Root** — na parte superior da hierarquia está o certificado raiz, que contém uma chave privada usada para assinar outros certificados. A raiz identifica uma organização de CA específica. Se você usar a mesma CA para todos os dispositivos de rede, precisará de apenas um certificado raiz.
- **Intermediate** — ramificação fora da raiz são os certificados intermediários. A CA emite um ou mais certificados intermediários para atuar como intermediários entre uma raiz protegida e certificados de servidor.
- **Servidor** — na parte inferior da cadeia está o certificado do servidor, que identifica sua entidade específica, como um site ou outro dispositivo. Cada controlador em um storage array requer um certificado de servidor separado.

#### Certificados autoassinados

Cada controladora no storage inclui um certificado pré-instalado e autoassinado. Um certificado autoassinado é semelhante a um certificado assinado pela CA, exceto que ele é validado pelo proprietário da entidade em vez de um terceiro. Como um certificado assinado pela CA, um certificado autoassinado contém sua própria chave privada e também garante que os dados sejam criptografados e enviados por uma conexão HTTPS entre um servidor e um cliente.

Os certificados autoassinados não são "confiáveis" pelos navegadores. Cada vez que você tenta se conetar a um site que contém apenas um certificado autoassinado, o navegador exibe uma mensagem de aviso. Você deve clicar em um link na mensagem de aviso que permite que você prossiga para o site; ao fazê-lo, você está essencialmente aceitando o certificado auto-assinado.

#### Certificados para Unified Manager

A interface do Unified Manager é instalada com o Web Services Proxy em um sistema host. Quando você abre um navegador e tenta se conetar ao Unified Manager, o navegador tenta verificar se o host é uma fonte confiável verificando se há um certificado digital. Se o navegador não localizar um certificado assinado pela CA para o servidor, ele abrirá uma mensagem de aviso. A partir daí, você pode continuar para o site para

aceitar o certificado autoassinado para essa sessão. Ou, você pode obter certificados digitais assinados de uma CA para que você não veja mais a mensagem de aviso.

#### Certificados para controladores

Durante uma sessão do Unified Manager, você pode ver mensagens de segurança adicionais quando tentar acessar um controlador que não tenha um certificado assinado pela CA. Nesse caso, você pode confiar permanentemente no certificado autoassinado ou importar os certificados assinados pela CA para os controladores para que o servidor Proxy de Serviços da Web possa autenticar solicitações de clientes recebidas desses controladores.

### Terminologia do certificado

Os termos a seguir se aplicam ao gerenciamento de certificados.

| Prazo | Descrição |
|---|---|
| CA | Uma autoridade de certificação (CA) é uma entidade confiável que emite documentos eletrônicos, chamados certificados digitais, para segurança na Internet. Esses certificados identificam proprietários de sites, o que permite conexões seguras entre clientes e servidores. |
| CSR | Uma solicitação de assinatura de certificado (CSR) é uma mensagem enviada de um requerente para uma autoridade de certificação (CA). O CSR valida as informações que a CA precisa para emitir um certificado. |
| Certificado | Um certificado identifica o proprietário de um site para fins de segurança, o que impede que atacantes personifiquem o site. O certificado contém informações sobre o proprietário do site e a identidade da entidade confiável que certifica (assina) essas informações. |
| Cadeia de certificados | Uma hierarquia de arquivos que adiciona uma camada de segurança aos certificados. Normalmente, a cadeia inclui um certificado raiz na parte superior da hierarquia, um ou mais certificados intermediários e os certificados de servidor que identificam as entidades. |
| Certificado intermédio | Um ou mais certificados intermediários ramificam da raiz na cadeia de certificados. A CA emite um ou mais certificados intermediários para atuar como intermediários entre uma raiz protegida e certificados de servidor. |
| Armazenamento de chaves | Um keystore é um repositório no seu sistema de gerenciamento de host que contém chaves privadas, juntamente com suas chaves públicas e certificados correspondentes. Essas chaves e certificados identificam suas próprias entidades, como os controladores. |
| Certificado raiz | O certificado raiz está no topo da hierarquia na cadeia de certificados e contém uma chave privada usada para assinar outros certificados. A raiz identifica uma organização de CA específica. Se você usar a mesma CA para todos os dispositivos de rede, precisará de apenas um certificado raiz. |

| Prazo | Descrição |
| --- | --- |
| Certificado assinado | Um certificado validado por uma autoridade de certificação (CA). Este arquivo de dados contém uma chave privada e garante que os dados sejam enviados de forma criptografada entre um servidor e um cliente através de uma conexão HTTPS. Além disso, um certificado assinado inclui detalhes sobre o proprietário da entidade (normalmente, um servidor ou site) e uma assinatura digital composta por letras e números. Um certificado assinado usa uma cadeia de confiança e, portanto, é mais frequentemente usado em ambientes de produção. Também referido como um "certificado assinado pela CA" ou um "certificado de gestão". |
| Certificado auto-assinado | Um certificado autoassinado é validado pelo proprietário da entidade. Este arquivo de dados contém uma chave privada e garante que os dados sejam enviados de forma criptografada entre um servidor e um cliente através de uma conexão HTTPS. Também inclui uma assinatura digital composta por letras e números. Um certificado autoassinado não usa a mesma cadeia de confiança que um certificado assinado pela CA e, portanto, é mais frequentemente usado em ambientes de teste. Também referido como um certificado "pré-instalado". |
| Certificado do servidor | O certificado do servidor está na parte inferior da cadeia de certificados. Ele identifica sua entidade específica, como um site ou outro dispositivo. Cada controlador em um sistema de storage requer um certificado de servidor separado. |
| Loja de confiança | Um repositório de confiança é um repositório que contém certificados de terceiros confiáveis, como CAs. |

## Use certificados assinados pela CA para o sistema de gerenciamento

Você pode obter e importar certificados assinados pela CA para acesso seguro ao sistema de gerenciamento que hospeda o Unified Manager.

### Antes de começar

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.

### Sobre esta tarefa

O uso de certificados assinados pela CA é um procedimento de três etapas.

### Passo 1: Complete um arquivo CSR

Primeiro, é necessário gerar um arquivo de solicitação de assinatura de certificado (CSR), que identifique sua organização e o sistema host onde o Proxy de Serviços Web e o Unified Manager estão instalados.

Como alternativa, você pode gerar um arquivo CSR usando uma ferramenta como OpenSSL e pular para Passo 2: Envie o arquivo CSR.

### Passos

1. Selecione **Gerenciamento de certificados**.

2. Na guia Gerenciamento, selecione **Complete CSR**.
3. Insira as seguintes informações e clique em **Next**:
   - **Organização** — o nome completo e legal de sua empresa ou organização. Inclua sufixos, como Inc. Ou Corp.
   - * Unidade organizacional (opcional) * — a divisão da sua organização que está a lidar com o certificado.
   - **Cidade/localidade** — a cidade onde o seu sistema de acolhimento ou negócio está localizado.
   - **Estado/região (opcional)** — o estado ou a região onde o seu sistema anfitrião ou negócio está localizado.
   - **Código ISO do país** — o código ISO de dois dígitos do seu país (Organização Internacional para Padronização), como os EUA.
4. Insira as seguintes informações sobre o sistema host onde o Proxy de Serviços Web está instalado:
   - **Nome comum** — o endereço IP ou o nome DNS do sistema host onde o Proxy de Serviços Web está instalado. Verifique se esse endereço está correto; ele deve corresponder exatamente ao que você digita para acessar o Unified Manager no navegador. Não inclua http:// ou https://. O nome DNS não pode começar com um curinga.
   - **Endereços IP alternativos** — se o nome comum for um endereço IP, você pode opcionalmente inserir quaisquer endereços IP adicionais ou aliases para o sistema host. Para várias entradas, use um formato delimitado por vírgulas.
   - **Nomes DNS alternativos** — se o nome comum for um nome DNS, insira quaisquer nomes DNS adicionais para o sistema host. Para várias entradas, use um formato delimitado por vírgulas. Se não houver nomes DNS alternativos, mas você inseriu um nome DNS no primeiro campo, copie esse nome aqui. O nome DNS não pode começar com um curinga.
5. Certifique-se de que as informações do host estão corretas. Se não estiver, os certificados retornados da CA falharão quando você tentar importá-los.
6. Clique em **Finish**.
7. Vá para Passo 2: Envie o arquivo CSR.

### Passo 2: Envie o arquivo CSR

Depois de criar um arquivo de solicitação de assinatura de certificado (CSR), você o enviará a uma Autoridade de Certificação (CA) para receber certificados de gerenciamento assinados para o sistema que hospeda o Unified Manager e o Proxy de Serviços da Web.

Os sistemas e-Series exigem o formato PEM (codificação ASCII Base64) para certificados assinados, que inclui os seguintes tipos de arquivo: .pem, .crt, .cer ou .key.

**Passos**

1. Localize o ficheiro CSR transferido.

   A localização da pasta do download depende do seu navegador.

2. Envie o arquivo CSR para uma CA (por exemplo, VeriSign ou DigiCert) e solicite certificados assinados no formato PEM.

**Depois de enviar um arquivo CSR para a CA, NÃO regenere outro arquivo CSR.** Sempre que você gera um CSR, o sistema cria um par de chaves privadas e públicas. A chave pública faz parte da CSR, enquanto a chave privada é mantida no keystore do sistema. Quando você recebe os certificados assinados e os importa, o sistema garante que as chaves privadas e públicas sejam o par original. Se as chaves não corresponderem, os certificados assinados não funcionarão e você deverá solicitar novos certificados à CA.

3. Quando a CA retornar os certificados assinados, vá para Passo 3: Importar certificados de gestão.

#### Passo 3: Importar certificados de gestão

Depois de receber certificados assinados da Autoridade de Certificação (CA), importe os certificados para o sistema host onde a interface Web Services Proxy e Unified Manager estão instalados.

**Antes de começar**

- Você recebeu certificados assinados da CA. Esses arquivos incluem o certificado raiz, um ou mais certificados intermediários e o certificado do servidor.
- Se a CA forneceu um arquivo de certificado encadeado (por exemplo, um arquivo .p7b), você deve descompactar o arquivo encadeado em arquivos individuais: O certificado raiz, um ou mais certificados intermediários e o certificado do servidor. Você pode usar o utilitário Windows `certmgr` para descompactar os arquivos (clique com o botão direito do Mouse e selecione **todas as tarefas › Exportar**). A codificação base-64 é recomendada. Quando as exportações estiverem concluídas, um arquivo CER é exibido para cada arquivo de certificado na cadeia.
- Você copiou os arquivos de certificado para o sistema host onde o Proxy de Serviços Web está sendo executado.

**Passos**

1. Selecione **Gerenciamento de certificados**.
2. Na guia Gerenciamento, selecione **Importar**.

   Abre-se uma caixa de diálogo para importar os ficheiros de certificado.

3. Clique em **Procurar** para selecionar primeiro os arquivos de certificado raiz e intermediário e, em seguida, selecione o certificado do servidor. Se você gerou o CSR a partir de uma ferramenta externa, você também deve importar o arquivo de chave privada que foi criado juntamente com o CSR.

   Os nomes de arquivo são exibidos na caixa de diálogo.

4. Clique em **Importar**.

**Resultados**

Os arquivos são carregados e validados. As informações do certificado são exibidas na página Gerenciamento de certificados.

## Repor certificados de gestão

Você pode reverter o certificado de gerenciamento para o estado original, autoassinado de fábrica.

**Antes de começar**

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança.

Caso contrário, as funções do certificado não aparecem.

**Sobre esta tarefa**

Esta tarefa exclui o certificado de gerenciamento atual do sistema host onde o Proxy de serviços da Web e o Unified Manager estão instalados. Depois que o certificado é redefinido, o sistema host reverte para usando o certificado autoassinado.

**Passos**

1. Selecione **Definições > certificados**.
2. Selecione a guia **Array Management** e, em seguida, selecione **Reset**.

   Uma caixa de diálogo confirmar certificado de gerenciamento de redefinição é aberta.

3. Digite `reset` o campo e clique em **Reset**.

   Após a atualização do navegador, o navegador pode bloquear o acesso ao site de destino e informar que o site está usando HTTP Strict Transport Security. Essa condição surge quando você volta para certificados autoassinados. Para limpar a condição que está bloqueando o acesso ao destino, você deve limpar os dados de navegação do navegador.

**Resultados**

O sistema reverte para o uso do certificado autoassinado do servidor. Como resultado, o sistema solicita aos usuários que aceitem manualmente o certificado autoassinado para suas sessões.

## Use certificados de matriz

### Importar certificados para matrizes

Se necessário, você pode importar certificados para os storages de armazenamento para que eles possam se autenticar com o sistema que hospeda o Unified Manager. Os certificados podem ser assinados por uma autoridade de certificação (CA) ou podem ser autoassinados.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Se você estiver importando certificados confiáveis, os certificados devem ser importados para os controladores de storage usando o System Manager.

**Passos**

1. Selecione **Gerenciamento de certificados**.
2. Selecione a guia **Trusted**.

   Esta página mostra todos os certificados reportados para os storages de armazenamento.

3. Selecione um **Importar › certificados** para importar um certificado de CA ou **Importar › certificados de matriz de armazenamento autoassinados** para importar um certificado autoassinado.

   Para limitar a exibição, você pode usar o campo de filtragem **Mostrar certificados que são…** ou pode classificar as linhas de certificado clicando em um dos cabeçalhos de coluna.

4. Na caixa de diálogo, selecione o certificado e clique em **Importar**.

   O certificado é carregado e validado.

### Excluir certificados confiáveis

Você pode excluir um ou mais certificados que não são mais necessários, como um certificado expirado.

#### Antes de começar

Importe o novo certificado antes de excluir o antigo.

> Esteja ciente de que a exclusão de um certificado raiz ou intermediário pode afetar vários storages, já que esses storages podem compartilhar os mesmos arquivos de certificado.

#### Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione a guia **Trusted**.
3. Selecione um ou mais certificados na tabela e clique em **Excluir**.

   > A função **Delete** não está disponível para certificados pré-instalados.

   A caixa de diálogo confirmar Excluir certificado confiável é aberta.

4. Confirme a exclusão e clique em **Excluir**.

   O certificado é removido da tabela.

### Resolver certificados não confiáveis

Certificados não confiáveis ocorrem quando um storage array tenta estabelecer uma conexão segura com o Unified Manager, mas a conexão não consegue confirmar como segura.

Na página certificado, você pode resolver certificados não confiáveis importando um certificado autoassinado da matriz de armazenamento ou importando um certificado de autoridade de certificação (CA) emitido por um terceiro confiável.

#### Antes de começar

- Você deve estar conetado com um perfil de usuário que inclua permissões de Administrador de Segurança.
- Se você pretende importar um certificado assinado pela CA:
  - Você gerou uma solicitação de assinatura de certificado (arquivo .CSR) para cada controlador na matriz de armazenamento e a enviou para a CA.
  - A CA retornou arquivos de certificado confiáveis.
  - Os ficheiros de certificado estão disponíveis no sistema local.

#### Sobre esta tarefa

Talvez seja necessário instalar certificados de CA confiáveis adicionais se alguma das seguintes opções for verdadeira:

- Recentemente, você adicionou uma matriz de armazenamento.
- Um ou ambos os certificados expiram.
- Um ou ambos os certificados são revogados.
- Um ou ambos os certificados estão faltando um certificado raiz ou intermediário.

**Passos**

1. Selecione **Gerenciamento de certificados**.
2. Selecione a guia **Trusted**.

   Esta página mostra todos os certificados reportados para os storages de armazenamento.

3. Selecione um **Importar › certificados** para importar um certificado de CA ou **Importar › certificados de matriz de armazenamento autoassinados** para importar um certificado autoassinado.

   Para limitar a exibição, você pode usar o campo de filtragem **Mostrar certificados que são…** ou pode classificar as linhas de certificado clicando em um dos cabeçalhos de coluna.

4. Na caixa de diálogo, selecione o certificado e clique em **Importar**.

   O certificado é carregado e validado.

## Gerenciar certificados

### Ver certificados

Você pode ver informações resumidas de um certificado, que inclui a organização usando o certificado, a autoridade que emitiu o certificado, o período de validade e as impressões digitais (identificadores exclusivos).

**Antes de começar**

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.

**Passos**

1. Selecione **Gerenciamento de certificados**.
2. Selecione um dos seguintes separadores:
   - **Gerenciamento** — mostra o certificado para o sistema que hospeda o Proxy de Serviços Web. Um certificado de gerenciamento pode ser autoassinado ou aprovado por uma autoridade de certificação (CA). Ele permite acesso seguro ao Unified Manager.
   - **Trusted** — mostra os certificados que o Unified Manager pode acessar para matrizes de armazenamento e outros servidores remotos, como um servidor LDAP. Os certificados podem ser emitidos a partir de uma autoridade de certificação (CA) ou podem ser autoassinados.
3. Para ver mais informações sobre um certificado, selecione sua linha, selecione as elipses no final da linha e clique em **Exibir** ou **Exportar**.

### Exportar certificados

Você pode exportar um certificado para exibir seus detalhes completos.

#### Antes de começar

Para abrir o ficheiro exportado, tem de ter uma aplicação de visualizador de certificados.

#### Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione um dos seguintes separadores:
   - **Gerenciamento** — mostra o certificado para o sistema que hospeda o Proxy de Serviços Web. Um certificado de gerenciamento pode ser autoassinado ou aprovado por uma autoridade de certificação (CA). Ele permite acesso seguro ao Unified Manager.
   - **Trusted** — mostra os certificados que o Unified Manager pode acessar para matrizes de armazenamento e outros servidores remotos, como um servidor LDAP. Os certificados podem ser emitidos a partir de uma autoridade de certificação (CA) ou podem ser autoassinados.
3. Selecione um certificado na página e, em seguida, clique nas elipses no final da linha.
4. Clique em **Exportar** e salve o arquivo de certificado.
5. Abra o arquivo no aplicativo visualizador de certificados.

# Gerenciamento de acesso

## Visão geral do Gerenciamento de Acesso

O Access Management é um método de configuração da autenticação de usuário no Unified Manager.

#### Quais métodos de autenticação estão disponíveis?

Estão disponíveis os seguintes métodos de autenticação:

- **Funções de usuário local** — a autenticação é gerenciada por meio de recursos RBAC (controle de acesso baseado em função). As funções de usuário local incluem perfis de usuário predefinidos e funções com permissões de acesso específicas.
- **Serviços de diretório** — a autenticação é gerenciada por meio de um servidor LDAP (Lightweight Directory Access Protocol) e serviço de diretório, como o ative Directory da Microsoft.
- **SAML** — a autenticação é gerenciada por meio de um Provedor de identidade (IDP) usando SAML 2,0.

Saiba mais:

- "Como o Gerenciamento de Acesso funciona"
- "Terminologia de Gerenciamento de Acesso"
- "Permissões para funções mapeadas"
- "SAML"

### Como faço para configurar o Gerenciamento de Acesso?

O software SANtricity está pré-configurado para utilizar funções de utilizador locais. Se pretender utilizar o LDAP, pode configurá-lo na página Gestão de acessos.

Saiba mais:

- "Gerenciamento de acesso com funções de usuário local"
- "Gerenciamento de acesso com serviços de diretório"
- "Configurar SAML"

## Conceitos

### Como o Gerenciamento de Acesso funciona

Use o Gerenciamento de acesso para estabelecer a autenticação de usuário no Unified Manager.

#### Fluxo de trabalho de configuração

A configuração do Access Management funciona da seguinte forma:

1. Um administrador faz login no Unified Manager com um perfil de usuário que inclui permissões de administrador de segurança.

   > Para iniciar sessão pela primeira vez, o nome de utilizador `admin` é apresentado automaticamente e não pode ser alterado. O `admin` utilizador tem acesso total a todas as funções do sistema. A palavra-passe tem de ser definida no início de sessão pela primeira vez.

2. O administrador navega para acessar o Gerenciamento na interface do usuário, que inclui funções de usuário locais pré-configuradas. Essas funções são uma implementação dos recursos RBAC (controle de acesso baseado em função).
3. O administrador configura um ou mais dos seguintes métodos de autenticação:
   - * Funções de usuário local* — a autenticação é gerenciada por meio de recursos RBAC. As funções de usuário local incluem usuários predefinidos e funções com permissões de acesso específicas. Os administradores podem usar essas funções de usuário local como o único método de autenticação ou usá-las em combinação com um serviço de diretório. Nenhuma configuração é necessária, além de definir senhas para usuários.
   - **Serviços de diretório** — a autenticação é gerenciada por meio de um servidor LDAP (Lightweight Directory Access Protocol) e serviço de diretório, como o ative Directory da Microsoft. Um administrador se coneta ao servidor LDAP e, em seguida, mapeia os usuários LDAP para as funções de usuário local.
   - **SAML** — a autenticação é gerenciada por meio de um Provedor de identidade (IDP) usando a Security Assertion Markup Language (SAML) 2,0. Um administrador estabelece a comunicação entre o sistema IDP e o storage array e, em seguida, mapeia os usuários IDP para as funções de usuário local incorporadas no storage array.
4. O administrador fornece aos usuários credenciais de login para o Unified Manager.
5. Os usuários fazem login no sistema inserindo suas credenciais. Durante o início de sessão, o sistema executa as seguintes tarefas em segundo plano:

- Autentica o nome de utilizador e a palavra-passe na conta de utilizador.
- Determina as permissões do usuário com base nas funções atribuídas.
- Fornece ao usuário acesso a funções na interface do usuário.
- Exibe o nome do usuário no banner superior.

#### Funções disponíveis no Unified Manager

O acesso a funções depende das funções atribuídas de um usuário, que incluem o seguinte:

- **Storage admin** — Acesso completo de leitura/gravação a objetos de armazenamento nas matrizes, mas sem acesso à configuração de segurança.
- **Security admin** — Acesso à configuração de segurança em Gerenciamento de Acesso e Gerenciamento de certificados.
- **Support admin** — Acesso a todos os recursos de hardware em matrizes de armazenamento, dados de falha e eventos mel. Sem acesso a objetos de armazenamento ou à configuração de segurança.
- **Monitor** — Acesso somente leitura a todos os objetos de armazenamento, mas sem acesso à configuração de segurança.

Uma função indisponível está a cinzento ou não é apresentada na interface do utilizador.

### Terminologia de Gerenciamento de Acesso

Saiba como os termos do Gerenciamento de Acesso se aplicam ao Unified Manager.

| Prazo | Descrição |
|---|---|
| Ative Directory | O ative Directory (AD) é um serviço de diretório da Microsoft que usa LDAP para redes de domínio do Windows. |
| Encadernação | As operações de vinculação são usadas para autenticar clientes no servidor de diretórios. A vinculação geralmente requer credenciais de conta e senha, mas alguns servidores permitem operações anônimas de vinculação. |
| CA | Uma autoridade de certificação (CA) é uma entidade confiável que emite documentos eletrônicos, chamados certificados digitais, para segurança na Internet. Esses certificados identificam proprietários de sites, o que permite conexões seguras entre clientes e servidores. |
| Certificado | Um certificado identifica o proprietário de um site para fins de segurança, o que impede que atacantes personifiquem o site. O certificado contém informações sobre o proprietário do site e a identidade da entidade confiável que certifica (assina) essas informações. |
| LDAP | O LDAP (Lightweight Directory Access Protocol) é um protocolo de aplicação para aceder e manter serviços de informação de diretório distribuído. Este protocolo permite que vários aplicativos e serviços diferentes se conetem ao servidor LDAP para validar usuários. |

| Prazo | Descrição |
| --- | --- |
| RBAC | O controle de acesso baseado em função (RBAC) é um método de regular o acesso a recursos de computador ou rede com base nas funções de usuários individuais. O Unified Manager inclui funções predefinidas. |
| SAML | Security Assertion Markup Language (SAML) é um padrão baseado em XML para autenticação e autorização entre duas entidades. O SAML permite a autenticação multifator, na qual os usuários devem fornecer dois ou mais itens para provar sua identidade (por exemplo, uma senha e uma impressão digital). O recurso SAML incorporado do storage array é compatível com SAML2,0 para afirmação, autenticação e autorização de identidade. |
| SSO | Logon único (SSO) é um serviço de autenticação que permite que um conjunto de credenciais de login acesse vários aplicativos. |
| Proxy de serviços Web | O Web Services Proxy, que fornece acesso através de mecanismos HTTPS padrão, permite que os administradores configurem serviços de gerenciamento para matrizes de armazenamento. O proxy pode ser instalado em hosts Windows ou Linux. A interface do Unified Manager está disponível com o Web Services Proxy. |

#### Permissões para funções mapeadas

Os recursos RBAC (controle de acesso baseado em função) incluem usuários predefinidos com uma ou mais funções mapeadas para eles. Cada função inclui permissões para acessar tarefas no Unified Manager.

As funções fornecem acesso do usuário a tarefas, como segue:

- **Storage admin** — Acesso completo de leitura/gravação a objetos de armazenamento nas matrizes, mas sem acesso à configuração de segurança.
- **Security admin** — Acesso à configuração de segurança em Gerenciamento de Acesso e Gerenciamento de certificados.
- **Support admin** — Acesso a todos os recursos de hardware em matrizes de armazenamento, dados de falha e eventos mel. Sem acesso a objetos de armazenamento ou à configuração de segurança.
- **Monitor** — Acesso somente leitura a todos os objetos de armazenamento, mas sem acesso à configuração de segurança.

Se um usuário não tiver permissões para uma determinada função, essa função não estará disponível para seleção ou não será exibida na interface do usuário.

#### Gerenciamento de acesso com funções de usuário local

Os administradores podem usar os recursos RBAC (controle de acesso baseado em função) aplicados no Unified Manager. Esses recursos são chamados de "funções de usuário local".

#### Fluxo de trabalho de configuração

As funções de utilizador local são pré-configuradas no sistema. Para usar funções de usuário local para autenticação, os administradores podem fazer o seguinte:

1. Um administrador faz login no Unified Manager com um perfil de usuário que inclui permissões de administrador de segurança.

   O `admin` utilizador tem acesso total a todas as funções do sistema.

2. Um administrador analisa os perfis de usuário, que são predefinidos e não podem ser modificados.
3. Opcionalmente, o administrador atribui novas senhas para cada perfil de usuário.
4. Os usuários fazem login no sistema com suas credenciais atribuídas.

#### Gerenciamento

Ao usar apenas funções de usuário local para autenticação, os administradores podem executar as seguintes tarefas de gerenciamento:

- Alterar senhas.
- Defina um comprimento mínimo para senhas.
- Permitir que os usuários façam login sem senhas.

### Gerenciamento de acesso com serviços de diretório

Os administradores podem usar um servidor LDAP (Lightweight Directory Access Protocol) e um serviço de diretório, como o ative Directory da Microsoft.

#### Fluxo de trabalho de configuração

Se um servidor LDAP e um serviço de diretório são usados na rede, a configuração funciona da seguinte forma:

1. Um administrador faz login no Unified Manager com um perfil de usuário que inclui permissões de administrador de segurança.

   O `admin` utilizador tem acesso total a todas as funções do sistema.

2. O administrador insere as configurações do servidor LDAP. As configurações incluem o nome do domínio, URL e informações da conta Bind.
3. Se o servidor LDAP usar um protocolo seguro (LDAPS), o administrador carrega uma cadeia de certificados de autoridade de certificação (CA) para autenticação entre o servidor LDAP e o sistema host onde o proxy de serviços da Web está instalado.
4. Depois de estabelecer a ligação ao servidor, o administrador mapeia os grupos de utilizadores para as funções de utilizador locais. Essas funções são predefinidas e não podem ser modificadas.
5. O administrador testa a conexão entre o servidor LDAP e o Proxy de serviços da Web.
6. Os usuários fazem login no sistema com suas credenciais LDAP/Directory Services atribuídas.

#### Gerenciamento

Ao usar serviços de diretório para autenticação, os administradores podem executar as seguintes tarefas de gerenciamento:

- Adicione um servidor de diretório.
- Editar definições do servidor de diretório.
- Mapeie usuários LDAP para funções de usuário locais.
- Remova um servidor de diretório.
- Alterar senhas.
- Defina um comprimento mínimo para senhas.
- Permitir que os usuários façam login sem senhas.

### Gerenciamento de acesso com SAML

Para Gerenciamento de Acesso, os administradores podem usar os recursos de Security Assertion Markup Language (SAML) 2,0 incorporados no array.

#### Fluxo de trabalho de configuração

A configuração SAML funciona da seguinte forma:

1. Um administrador faz login no Unified Manager com um perfil de usuário que inclui permissões de administrador de segurança.

   O `admin` utilizador tem acesso total a todas as funções do System Manager.

2. O administrador vai para a guia **SAML** em Gerenciamento de Acesso.
3. Um administrador configura as comunicações com o Provedor de identidade (IDP). Um IDP é um sistema externo usado para solicitar credenciais de um usuário e determinar se o usuário foi autenticado com êxito. Para configurar as comunicações com o storage array, o administrador baixa o arquivo de metadados IDP do sistema IDP e, em seguida, usa o Unified Manager para carregar o arquivo para o storage array.
4. Um administrador estabelece uma relação de confiança entre o Fornecedor de Serviços e o IDP. Um Fornecedor de Serviços controla a autorização do utilizador; neste caso, o controlador na matriz de armazenamento atua como o Fornecedor de Serviços. Para configurar as comunicações, o administrador usa o Unified Manager para exportar um arquivo de metadados do provedor de serviços para o controlador. A partir do sistema IDP, o administrador então importa o arquivo de metadados para o IDP.

   Os administradores também devem certificar-se de que o IDP suporta a capacidade de retornar um ID de nome na autenticação.

5. O administrador mapeia as funções do storage array para atributos de usuário definidos no IDP. Para fazer isso, o administrador usa o Unified Manager para criar os mapeamentos.
6. O administrador testa o login SSO para o URL do IDP. Este teste garante que a matriz de armazenamento e o IDP possam se comunicar.

Uma vez que o SAML está ativado, você *não pode* desabilitá-lo através da interface do usuário, nem pode editar as configurações de IDP. Se você precisar desativar ou editar a configuração SAML, entre em Contato com o suporte técnico para obter assistência.

7. No Unified Manager, o administrador habilita o SAML para o storage array.
8. Os usuários fazem login no sistema com suas credenciais SSO.

#### Gerenciamento

Ao usar o SAML para autenticação, os administradores podem executar as seguintes tarefas de gerenciamento:

- Modificar ou criar novos mapeamentos de função
- Exportar ficheiros do fornecedor de serviços

#### Restrições de acesso

Quando o SAML está ativado, os usuários não podem descobrir ou gerenciar o armazenamento desse array a partir da interface herdada do Storage Manager.

Além disso, os seguintes clientes não podem acessar os serviços e recursos do storage array:

- Janela de gerenciamento empresarial (EMW)
- Interface de linha de comando (CLI)
- Clientes de Software Developer Kits (SDK)
- Clientes na banda
- Clientes API REST de Autenticação básica HTTP
- Faça login usando o endpoint padrão da API REST

## Use funções de usuário local

### Ver funções de utilizador locais

Na guia funções do usuário local, você pode exibir os mapeamentos dos usuários para as funções padrão. Esses mapeamentos fazem parte do RBAC (controles de acesso baseados em função) aplicado no Proxy de serviços da Web para Unified Manager.

#### Antes de começar

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.

#### Sobre esta tarefa

Os usuários e mapeamentos não podem ser alterados. Apenas as senhas podem ser modificadas.

#### Passos

1. Selecione **Gerenciamento de Acesso**.
2. Selecione a guia **funções de usuário local**.

   Os usuários são mostrados na tabela:

- **Admin** — Super administrador que tem acesso a todas as funções do sistema. Este usuário inclui todas as funções.
- **Storage** — o administrador responsável por todo o provisionamento de armazenamento. Esse usuário inclui as seguintes funções: Administrador de storage, administrador de suporte e monitor.
- **Segurança** — o usuário responsável pela configuração de segurança, incluindo Gerenciamento de Acesso e Gerenciamento de certificados. Este usuário inclui as seguintes funções: Admin de segurança e Monitor.
- **Suporte** — o usuário responsável por recursos de hardware, dados de falha e atualizações de firmware. Este usuário inclui as seguintes funções: Admin de suporte e Monitor.
- **Monitor** — Um usuário com acesso somente leitura ao sistema. Este utilizador inclui apenas a função Monitor.
- **rw** (leitura/gravação) — este usuário inclui as seguintes funções: Administrador de armazenamento, administrador de suporte e monitor.
- **Ro** (somente leitura) — este usuário inclui somente a função Monitor.

### Alterar senhas para perfis de usuário locais

Você pode alterar as senhas de usuário para cada usuário no Gerenciamento de acesso.

#### Antes de começar

- Você deve estar logado como administrador local, o que inclui permissões de administrador raiz.
- Você deve saber a senha do administrador local.

#### Sobre esta tarefa

Tenha em mente estas diretrizes ao escolher uma senha:

- Quaisquer novas senhas de usuário local devem atender ou exceder a configuração atual para uma senha mínima (em Configurações de visualização/edição).
- As senhas diferenciam maiúsculas de minúsculas.
- Os espaços de saída não são removidos das senhas quando são definidos. Tenha cuidado para incluir espaços se eles foram incluídos na senha.
- Para maior segurança, use pelo menos 15 carateres alfanuméricos e altere a senha com frequência.

#### Passos

1. Selecione **Gerenciamento de Acesso**.
2. Selecione a guia **funções de usuário local**.
3. Selecione um usuário na tabela.

   O botão alterar senha fica disponível.

4. Selecione **alterar palavra-passe**.

   A caixa de diálogo alterar senha será exibida.

5. Se não estiver definido um comprimento mínimo de palavra-passe para palavras-passe de utilizador local, pode selecionar a caixa de verificação para exigir que o utilizador introduza uma palavra-passe para aceder ao sistema.
6. Introduza a nova palavra-passe para o utilizador selecionado nos dois campos.

7. Introduza a palavra-passe do administrador local para confirmar esta operação e, em seguida, clique em **alterar**.

**Resultados**

Se o usuário estiver conetado no momento, a alteração da senha fará com que a sessão ativa do usuário seja encerrada.

### Altere as definições de palavra-passe do utilizador local

Pode definir o comprimento mínimo necessário para todas as palavras-passe de utilizador locais novas ou atualizadas. Também pode permitir que os utilizadores locais acedam ao sistema sem introduzir uma palavra-passe.

**Antes de começar**

Você deve estar logado como administrador local, o que inclui permissões de administrador raiz.

**Sobre esta tarefa**

Tenha estas diretrizes em mente ao definir o comprimento mínimo para senhas de usuário local:

- A definição de alterações não afeta as palavras-passe de utilizador locais existentes.
- A definição de comprimento mínimo necessário para palavras-passe de utilizador local tem de ter entre 0 e 30 carateres.
- Quaisquer novas senhas de usuário local devem atender ou exceder a configuração de comprimento mínimo atual.
- Não defina um comprimento mínimo para a palavra-passe se pretender que os utilizadores locais acedam ao sistema sem introduzir uma palavra-passe.

**Passos**

1. Selecione **Gerenciamento de Acesso**.
2. Selecione a guia **funções de usuário local**.
3. Selecione **Exibir/Editar configurações**.

   A caixa de diálogo Configurações de senha do usuário local é aberta.

4. Execute um dos seguintes procedimentos:
   - Para permitir que os usuários locais acessem o sistema *sem* inserir uma senha, desmarque a caixa de seleção "exigir que todas as senhas de usuário local sejam pelo menos".
   - Para definir um comprimento mínimo de palavra-passe para todas as palavras-passe de utilizador local, selecione a caixa de verificação "exigir que todas as palavras-passe de utilizador local sejam pelo menos" e, em seguida, utilize a caixa de seleção para definir o comprimento mínimo necessário para todas as palavras-passe de utilizador local.

     Todas as novas senhas de usuário local devem atender ou exceder a configuração atual.

5. Clique em **Salvar**.

## Use os serviços de diretório

### Adicionar servidor de diretório

Para configurar a autenticação para o Gerenciamento de Acesso, você estabelece comunicações entre um servidor LDAP e o host que executa o Proxy de Serviços Web para Unified Manager. Em seguida, mapeia os grupos de utilizadores LDAP para as funções de utilizador local.

#### Antes de começar

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- Os grupos de usuários devem ser definidos em seu serviço de diretório.
- As credenciais do servidor LDAP devem estar disponíveis, incluindo o nome de domínio, o URL do servidor e, opcionalmente, o nome de usuário e a senha da conta BIND.
- Para servidores LDAPS que usam um protocolo seguro, a cadeia de certificados do servidor LDAP deve ser instalada na sua máquina local.

#### Sobre esta tarefa

Adicionar um servidor de diretório é um processo de duas etapas. Primeiro você insere o nome de domínio e URL. Se o servidor usar um protocolo seguro, você também deve carregar um certificado de CA para autenticação se ele for assinado por uma autoridade de assinatura não padrão. Se tiver credenciais para uma conta BIND, também poderá introduzir o nome da conta de utilizador e a palavra-passe. Em seguida, você mapeia os grupos de usuários do servidor LDAP para funções de usuário locais.

#### Passos

1. Selecione **Gerenciamento de Acesso**.
2. Na guia **Serviços de diretório**, selecione **Adicionar servidor de diretório**.

   A caixa de diálogo Adicionar servidor de diretório é aberta.

3. Na guia **Configurações do servidor**, insira as credenciais do servidor LDAP.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| **Configurações de configuração** | Domínio(s) |
| Introduza o nome de domínio do servidor LDAP. Para vários domínios, insira os domínios em uma lista separada por vírgulas. O nome de domínio é usado no login (*username__domain*) para especificar em qual servidor de diretório se autenticar. | URL do servidor |
| Insira o URL para acessar o servidor LDAP na forma `ldap[s]://**host**:*port*` de . | Carregar certificado (opcional) |
| Este campo aparece apenas se um protocolo LDAPS for especificado no campo URL do servidor acima.<br><br>Clique em **Procurar** e selecione um certificado de CA para carregar. Este é o certificado confiável ou cadeia de certificados usada para autenticar o servidor LDAP. | Vincular conta (opcional) |

| Definição | Descrição |
| --- | --- |
| Insira uma conta de usuário somente leitura para consultas de pesquisa no servidor LDAP e para pesquisar nos grupos. Introduza o nome da conta num formato de tipo LDAP. Por exemplo, se o usuário bind for chamado de "bindacct", você poderá inserir um valor como `CN=bindacct,CN=Users,DC=cpoc,DC=local` . | Vincular senha (opcional) |
| Este campo é exibido quando você insere uma conta BIND.<br><br>Introduza a palavra-passe para a conta vincular. | Teste a conexão do servidor antes de adicionar |

| Definição | Descrição |
| --- | --- |
| Selecione esta caixa de verificação se pretender certificar-se de que o sistema pode comunicar com a configuração do servidor LDAP introduzida. O teste ocorre depois de clicar em **Add** na parte inferior da caixa de diálogo.<br><br>Se esta caixa de verificação estiver selecionada e o teste falhar, a configuração não será adicionada. Você deve resolver o erro ou desmarcar a caixa de seleção para ignorar o teste e adicionar a configuração. | • Configurações de privilégio* |
| Pesquisar DN base | Introduza o contexto LDAP para procurar utilizadores, normalmente na forma `CN=Users, DC=cpoc, DC=local` de . |
| Atributo de nome de usuário | Insira o atributo que está vinculado ao ID do usuário para autenticação. Por exemplo `sAMAccountName`: . |
| Atributo(s) de grupo | Insira uma lista de atributos de grupo no usuário, que é usada para mapeamento de grupo para função. Por exemplo `memberOf, managedObjects`: . |

4. Clique na guia **Mapeamento de função**.
5. Atribua grupos LDAP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| **Mapeamentos** | DN do grupo |
| Especifique o nome distinto do grupo (DN) para o grupo de usuários LDAP a ser mapeado. Expressões regulares são suportadas. Estes carateres especiais de expressão regular devem ser escapados com uma barra invertida () se eles não são parte de um padrão de expressão regular | Funções |

A função Monitor é necessária para todos os usuários, incluindo o administrador.

6. Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.
7. Quando terminar com os mapeamentos, clique em **Add**.

   O sistema executa uma validação, certificando-se de que a matriz de armazenamento e o servidor LDAP possam se comunicar. Se for apresentada uma mensagem de erro, assinale as credenciais introduzidas na caixa de diálogo e volte a introduzir as informações, se necessário.

### Edite as configurações do servidor de diretório e mapeamentos de função

Se você configurou anteriormente um servidor de diretório em Gerenciamento de Acesso, poderá alterar suas configurações a qualquer momento. As configurações incluem as informações de conexão do servidor e os mapeamentos de grupo para função.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- Um servidor de diretório deve ser definido.

**Passos**

1. Selecione **Gerenciamento de Acesso**.
2. Selecione a guia **Serviços de diretório**.
3. Se mais de um servidor estiver definido, selecione o servidor que deseja editar na tabela.

4. Selecione **Exibir/Editar configurações**.

   A caixa de diálogo Configurações do servidor de diretório é aberta.

5. Na guia **Configurações do servidor**, altere as configurações desejadas.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| **Configurações de configuração** | Domínio(s) |
| O(s) nome(s) de domínio do(s) servidor(es) LDAP. Para vários domínios, insira os domínios em uma lista separada por vírgulas. O nome de domínio é usado no login (*username__domain*) para especificar em qual servidor de diretório se autenticar. | URL do servidor |
| O URL para acessar o servidor LDAP na forma `ldap[s]://host:port` de . | Vincular conta (opcional) |
| A conta de usuário somente leitura para consultas de pesquisa no servidor LDAP e para pesquisa dentro dos grupos. | Vincular senha (opcional) |
| A senha para a conta vincular. (Este campo é exibido quando uma conta BIND é inserida.) | Teste a conexão do servidor antes de salvar |

| Definição | Descrição |
| --- | --- |
| Verifica se o sistema pode comunicar com a configuração do servidor LDAP. O teste ocorre depois de clicar em **Salvar**. Se esta caixa de verificação estiver selecionada e o teste falhar, a configuração não será alterada. Você deve resolver o erro ou desmarcar a caixa de seleção para ignorar o teste e reeditar a configuração. | • Configurações de privilégio* |
| Pesquisar DN base | O contexto LDAP para procurar usuários, normalmente na forma `CN=Users, DC=cpoc, DC=local` de . |
| Atributo de nome de usuário | O atributo que está vinculado ao ID do usuário para autenticação. Por exemplo `sAMAccountName`: . |
| Atributo(s) de grupo | Uma lista de atributos de grupo no usuário, que é usada para mapeamento de grupo para função. Por exemplo `memberOf, managedObjects`: . |

6. Na guia **Mapeamento de função**, altere o mapeamento desejado.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| **Mapeamentos** | DN do grupo |
| O nome de domínio para o grupo de utilizadores LDAP a ser mapeado. Expressões regulares são suportadas. Esses carateres especiais de expressão regular devem ser escapados com uma barra invertida () se não fizerem parte de um padrão de expressão regular:<br><br>O que é que é que não é possível | Funções |

A função Monitor é necessária para todos os usuários, incluindo o administrador.

7. Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.
8. Clique em **Salvar**.

**Resultados**

Depois de concluir esta tarefa, todas as sessões ativas do utilizador são encerradas. Apenas a sessão de utilizador atual é mantida.

### Remova o servidor de diretório

Para interromper a conexão entre um servidor de diretório e o Proxy de serviços da Web, você pode remover as informações do servidor da página Gerenciamento de acesso. Talvez você queira executar essa tarefa se tiver configurado um novo servidor e, em seguida, desejar remover o antigo.

**Antes de começar**

Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.

**Sobre esta tarefa**

Depois de concluir esta tarefa, todas as sessões ativas do utilizador são encerradas. Apenas a sessão de utilizador atual é mantida.

**Passos**

1. Selecione **Gerenciamento de Acesso**.
2. Selecione a guia **Serviços de diretório**.
3. Na lista, selecione o servidor de diretório que deseja excluir.
4. Clique em **Remover**.

   A caixa de diálogo Remover servidor de diretório é aberta.

5. Digite `remove` o campo e clique em **Remover**.

   As configurações do servidor de diretório, as configurações de privilégio e os mapeamentos de função são removidos. Os usuários não podem mais fazer login com credenciais deste servidor.

## Use SAML

### Configurar SAML

Para configurar a autenticação para o Access Management, você pode usar os recursos de Security Assertion Markup Language (SAML) incorporados no storage array. Esta configuração estabelece uma conexão entre um Provedor de identidade e o Provedor de armazenamento.

#### Antes de começar

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- Você deve saber o endereço IP ou o nome de domínio do controlador na matriz de armazenamento.
- Um administrador de IDP configurou um sistema de IDP.
- Um administrador de IDP garantiu que o IDP suporta a capacidade de retornar um ID de nome na autenticação.
- Um administrador garantiu que o servidor IDP e o relógio do controlador são sincronizados (através de um servidor NTP ou ajustando as definições do relógio do controlador).
- Um arquivo de metadados IDP é baixado do sistema IDP e está disponível no sistema local usado para acessar o Unified Manager.

#### Sobre esta tarefa

Um Provedor de identidade (IDP) é um sistema externo usado para solicitar credenciais de um usuário e para determinar se esse usuário foi autenticado com êxito. O IDP pode ser configurado para fornecer autenticação multifator e usar qualquer banco de dados de usuários, como o ative Directory. Sua equipe de segurança é responsável por manter o IDP. Um provedor de serviços (SP) é um sistema que controla a autenticação e o acesso do usuário. Quando o Gerenciamento de Acesso é configurado com SAML, o storage array atua como o provedor de serviços para solicitar autenticação do provedor de identidade. Para estabelecer uma conexão entre o IDP e o storage array, você compartilha arquivos de metadados entre essas duas entidades. Em seguida, você mapeia as entidades de usuário IDP para as funções de storage array. E, finalmente, você testa os logins de conexão e SSO antes de ativar o SAML.

**SAML e Serviços de diretório**. Se você ativar o SAML quando os Serviços de diretório estiverem configurados como o método de autenticação, o SAML substituirá os Serviços de diretório no Unified Manager. Se você desabilitar o SAML mais tarde, a configuração dos Serviços de diretório retornará à configuração anterior.

**Edição e desativação.** Uma vez que o SAML está ativado, você *não pode* desabilitá-lo através da interface do usuário, nem pode editar as configurações de IDP. Se você precisar desativar ou editar a configuração SAML, entre em Contato com o suporte técnico para obter assistência.

Configurar a autenticação SAML é um procedimento de várias etapas.

#### Passo 1: Faça o upload do arquivo de metadados IDP

Para fornecer ao storage array informações de conexão IDP, você importa metadados IDP para o Unified Manager. O sistema de IDP precisa desses metadados para redirecionar as solicitações de autenticação para o URL correto e para validar as respostas recebidas.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **SAML**.

   A página exibe uma visão geral das etapas de configuração.

3. Clique no link **Import Identity Provider (IDP) file**.

   A caixa de diálogo Importar arquivo do provedor de identidade será aberta.

4. Clique em **Procurar** para selecionar e carregar o ficheiro de metadados IDP copiado para o sistema local.

   Depois de selecionar o ficheiro, é apresentado o ID da entidade IDP.

5. Clique em **Importar**.

#### Passo 2: Exportar arquivos do provedor de serviços

Para estabelecer uma relação de confiança entre o IDP e o storage array, você importa os metadados do provedor de serviços para o IDP. O IDP precisa desses metadados para estabelecer uma relação de confiança com o controlador e processar solicitações de autorização. O arquivo inclui informações como o nome de domínio do controlador ou endereço IP, para que o IDP possa se comunicar com os provedores de serviços.

**Passos**

1. Clique no link **Exportar arquivos do provedor de serviços**.

   A caixa de diálogo Exportar ficheiros do fornecedor de serviços abre-se.

2. Introduza o endereço IP do controlador ou o nome DNS no campo **Controller A** e, em seguida, clique em **Export** para guardar o ficheiro de metadados no sistema local.

   Depois de clicar em **Exportar**, os metadados do fornecedor de serviços são transferidos para o seu sistema local. Anote onde o arquivo é armazenado.

3. No sistema local, localize o arquivo de metadados do provedor de serviços formatado em XML que você exportou.
4. A partir do servidor IDP, importe o arquivo de metadados do provedor de serviços para estabelecer a relação de confiança. Você pode importar o arquivo diretamente ou inserir manualmente as informações do controlador a partir do arquivo.

#### Passo 3: Mapear funções

Para fornecer aos usuários autorização e acesso ao Unified Manager, é necessário mapear os atributos de usuário e associações a grupos de IDP para as funções predefinidas do storage array.

**Antes de começar**

- Um administrador de IDP configurou atributos de usuário e associação de grupo no sistema de IDP.
- O arquivo de metadados de IDP é importado para o Unified Manager.
- Um arquivo de metadados do provedor de serviços para o controlador é importado para o sistema IDP para a relação de confiança.

**Passos**

1. Clique no link para **Mapping Unified Manager** Roles.

   A caixa de diálogo Mapeamento de função é aberta.

2. Atribua atributos de usuário e grupos IDP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

   **Detalhes do campo**

| Definição | Descrição |
|---|---|
| **Mapeamentos** | Atributo do utilizador |
| Especifique o atributo (por exemplo, "membro de") para o grupo SAML a ser mapeado. | Valor do atributo |
| Especifique o valor do atributo para o grupo a ser mapeado. Expressões regulares são suportadas. Esses carateres especiais de expressão regular devem ser escapados com uma barra invertida (\) se eles não forem parte de um padrão de expressão regular | Funções |

   A função Monitor é necessária para todos os usuários, incluindo o administrador. O Unified Manager não funcionará corretamente para nenhum usuário sem a função Monitor presente.

3. Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.

Mapeamentos de função podem ser modificados depois que o SAML estiver habilitado.

4. Quando terminar com os mapeamentos, clique em **Salvar**.

#### Passo 4: Teste o login SSO

Para garantir que o sistema IDP e o storage array possam se comunicar, você pode testar opcionalmente um login SSO. Este teste também é realizado durante a etapa final para ativar o SAML.

**Antes de começar**

- O arquivo de metadados de IDP é importado para o Unified Manager.
- Um arquivo de metadados do provedor de serviços para o controlador é importado para o sistema IDP para a relação de confiança.

**Passos**

1. Selecione o link **Test SSO Login**.

   Abre-se uma caixa de diálogo para introduzir credenciais SSO.

2. Insira credenciais de login para um usuário com permissões de Administrador de Segurança e permissões de Monitor.

   Abre-se uma caixa de diálogo enquanto o sistema testa o início de sessão.

3. Procure uma mensagem Teste bem-sucedida. Se o teste for concluído com êxito, vá para a próxima etapa para ativar o SAML.

   Se o teste não for concluído com êxito, é apresentada uma mensagem de erro com mais informações. Certifique-se de que:

   - O usuário pertence a um grupo com permissões para Administrador de Segurança e Monitor.
   - Os metadados carregados para o servidor IDP estão corretos.
   - O endereço do controlador nos arquivos de metadados do SP está correto.

#### Passo 5: Ative o SAML

Sua etapa final é concluir a configuração SAML para autenticação de usuário. Durante esse processo, o sistema também solicita que você teste um login SSO. O processo de teste SSO Login é descrito na etapa anterior.

**Antes de começar**

- O arquivo de metadados de IDP é importado para o Unified Manager.
- Um arquivo de metadados do provedor de serviços para o controlador é importado para o sistema IDP para a relação de confiança.
- Pelo menos um mapeamento de função Monitor e um Admin de segurança está configurado.

**Edição e desativação.** Uma vez que o SAML está ativado, você *não pode* desabilitá-lo através da interface do usuário, nem pode editar as configurações de IDP. Se você precisar desativar ou editar a configuração SAML, entre em Contato com o suporte técnico para obter assistência.

**Passos**

1. Na guia **SAML**, selecione o link **Ativar SAML**.

   A caixa de diálogo confirmar ativação SAML é aberta.

2. Digite `enable`e clique em **Ativar**.
3. Insira as credenciais do usuário para um teste de login SSO.

**Resultados**

Depois que o sistema ativa o SAML, ele termina todas as sessões ativas e começa a autenticar usuários por meio do SAML.

### Alterar mapeamentos de função SAML

Se você configurou o SAML para Gerenciamento de Acesso anteriormente, poderá alterar os mapeamentos de função entre os grupos de IDP e as funções predefinidas do storage array.

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- Um administrador de IDP configurou atributos de usuário e associação de grupo no sistema de IDP.
- O SAML está configurado e ativado.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **SAML**.
3. Selecione **Mapeamento de função**.

   A caixa de diálogo Mapeamento de função é aberta.

4. Atribua atributos de usuário e grupos IDP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

   Tenha cuidado para não remover suas permissões enquanto o SAML estiver ativado ou você perderá o acesso ao Unified Manager.

**Detalhes do campo**

| Definição | Descrição |
| --- | --- |
| **Mapeamentos** | Atributo do utilizador |
| Especifique o atributo (por exemplo, "membro de") para o grupo SAML a ser mapeado. | Valor do atributo |
| Especifique o valor do atributo para o grupo a ser mapeado. | Funções |

> A função Monitor é necessária para todos os usuários, incluindo o administrador. O Unified Manager não funcionará corretamente para nenhum usuário sem a função Monitor presente.

5. Opcionalmente, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.
6. Clique em **Salvar**.

**Resultados**

Depois de concluir esta tarefa, todas as sessões ativas do utilizador são encerradas. Apenas a sessão de utilizador atual é mantida.

### Exporte arquivos do provedor de serviços SAML

Se necessário, você pode exportar metadados do provedor de serviços para o storage array e reimportar o arquivo para o sistema de provedor de identidade (IDP).

**Antes de começar**

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- O SAML está configurado e ativado.

**Sobre esta tarefa**

Nesta tarefa, você exporta metadados do controlador. O IDP precisa desses metadados para estabelecer uma relação de confiança com o controlador e processar solicitações de autenticação. O arquivo inclui informações como o nome de domínio do controlador ou endereço IP que o IDP pode usar para enviar solicitações.

**Passos**

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **SAML**.
3. Selecione **Exportar**.

   A caixa de diálogo Exportar ficheiros do fornecedor de serviços abre-se.

4. Clique em **Exportar** para salvar o arquivo de metadados no sistema local.

   O campo de nome de domínio é somente leitura.

   Anote onde o arquivo é armazenado.

5. No sistema local, localize o arquivo de metadados do provedor de serviços formatado em XML que você exportou.
6. No servidor IDP, importe o arquivo de metadados do provedor de serviços. Você pode importar o arquivo diretamente ou inserir manualmente as informações do controlador.
7. Clique em **Fechar**.

## FAQs

**Por que não consigo fazer login?**

Se receber um erro ao tentar iniciar sessão, reveja estas possíveis causas.

Erros de login podem ocorrer por um destes motivos:

- Introduziu um nome de utilizador ou uma palavra-passe incorretos.
- Você não tem Privileges suficiente.
- Tentou iniciar sessão sem sucesso várias vezes, o que acionou o modo de bloqueio. Aguarde 10 minutos para voltar a iniciar sessão.
- A autenticação SAML está ativada. Atualize seu navegador para fazer login.

**O que eu preciso saber antes de adicionar um servidor de diretório?**

Antes de adicionar um servidor de diretório no Gerenciamento de Acesso, você deve atender a certos requisitos.

- Os grupos de usuários devem ser definidos em seu serviço de diretório.
- As credenciais do servidor LDAP devem estar disponíveis, incluindo o nome de domínio, o URL do servidor e, opcionalmente, o nome de usuário e a senha da conta BIND.
- Para servidores LDAPS que usam um protocolo seguro, a cadeia de certificados do servidor LDAP deve ser instalada na sua máquina local.

**O que eu preciso saber sobre mapeamento para funções de storage array?**

Antes de mapear grupos para funções, revise as diretrizes.

Os recursos RBAC (controle de acesso baseado em função) incluem as seguintes funções:

- **Storage admin** — Acesso completo de leitura/gravação a objetos de armazenamento nas matrizes, mas sem acesso à configuração de segurança.
- **Security admin** — Acesso à configuração de segurança em Gerenciamento de Acesso e Gerenciamento de certificados.
- **Support admin** — Acesso a todos os recursos de hardware em matrizes de armazenamento, dados de falha e eventos mel. Sem acesso a objetos de armazenamento ou à configuração de segurança.

- **Monitor** — Acesso somente leitura a todos os objetos de armazenamento, mas sem acesso à configuração de segurança.

> A função Monitor é necessária para todos os usuários, incluindo o administrador.

Se estiver a utilizar um servidor LDAP (Lightweight Directory Access Protocol) e Serviços de diretório, certifique-se de que:

- Um administrador definiu grupos de usuários no serviço de diretório.
- Você conhece os nomes de domínio de grupo para os grupos de usuários LDAP.

#### SAML

Se você estiver usando os recursos de Security Assertion Markup Language (SAML) incorporados ao storage array, verifique se:

- Um administrador do Provedor de identidade (IDP) configurou atributos de usuário e associação de grupo no sistema IDP.
- Você conhece os nomes dos membros do grupo.
- Você sabe o valor do atributo para o grupo a ser mapeado. Expressões regulares são suportadas. Esses carateres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular:

```
\.[]{}()<>*+-=!?^$|
```

- A função Monitor é necessária para todos os usuários, incluindo o administrador. O Unified Manager não funcionará corretamente para nenhum usuário sem a função Monitor presente.

### O que eu preciso saber antes de configurar e ativar o SAML?

Antes de configurar e habilitar os recursos de Security Assertion Markup Language (SAML) para autenticação, certifique-se de atender aos requisitos a seguir e entender as restrições SAML.

#### Requisitos

Antes de começar, certifique-se de que:

- Um Provedor de identidade (IDP) está configurado na sua rede. Um IDP é um sistema externo usado para solicitar credenciais de um usuário e determinar se o usuário foi autenticado com êxito. Sua equipe de segurança é responsável por manter o IDP.
- Um administrador de IDP configurou atributos de usuário e grupos no sistema de IDP.
- Um administrador de IDP garantiu que o IDP suporta a capacidade de retornar um ID de nome na autenticação.
- Um administrador garantiu que o servidor IDP e o relógio do controlador são sincronizados (através de um servidor NTP ou ajustando as definições do relógio do controlador).
- Um arquivo de metadados IDP é baixado do sistema IDP e está disponível no sistema local usado para acessar o Unified Manager.

- Você sabe o endereço IP ou o nome de domínio do controlador na matriz de armazenamento.

#### Restrições

Além dos requisitos acima, certifique-se de que compreende as seguintes restrições:

- Uma vez que o SAML está ativado, você *não pode* desabilitá-lo através da interface do usuário, nem pode editar as configurações de IDP. Se você precisar desativar ou editar a configuração SAML, entre em Contato com o suporte técnico para obter assistência. Recomendamos que você teste os logins SSO antes de ativar o SAML na etapa final de configuração. (O sistema também executa um teste de login SSO antes de ativar o SAML.)
- Se você desabilitar o SAML no futuro, o sistema restaurará automaticamente a configuração anterior (funções de usuário local e/ou Serviços de diretório).
- Se os Serviços de diretório estiverem configurados atualmente para autenticação de usuário, o SAML substituirá essa configuração.
- Quando o SAML é configurado, os seguintes clientes não podem acessar os recursos do storage array:
  - Janela de gerenciamento empresarial (EMW)
  - Interface de linha de comando (CLI)
  - Clientes de Software Developer Kits (SDK)
  - Clientes na banda
  - Clientes API REST de Autenticação básica HTTP
  - Faça login usando o endpoint padrão da API REST

### Quais são os usuários locais?

Os usuários locais são predefinidos no sistema e incluem permissões específicas.

Os usuários locais incluem:

- **Admin** — Super administrador que tem acesso a todas as funções do sistema. Este usuário inclui todas as funções. A palavra-passe tem de ser definida no início de sessão pela primeira vez.
- **Storage** — o administrador responsável por todo o provisionamento de armazenamento. Esse usuário inclui as seguintes funções: Administrador de storage, administrador de suporte e monitor. Esta conta é desativada até que uma palavra-passe seja definida.
- **Segurança** — o usuário responsável pela configuração de segurança, incluindo Gerenciamento de Acesso e Gerenciamento de certificados. Este usuário inclui as seguintes funções: Admin de segurança e Monitor. Esta conta é desativada até que uma palavra-passe seja definida.
- **Suporte** — o usuário responsável por recursos de hardware, dados de falha e atualizações de firmware. Este usuário inclui as seguintes funções: Admin de suporte e Monitor. Esta conta é desativada até que uma palavra-passe seja definida.
- **Monitor** — Um usuário com acesso somente leitura ao sistema. Este utilizador inclui apenas a função Monitor. Esta conta é desativada até que uma palavra-passe seja definida.
- **rw** (leitura/gravação) — este usuário inclui as seguintes funções: Administrador de armazenamento, administrador de suporte e monitor. Esta conta é desativada até que uma palavra-passe seja definida.
- **Ro** (somente leitura) — este usuário inclui somente a função Monitor. Esta conta é desativada até que uma palavra-passe seja definida.

# Versões anteriores

Confira os links abaixo para acessar a documentação de versões anteriores do hardware e do software SANtricity do e-Series. Os links levam você a um site de documentação diferente.

## Documentação de hardware para versões anteriores

- "Instalar bandejas de unidades e controlador E2712, E2724, E5612, E5624 e bandejas de unidades de expansão DE1600 e DE5600"
- "Instalar bandejas de unidades e controlador E2760 e E5660 e bandejas de unidades de expansão DE6600"
- "Instalar flash arrays EF560 e DE5600 bandejas de expansão flash"
- "Instale sistemas mais antigos"
- "Manter sistemas mais antigos"
- "Adicione o segundo controlador ao E2600 e ao E2700"
- "Alterar ou adicionar protocolos de host"
- "Converter de alimentação CA para CC"

## Documentação de software para versões anteriores

### SANtricity versão 11,7

- "Ajuda do System Manager"
- "Ajuda do Unified Manager"

### SANtricity versão 11,6

- "Ajuda do System Manager"
- "Ajuda do Unified Manager"

### SANtricity versão 11,5

- "Ajuda do System Manager"

### SANtricity versão 11,4

- "AJUDA AMW (E2700, E5600/EF560)"
- "AJUDA DE EMW (E2700, E5600/EF560)"

# Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

## Direitos de autor

"https://www.netapp.com/company/legal/copyright/"

## Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respetivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

## Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

## Política de privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

## Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

"Aviso para o e-Series/EF-Series SANtricity os"

## Informações sobre direitos autorais



## Informações sobre marcas comerciais