SANtricity System Manager

SANtricity software

NetApp
March 17, 2026

This PDF was generated from https://docs.netapp.com/pt-br/e-series-santricity-119/sm-interface/overview-interface-sam.html on March 17, 2026. Always check docs.netapp.com for the latest.

Índice

Gerenciamento de array único com SANtricity System Manager 11.9 . . . 1
Interface principal . . . 1
Saiba mais sobre a interface SANtricity System Manager . . . 1
Ver dados de desempenho . . . 2
Visualizar a hierarquia de armazenamento no SANtricity System Manager . . . 11
Gerenciar configurações da interface . . . 13
Gerenciar notificações . . . 16
Perguntas frequentes sobre a interface de gerenciamento SANtricity System Manager . . . 20
Pools e grupos de volume . . . 24
Saiba mais sobre pools e grupos de volume no SANtricity System Manager . . . 24
Conceitos . . . 25
Configurar storage . . . 34
Gerenciar armazenamento . . . 46
Modificar configurações de pool e grupo . . . 52
Gerenciar cache SSD . . . 61
Gerenciar capacidade reservada . . . 68
Perguntas frequentes sobre pools e grupos de volume para SANtricity System Manager . . . 78
Volumes e cargas de trabalho . . . 91
Saiba mais sobre volumes e cargas de trabalho no SANtricity System Manager . . . 91
Conceitos . . . 92
Configurar storage . . . 110
Gerenciar volumes . . . 121
Gerenciar configurações . . . 126
Use os serviços de cópia . . . 136
Perguntas frequentes sobre volumes e cargas de trabalho para SANtricity System Manager . . . 143
Hosts e clusters de hosts . . . 148
Aprenda sobre hosts e clusters de hosts no SANtricity software . . . 148
Conceitos . . . 148
Configurar acesso ao host . . . 152
Gerenciar hosts e clusters . . . 157
Gerenciar configurações . . . 160
Perguntas frequentes sobre sistemas host e clusters de hosts para SANtricity System Manager . . . 163
Instantâneos . . . 167
Saiba mais sobre snapshots no SANtricity System Manager . . . 167
Conceitos . . . 168
Criar Snapshots e objetos de Snapshot . . . 179
Gerenciar agendamentos de Snapshot . . . 192
Gerenciar imagens de Snapshot . . . 194
Gerenciar grupos de consistência de Snapshot . . . 200
Gerenciar volumes de Snapshot . . . 204
Perguntas frequentes sobre Snapshots para SANtricity System Manager . . . 209
Espelhamento . . . 212
Visão geral . . . 212

Conceitos assíncronos . . . 214
Conceitos de sincronização . . . 225
Gerenciar grupos de consistência de espelhamento assíncrono . . . 234
Gerenciar pares espelhados assíncronos . . . 240
Gerenciar pares espelhados de sync . . . 244
Desativar espelhamento . . . 248
Perguntas frequentes sobre espelhamento assíncrono para SANtricity System Manager . . . 249
Perguntas frequentes sobre espelhamento síncrono para o SANtricity System Manager . . . 254
Armazenamento remoto . . . 258
Saiba mais sobre o recurso Remote Storage no SANtricity System Manager . . . 258
Conceitos . . . 259
Gerenciar armazenamento remoto . . . 263
Perguntas frequentes sobre storage remoto para SANtricity System Manager . . . 267
Componentes de hardware . . . 270
Visualize e gerencie componentes de hardware no SANtricity System Manager . . . 270
Informações relacionadas . . . 270
Conceitos . . . 270
Gerenciar componentes de prateleira . . . 281
Gerenciar controladores . . . 286
Gerenciar portas iSCSI . . . 298
Gerenciar portas NVMe . . . 309
Gerenciar unidades . . . 314
Gerenciar hot spares . . . 327
Perguntas frequentes sobre compartimentos de armazenamento para SANtricity System Manager . . . 330
Perguntas frequentes sobre o controlador de storage para SANtricity System Manager . . . 333
Perguntas frequentes sobre o protocolo iSCSI para o SANtricity System Manager . . . 336
Perguntas frequentes do protocolo NVMe para SANtricity System Manager . . . 338
Perguntas frequentes sobre storage drives para SANtricity System Manager . . . 340
Alertas . . . 341
Saiba mais sobre alertas no SANtricity System Manager . . . 341
Conceitos . . . 342
Gerenciar alertas de email . . . 344
Gerenciar alertas SNMP . . . 347
Gerenciar alertas do syslog . . . 355
Perguntas frequentes sobre alertas do storage system para SANtricity System Manager . . . 357
Configurações do array . . . 357
Saiba mais sobre a visão geral das configurações no SANtricity System Manager . . . 357
Conceitos . . . 358
Configurar configurações do array . . . 361
Configurar recursos adicionais . . . 367
Baixe a interface de linha de comando (CLI) do SANtricity . . . 371
Perguntas frequentes sobre as configurações do array de storage para SANtricity System Manager . . . 371
Segurança de unidade . . . 374
Saiba mais sobre segurança de unidades em SANtricity System Manager . . . 374
Conceitos . . . 375

Configurar chaves de segurança . . . 379
Gerenciar chaves de segurança . . . 383
Perguntas frequentes sobre segurança de storage drive para SANtricity System Manager . . . 391
Gerenciamento de acesso . . . 394
Saiba mais sobre controle de acesso no SANtricity System Manager . . . 394
Conceitos . . . 395
Use funções de usuário locais . . . 402
Use os serviços de diretório . . . 404
Usar SAML . . . 414
Use tokens de acesso . . . 421
Gerenciar syslog . . . 423
Perguntas frequentes sobre gerenciamento de acesso de usuário para SANtricity System Manager . . . 429
Certificados . . . 433
Saiba mais sobre certificados no SANtricity System Manager . . . 433
Conceitos . . . 434
Usar certificados . . . 437
Perguntas frequentes sobre certificados assinados por CA e autoassinados para SANtricity System Manager . . . 446
Suporte . . . 447
Obtenha suporte no SANtricity System Manager . . . 447
Visualizar informações e diagnósticos . . . 447
Coletar dados de diagnóstico . . . 452
Adote medidas de recuperação . . . 456
Gerenciar AutoSupport . . . 458
Ver eventos . . . 464
Gerenciar atualizações . . . 468
AutoSupport FAQ para SANtricity System Manager . . . 480

Gerenciamento de array único com SANtricity System Manager 11.9

Interface principal

Saiba mais sobre a interface SANtricity System Manager

SANtricity System Manager é uma interface Web que permite gerenciar um array de storage em uma única visualização.

Página inicial

A página inicial fornece uma visão geral do painel de controle para o gerenciamento diário do seu array de storage. Ao fazer login no System Manager, a página inicial é a primeira tela exibida.

O painel de controle é composto por quatro áreas de resumo que contêm informações importantes sobre o estado e a integridade do seu array de storage. Você pode encontrar mais informações na área de resumo.

Área	Descrição
Notificações	A área de Notificações exibe notificações de problemas que indicam o status do array de storage e seus componentes. Além disso, este portlet exibe alertas automatizados que podem ajudar você a solucionar problemas antes que eles afetem outras áreas do seu ambiente de storage.
Desempenho	A área Desempenho permite comparar e contrastar o uso de recursos ao longo do tempo. Você pode visualizar as métricas de desempenho do array de storage para tempo de resposta (IOPS), taxas de transferência (MiB/s) e a quantidade de capacidade de processamento utilizada (CPU).
Capacidade	A área Capacidade exibe um gráfico com a capacidade alocada, capacidade de storage livre e capacidade de storage não atribuída em seu array de storage.
Hierarquia de armazenamento	A área Hierarquia de Armazenamento fornece uma visão organizada dos vários componentes de hardware e objetos de storage gerenciados pelo seu array de storage. Clique na seta suspensa para executar uma determinada ação nesse componente de hardware ou objeto de storage.

Configurações de interface

Você pode alterar as preferências de exibição e outras configurações na interface principal.

Configuração	Descrição
Preferências de exibição	Altere os valores de capacidade e o período de tempo no menu suspenso Preferências no canto superior direito da interface.

Configuração	Descrição
Tempo limite da sessão	Configure os tempos limite para que as sessões inativas dos usuários sejam desconectadas após um tempo especificado.
Ajuda	Acesse a documentação de ajuda e outros recursos no menu suspenso no canto superior direito da interface.

Logins e senhas de usuário

O usuário atualmente conectado ao sistema é exibido no canto superior direito da interface.

Para obter mais informações sobre usuários e senhas, consulte:

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

Ver dados de desempenho

${post_edited_translations.segment}

A página de Performance oferece maneiras fáceis de monitorar o desempenho do seu array de storage.

${post_edited_translations.segment}

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

Saiba mais:

- "${post_edited_translations.segment}"
- "Termos de desempenho"

Como posso visualizar dados de desempenho?

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

Saiba mais:

- "Visualizar dados gráficos de desempenho"
- "Visualize e salve dados tabulares de desempenho"
- "Interpretar dados de desempenho"

Saiba mais sobre gráficos de desempenho e diretrizes no SANtricity System Manager

A página de Desempenho fornece gráficos e tabelas de dados que permitem avaliar o desempenho do array de storage em diversas áreas importantes.

As funções de desempenho permitem que você realize estas tarefas:

- Visualize dados de desempenho em tempo quase real para ajudá-lo a determinar se um array de storage está apresentando problemas.
- Exporte dados de desempenho para construir uma visão histórica de um array de storage e identificar quando um problema começou ou o que causou um problema.
- Selecione os objetos, métricas de desempenho e o período que deseja visualizar.
- Compare métricas.

Você pode visualizar os dados de desempenho em três formatos:

- **Gráfico em tempo real** — Exibe dados de desempenho em um gráfico quase em tempo real.
- **Tabela quase em tempo real** — Lista 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 posteriores.

Características 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
Gráficos em tempo real, ao vivo Gráfico em tempo real, histórico	10 seg (ao vivo) 5 min (histórico) Os pontos de dados exibidos dependem do período de tempo selecionado	O período de tempo padrão é de 1 hora. Opções: • 5 minutos • 1 hora • 8 horas • 1 dia • 7 dias • 30 dias	5	Não
Visualização tabular (tabela) em tempo quase real	10 segundos - 1 hora	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 desativá-la.
- Cada vez que o intervalo de amostragem se encerra, o array de storage é consultado e os dados são atualizados.

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

Aprenda sobre a terminologia de desempenho no SANtricity software

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

Termo	Descrição
Aplicativo	Um aplicativo é um programa de software, como SQL ou Exchange.
CPU	CPU é a abreviação de "unidade central de processamento". CPU indica a porcentagem da capacidade de processamento do array de storage que está sendo utilizada.
Host	Um host é um servidor que envia I/O para um volume em um array de storage.
IOPS	IOPS significa operações de entrada/saída por segundo.
Latência	Latência é o intervalo de tempo entre uma solicitação, como um comando de leitura ou gravação, e a resposta do host ou do array de storage.
LUN	Um número de unidade lógica (LUN, na sigla em inglês) é o número atribuído ao espaço de endereçamento que um host usa para acessar um volume. O volume é apresentado ao host como capacidade na forma de um LUN. Cada host possui seu próprio espaço de endereçamento LUN. Portanto, o mesmo LUN pode ser usado por diferentes hosts para acessar volumes diferentes.
MiB	MiB é a abreviação de mebibyte (mega binary byte). Um MiB equivale a 2^{20}, ou 1.048.576 bytes. Compare com MB, que representa um valor na base 10. Um MB equivale a 1.024 bytes.
Objeto	Um objeto é qualquer componente de armazenamento lógico ou storage físico. Os objetos lógicos incluem grupos de volumes, pools e volumes. Os objetos físicos incluem o array de storage, os controladores de array, os hosts e as unidades.

Termo	Descrição
Pool	Um pool é um conjunto de unidades agrupadas 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 volume.)
Ler	Read é a abreviação de "operação de leitura", que ocorre quando o host solicita dados do array de storage.
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 array de storage. Um volume é criado a partir da capacidade disponível em um pool ou um grupo de volume. 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	O nome de um volume é uma sequência de caracteres atribuída ao volume no momento de sua criação. Você pode aceitar o nome padrão ou fornecer um nome mais descritivo que indique o tipo de dados armazenados no volume.
Grupo de volume	Um grupo de volume é um contêiner para volumes com características compartilhadas. Um grupo de volume tem uma capacidade definida e nível RAID. Você pode usar um grupo de volume para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um grupo de volume ou de um pool.)
Carga de trabalho	Uma carga de trabalho é um objeto de storage que suporta uma aplicação. Você pode definir uma ou mais cargas de trabalho, ou instâncias, por aplicação. Para algumas aplicações, o sistema configura a carga de trabalho para conter volumes com características subjacentes semelhantes. Essas características de volume são otimizadas com base no tipo de aplicação que a carga de trabalho suporta. Por exemplo, se você criar uma carga de trabalho que suporte uma aplicação Microsoft SQL Server e, posteriormente, criar volumes para essa carga de trabalho, as características subjacentes do volume serão otimizadas para suportar Microsoft SQL Server.
Escrever	Write é a abreviação de "operação de gravação", quando os dados são enviados do host para o array para armazenamento.

Visualize dados gráficos de desempenho no SANtricity System Manager

Você pode visualizar dados gráficos de desempenho para objetos lógicos, objetos físicos, aplicações e cargas de trabalho.

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 como Live updating, distingue dados históricos de dados em tempo real.

Visualização da home page

A página inicial contém um gráfico que mostra o desempenho do array de storage. Você pode selecionar métricas limitadas nessa visualização ou clicar em **Exibir detalhes de desempenho** para selecionar todas as métricas disponíveis.

Visão detalhada

Os gráficos disponíveis na visualização detalhada de desempenho estão organizados em três abas:

- **Visão Lógica** — Exibe dados de desempenho para objetos lógicos agrupados por grupos de volumes e pools. Objetos lógicos incluem grupos de volumes, pools e volumes.
- **Visão Física** — Exibe dados de desempenho para o controlador, canais do host, canais de drive e drives.
- **Visualização de Applications & Workloads** — Exibe uma lista de objetos lógicos (volumes) agrupados pelos tipos de aplicação e cargas de trabalho que você definiu.

Passos

1. Selecione **Home**.
2. Para selecionar uma visualização em nível de array, clique no botão IOPS, MiB/s ou CPU.
3. Para ver mais detalhes, clique em **View Performance Details**.
4. Selecione a guia **Logical View**, a guia **Physical View** ou a guia **Applications & Workloads View**.

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

Exibir abas	Dados de desempenho exibidos para cada tipo de objeto
Visão lógica	• **array de storage**: IOPS, MiB/s • **Pools**: Latência, IOPS, MiB/s • **Grupos de volume**: Latência, IOPS, MiB/s • **Volumes**: latência, IOPS, MiB/s
Vista física	• **Controladores**: IOPS, MiB/s, CPU, Headroom • **Canais do host**: Latência, IOPS, MiB/s, Headroom • **Drive channels**: Latência, IOPS, MiB/s • **Drives**: Latência, IOPS, MiB/s
Visualização de Applications & Workloads	• **array de storage**: IOPS, MiB/s • **Aplicações**: latência, IOPS, MiB/s • **Cargas de trabalho**: latência, IOPS, MiB/s • **Volumes**: latência, IOPS, MiB/s

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

Opções

Opções para visualizar objetos	Descrição
Expanda uma gaveta para ver a lista de objetos.	As gavetas de navegação contêm objetos de armazenamento, como pools, grupos de volume e unidades. Clique na gaveta para visualizar a lista de objetos na gaveta.
Selecione objetos para visualizar.	Selecione a caixa de seleção à esquerda de cada objeto para escolher os dados de desempenho que você deseja visualizar.
Use Filter para encontrar nomes de objetos ou nomes parciais.	Na caixa Filter, insira o nome ou parte do nome de objetos para listar apenas esses objetos na gaveta.
Clique em **Atualizar gráficos** após selecionar objetos.	Após selecionar objetos nas gavetas, selecione **Atualizar Gráficos** para visualizar dados gráficos dos itens que você selecionou.
Ocultar ou mostrar gráfico	Selecione o título do gráfico para ocultar ou mostrar o gráfico.

6. Se necessário, utilize as opções adicionais para visualizar os dados de desempenho.

Opções adicionais

Opção	Descrição
Período de tempo	Selecione o período de tempo que deseja visualizar (5 minutos, 1 hora, 8 horas, 1 dia, 7 dias ou 30 dias). O padrão é 1 hora. O carregamento de dados de desempenho para um período de 30 dias pode levar vários minutos. Não saia da página da web, não atualize a página da web nem feche o navegador enquanto os dados estiverem 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 rolagem	Use a barra de rolagem abaixo do gráfico para visualizar um período anterior ou posterior.
Barra de zoom	Abaixo do gráfico, arraste as alças da barra de zoom para diminuir o zoom em um intervalo de tempo. Quanto mais larga a barra de zoom, menos granulares serão os detalhes do gráfico. Para redefinir o gráfico, selecione uma das opções de período de tempo.
Arraste e solte	No gráfico, arraste o cursor de um ponto no tempo para outro para ampliar um intervalo de tempo. Para redefinir o gráfico, selecione uma das opções de período de tempo.

Visualize e salve dados tabulares de desempenho no SANtricity System Manager

Você pode visualizar e salvar dados de gráficos de desempenho em formato tabular. Isso permite filtrar os dados que deseja exibir.

Passos

1. De qualquer gráfico de dados de desempenho, clique em **Launch table view**.

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

2. Use o menu suspenso de seleção de objetos e o filtro conforme necessário.
3. Clique no botão **Mostrar/Ocultar Colunas** para selecionar as colunas que você deseja incluir na tabela.

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

4. Selecione **Export** na parte inferior da tela para salvar a visualização 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 do 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 seu navegador, o arquivo é salvo ou você é solicitado a escolher um nome e um 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 desempenho no SANtricity System Manager

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

Ao interpretar os dados de desempenho, lembre-se de que diversos fatores afetam o desempenho do seu array de storage. A tabela a seguir descreve as principais áreas a considerar.

Dados de desempenho	Implicações para ajuste de desempenho
Latência (milissegundos ou ms)	Monitore a atividade de I/O de um objeto específico. Identifique objetos que são potencialmente gargalos: • Se um grupo de volume for compartilhado entre vários volumes, os volumes individuais podem precisar de seus próprios grupos de volume para melhorar o desempenho sequencial das unidades e diminuir a latência. • Com pools, são introduzidas latências maiores e podem existir cargas de trabalho desiguais entre as unidades, tornando os valores de latência menos significativos e, em geral, mais altos. • O tipo e a velocidade da unidade influenciam a latência. Com E/S aleatória, unidades com rotação mais rápida passam menos tempo se movendo entre diferentes locais do disco. • 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. • Entradas/saídas maiores apresentam maior latência devido ao tempo adicional envolvido com a transferência de dados. • Latência mais alta pode indicar que o padrão de E/S é aleatório. Unidades com E/S aleatória terão maior latência do que aquelas com fluxos sequenciais. • Uma disparidade na latência entre unidades ou volumes de um grupo de volume comum pode indicar uma unidade lenta.

Dados de desempenho	Implicações para ajuste de desempenho
IOPS	Fatores que afetam as operações de entrada/saída por segundo (IOPS ou IOs/sec) incluem estes itens: • Padrão de acesso (aleatório ou sequencial) • Tamanho de E/S • Nível RAID • Tamanho do bloco de cache • Se o armazenamento em cache está ativado • Se o armazenamento em cache está ativado • Pré-busca de leitura de cache dinâmico • Tamanho do segmento • O número de unidades nos grupos de volumes ou array de storage Quanto maior a taxa de acerto do cache, maiores serão as taxas de E/S. Taxas de E/S de gravação mais altas são observadas com armazenamento em cache ativado em comparação com desativado. Ao decidir se deve ativar o armazenamento em cache de gravação para um volume individual, observe o IOPS atual e o IOPS máximo. Você deve observar 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. É possível observar melhorias de desempenho causadas pela alteração do tamanho do segmento nas estatísticas de IOPS de um volume. Faça testes para determinar o tamanho ideal do segmento ou utilize o tamanho do sistema de arquivos ou o tamanho do bloco do banco de dados.
MiB/s	As taxas de transferência ou throughput são determinadas pelo tamanho da E/S da aplicação e pela taxa de E/S. Geralmente, solicitações de E/S pequenas resultam em uma taxa de transferência mais baixa, mas proporcionam uma taxa de E/S mais rápida e um tempo de resposta mais curto. Com solicitações de E/S maiores, taxas de throughput mais altas são possíveis. Compreender os padrões típicos de E/S da sua aplicação pode ajudá-lo a determinar as taxas máximas de transferência de E/S para um array de storage específico.

Dados de desempenho	Implicações para ajuste de desempenho
CPU	Esse valor é uma porcentagem da capacidade de processamento que está sendo utilizada. Você pode notar uma disparidade no uso da CPU de objetos do mesmo tipo. Por exemplo, o uso da CPU de um controlador é alto ou está aumentando com o tempo, enquanto o de outro controlador é mais baixo ou mais estável. Nesse caso, você pode querer alterar a propriedade do controlador de um ou mais volumes para o controlador com a menor porcentagem de CPU. Você pode querer monitorar a CPU em todo o array de storage. Se a CPU continuar aumentando ao longo do tempo enquanto o desempenho do aplicativo diminui, talvez seja necessário adicionar arrays de storage. Ao adicionar arrays de storage à sua empresa, você pode continuar atendendo às necessidades do aplicativo com um nível de desempenho aceitável.
Margem	A margem de segurança refere-se à capacidade de desempenho restante dos controladores, dos canais de host do controlador e dos canais de acionamento do controlador. Esse valor é expresso em porcentagem e representa a diferença entre o desempenho máximo possível que esses objetos são capazes de fornecer e os níveis de desempenho atuais. • Para os controladores, a margem de segurança é uma porcentagem do máximo possível de IOPS. • Para os canais, a margem de segurança é uma porcentagem da taxa de transferência máxima, ou MiB/s. A taxa de transferência de leitura, a taxa de transferência de gravação e a taxa de transferência bidirecional estão incluídas no cálculo.

Visualizar a hierarquia de armazenamento no SANtricity System Manager

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

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

Componentes físicos

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

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

Componente	Descrição
Compartimento	Um shelf é um compartimento instalado em um gabinete ou rack. Ele contém os componentes de hardware para o array de storage. Existem dois tipos de shelf: um controller shelf e um drive shelf. Um controller shelf inclui controladores e unidades. Um drive shelf inclui módulos de entrada/saída (IOMs) e unidades. Se o seu array de storage contiver diferentes tipos de mídia ou diferentes tipos de interface, uma gaveta de unidades para cada tipo de unidade será exibida.
Drive	Um drive é um dispositivo mecânico eletromagnético ou um dispositivo de memória de estado sólido que fornece o storage físico para os dados.
Host	Um host é um servidor que envia I/O para um volume em um array de storage.
Adaptador de barramento de host (HBA)	Um adaptador de barramento de host (HBA, na sigla em inglês) é uma placa que reside em um host e contém uma ou mais portas de host.
Porta do 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 I/O.
Cliente de gerenciamento	Um cliente de gerenciamento é o computador onde um navegador está instalado para acessar System Manager.

Componentes lógicos

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

Componente	Descrição
Pool	Um pool é um conjunto de unidades agrupadas 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 volume.)
Grupo de volume	Um grupo de volume é um contêiner para volumes com características compartilhadas. Um grupo de volume tem uma capacidade definida e nível RAID. Você pode usar um grupo de volume para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um grupo de volume 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 array de storage.

Componente	Descrição
Unidade lógica (LUN)	Um número de unidade lógica (LUN, na sigla em inglês) é o número atribuído ao espaço de endereçamento que um host usa para acessar um volume. O volume é apresentado ao host como capacidade na forma de um LUN. Cada host possui seu próprio espaço de endereçamento LUN. Portanto, o mesmo LUN pode ser usado por diferentes hosts para acessar volumes diferentes.

Gerenciar configurações da interface

Gerenciar a proteção por senha no SANtricity System Manager

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

Definir e alterar senhas

Ao iniciar System Manager pela primeira vez, você será solicitado a definir uma senha de administrador. Qualquer usuário que possua a senha de administrador pode fazer alterações de configuração no array de storage, como adicionar, alterar ou remover objetos ou configurações. Para definir a senha de administrador durante a inicialização, consulte "Acesse o System Manager".

Por motivos de segurança, você só pode tentar inserir uma senha cinco vezes antes que o array de storage entre em estado de "bloqueio". Nesse estado, o array de storage rejeitará as tentativas subsequentes de senha. Você deve aguardar 10 minutos para que o array de storage retorne ao estado "normal" antes de tentar inserir uma senha novamente.

Além da senha de administrador, o array de storage inclui perfis de usuário predefinidos com uma ou mais funções mapeadas a eles. Para obter mais informações, consulte "Permissões para funções mapeadas". Os perfis de usuário e os mapeamentos não podem ser alterados. Somente as senhas podem ser modificadas. Se você deseja alterar a senha de administrador ou outras senhas de usuário, consulte "Alterar senhas".

Digite novamente as senhas após o término da sessão

O sistema solicita a senha apenas uma vez durante uma sessão de gerenciamento. No entanto, uma sessão expira após 30 minutos de inatividade, momento em que você deve inserir a senha novamente. Se outro usuário gerenciando o mesmo array de storage a partir de outro cliente de gerenciamento alterar a senha enquanto sua sessão estiver em andamento, você será solicitado a inserir a senha na próxima vez que tentar realizar uma operação de configuração ou de visualização.

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

Remover unidades ou proteção por senha

Se você remover unidades protegidas por senha ou quiser desativar a proteção por senha, esteja ciente do seguinte:

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

storage.

- **Se desejar remover a proteção por senha** — Se não quiser mais que os comandos sejam protegidos por senha, digite a senha de administrador atual e deixe as caixas de texto da nova senha em branco.

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

Definir as unidades padrão para os valores de capacidade no SANtricity System Manager

SANtricity System Manager pode exibir valores de capacidade em gibibytes (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 o menu: Preferências [Definir preferências].
2. Clique no botão de opção para **Gibibytes** ou **Tebibytes** e confirme que deseja realizar a operação.

   Consulte a tabela a seguir para abreviações e valores.

Abreviação	Valor
GiB	1.024^3 bytes
TiB	1.024^4 bytes

Defina o período de tempo padrão para os gráficos de desempenho no SANtricity System Manager

Você pode alterar o período de tempo padrão exibido nos gráficos de desempenho.

Sobre esta tarefa

Os gráficos de desempenho exibidos na página inicial e na página de desempenho mostram inicialmente um período de 1 hora. As preferências são armazenadas no armazenamento local do navegador, assim todos os usuários podem ter suas próprias configurações.

Passos

1. Selecione o menu: Preferências [Definir preferências].
2. Na lista suspensa, selecione **5 minutos**, **1 hora**, **8 horas**, **1 dia** ou **7 dias** e confirme que você deseja realizar a operação.

Configurar o banner de login no SANtricity System Manager

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

Sobre esta tarefa

Ao criar um banner, ele aparece antes da tela de login em uma caixa de diálogo.

Passos

1. Selecione o menu: configurações [Sistema].
2. Na seção Geral, selecione **Configurar Login Banner**.

   A caixa de diálogo Configurar Login Banner é aberta.

3. Digite o texto que você deseja que apareça no banner de login.

   Não utilize tags HTML ou outras tags de margem de lucro 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 os tempos limite de sessão no SANtricity System Manager

É possível configurar tempos limite no SANtricity System Manager, para que as sessões inativas dos usuários sejam desconectadas após um período especificado.

Sobre esta tarefa

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

Se o Access Management estiver configurado usando os recursos de Security Assertion Markup Language (SAML) incorporados no array, pode ocorrer um tempo limite de sessão 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 o menu: configurações [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. Use os controles giratórios para aumentar ou diminuir o tempo em minutos.

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

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

4. Clique em **Salvar**.

Gerenciar notificações

Saiba mais sobre as notificações de problemas do SANtricity System Manager

SANtricity System Manager usa ícones e vários outros métodos para notificá-lo de que existem problemas com o array de storage.

Ícones

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

Ícone	Descrição
	Ideal
	Não ideal ou com falha
	Precisa de atenção ou reparos
	Cuidado

System Manager exibe esses ícones em vários locais.

- A área de Notifications na página inicial exibe o ícone de falha e uma mensagem.
- O ícone da Home page na área de navegação exibe o ícone de falha.
- Na página Componentes, os gráficos para unidades e controladores exibem o ícone de falha.

Alertas e LEDs

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

- System Manager envia notificações SNMP ou mensagens de erro por email.
- Os LEDs de Service Action Required no hardware acendem.

Ao receber uma notificação de problema, utilize o Recovery Guru para ajudá-lo a resolver o problema. Quando necessário, utilize a documentação do hardware com os passos de recuperação para substituir os componentes com falha.

Visualize e tome medidas em operações em andamento no SANtricity System Manager

Para visualizar e tomar medidas em operações de longa duração, utilize a página Operações em progresso.

Sobre esta tarefa

Para cada operação listada na página Operações em Andamento, são exibidos a porcentagem de conclusão e o tempo estimado restante para concluir a operação. Em alguns casos, você pode interromper uma operação ou atribuir a ela uma prioridade maior ou menor. Você também pode remover 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 Actions para interromper ou alterar a prioridade de uma operação.

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

   Você pode interromper uma operação de cópia de volume ou alterar sua prioridade.

3. Após a conclusão de uma operação de cópia de volume, você pode selecionar **Limpar** para removê-la da lista.

   Na parte superior da página inicial, uma mensagem informativa e um ícone de chave inglesa amarela aparecem quando uma operação é concluída. Essa mensagem inclui um link que permite limpar a operação da página Operações em Andamento.

As operações que aparecem na página Operações em Andamento incluem as seguintes:

Operação	Possível status da operação	Ações que você pode tomar
Cópia de volume	Concluído	Limpar
Cópia de volume	Em andamento	• Alterar prioridade • Parar
Cópia de volume	Pendente	Limpar
Cópia de volume	Falha	• Limpar • Recopiar
Cópia de volume	Parado	• Limpar • Recopiar
Criar volume (somente volumes de pool espesso maiores que 64TiB)	Em andamento	*none*
Exclusão de volume (somente volumes de pool espesso maiores que 64TiB)	Em andamento	*none*
Sincronização inicial do grupo de espelhamento assíncrono	Em andamento	Suspender
Sincronização inicial do grupo de espelhamento assíncrono	Suspenso	Retomar

Operação	Possível status da operação	Ações que você pode tomar
Espelhamento síncrono	Em andamento	Suspender
Espelhamento síncrono	Suspenso	Retomar
Reverter imagem de Snapshot	Em andamento	Cancelar
Reverter imagem de Snapshot	Pendente	Cancelar
Reverter imagem de Snapshot	Pausado	• Cancelar • Retomar
Evacuação de unidade	Em andamento	Cancelar (depende do tipo de evacuação da unidade)
Adicionar capacidade ao pool ou volume group	Em andamento	*none*
Alterar um nível RAID de um volume	Em andamento	*none*
Reduzir a capacidade de um pool	Em andamento	*none*
Reclamação de volume thin	Em andamento	*none*
Verifique o tempo restante em uma operação de formato de disponibilidade instantânea (IAF) para volumes de pool	Em andamento	*none*
Verifique a redundância de dados de um grupo de volume	Em andamento	*none*
Desfragmentar um grupo de volume	Em andamento	*none*
Inicializar um volume	Em andamento	*none*
Aumentar a capacidade de um volume	Em andamento	*none*
Alterar o tamanho do segmento de um volume	Em andamento	*none*
Cópia de drive	Em andamento	*none*

Operação	Possível status da operação	Ações que você pode tomar
Reconstrução de dados	Em andamento	*none*
Copyback	Em andamento	*none*
Apagar unidade	Em andamento	*none*
Importação de storage remoto	Em andamento	• Alterar prioridade • Parar
Importação de storage remoto	Parado	• Retomar • Desconectar
Importação de storage remoto	Falha	• Retomar • Desconectar
Importação de storage remoto	Concluído	Desconectar

Recupere-se de problemas usando o SANtricity System Manager Recovery Guru

O Recovery Guru é um componente do SANtricity System Manager que diagnostica problemas no array de storage e recomenda procedimentos de recuperação para corrigi-los.

Passos

1. Selecione **Home**.
2. Clique no link com a etiqueta **Recuperar de *n* problemas** no centro-topo da janela.

   A caixa de diálogo Recovery Guru é exibida.

3. Selecione o primeiro problema exibido na lista de resumo e siga as instruções do procedimento de recuperação para corrigir o problema. Onde necessário, utilize as instruções de substituição para substituir os componentes com falha. Repita esta etapa para cada problema listado.

   Vários problemas em um array de storage podem estar relacionados. Nesse 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.

   Múltiplas falhas em um compartimento da fonte de alimentação são agrupadas e listadas como um único problema na lista de resumo. Múltiplas falhas em um compartimento do ventilador também são listadas como um único problema.

4. Para garantir que o procedimento de recuperação foi bem-sucedido, clique em **Recheck**.

   Se você selecionou um problema para um grupo de espelhamento assíncrono ou um membro de um grupo de espelhamento assíncrono, clique em **Limpar** primeiro para limpar a falha do controlador e, em seguida, clique em **Verificar novamente** para remover o evento do Recovery Guru.

Se todos os problemas forem corrigidos, o ícone do array de storage eventualmente mudará de "Precisa de Atenção" para "Ideal". Para alguns problemas, um ícone "Corrigindo" aparece enquanto uma operação, como reconstrução, está em andamento.

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

   O arquivo é salvo na pasta Downloads do seu 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**.

Perguntas frequentes sobre a interface de gerenciamento SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

Quais são os navegadores compatíveis?

SANtricity System Manager é compatível com estas versões de 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 SANtricity System Manager usando apenas o teclado.

Navegação geral

Ação	Atalho de teclado
Passe para o próximo item.	Aba
Mover para o item anterior.	Shift + Tab
Selecione um item.	Digite
Lista suspensa—Mover para o item seguinte ou anterior.	Seta para baixo ou seta para cima
Caixa de seleção—Selecione um item.	Barra de espaço

Ação	Atalho de teclado
Botões de opção—Alternam entre os itens.	Seta para baixo ou seta para cima
Texto expansível—Expandir ou contrair item.	Digite

Navegação na tabela

Ação	Atalho de teclado
Selecione uma linha.	Use a tecla Tab para selecionar uma linha e, em seguida, pressione Enter
Role para cima ou para baixo.	Seta para baixo/seta para cima ou Page Down/Page Up
Altere a ordem de classificação de uma coluna.	Use a tecla Tab para selecionar um cabeçalho de coluna e, em seguida, pressione Enter

Navegação no calendário

Ação	Atalho de teclado
Ir para o mês anterior.	Page Up
Ir para o próximo mês.	Page Down
Ir para o ano anterior.	Ctrl + Page Up
Passe para o próximo ano.	Ctrl + Page Down
Abra o seletor de datas se estiver fechado.	Control + Início
Mover para o mês atual.	Control / Command + Home
Mover para o dia anterior.	Control / Command + Esquerda
Passe para o dia seguinte.	Control / Command + Direita
Vá para a semana anterior.	Control/Command + Up
Passe para a próxima semana.	Control / Command + Baixo
Selecione a data focalizada.	Digite
Feche o seletor de datas e apague a data.	Control / Command + End

Ação	Atalho de teclado
Feche o seletor de datas sem seleção.	Escapar

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

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

A capacidade reservada é usada internamente pelo sistema de storage para suportar volumes finos, snapshots e espelhamento assíncrono, e não é visível para os hosts de E/S. Como resultado, as estatísticas do pool, do controlador e do array de storage podem não corresponder à soma dos volumes visíveis.

No entanto, para estatísticas de aplicativos 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 valor zero é exibido para um ponto de dados nos gráficos e na tabela, significa que não há atividade de E/S para o objeto naquele 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 exibirão dados diferentes de zero assim que a atividade de I/O começar a ocorrer para o objeto.

A tabela a seguir lista os motivos mais comuns pelos quais o valor de um ponto de dados pode ser zero para qualquer objeto.

Tipo de objeto em nível de array	Motivo dos dados exibidos como zero
Volume	• O volume não tinha atribuição de host.
Grupo de volume	• O grupo de volume está sendo importado. • O grupo de volumes não contém um volume atribuído a um host, ***e*** o grupo de volumes não contém nenhuma capacidade reservada.
Drive	• A unidade falhou. • A unidade foi removida. • A unidade está em um estado desconhecido.
Controlador	• Controlador está offline. • Controladora falhou. • O controlador foi removido. • Controlador está em um estado desconhecido.
Array de storage	• O array de storage 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 volume, pools, aplicativos e cargas de trabalho. Este gráfico aparece nas guias Visualização Lógica, Visualização Física e Visualização de Aplicativos e Cargas de Trabalho.

Latência refere-se a qualquer atraso que ocorre durante a leitura ou gravação de dados. Passe o cursor sobre um ponto no gráfico para visualizar os seguintes valores, em milissegundos (ms), para aquele ponto no tempo:

- Tempo de leitura.
- Tempo de gravação.
- Tamanho médio de I/O.

O que o gráfico de IOPS mostra?

O gráfico de IOPS exibe estatísticas de operações de entrada/saída por segundo. Na página inicial, este gráfico exibe estatísticas para o array de storage. Nas guias Visualização Lógica, Visualização Física e Visualização de Aplicativos e Cargas de Trabalho do bloco Desempenho, este gráfico exibe estatísticas para o array de storage, volumes, grupos de volumes, pools, aplicativos e cargas de trabalho.

IOPS é a abreviação de *operações de entrada/saída (I/O) por segundo*. Passe o cursor sobre um ponto no gráfico para visualizar os seguintes valores para aquele ponto no tempo:

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

O que o gráfico de 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 o array de storage. Nas guias Visualização Lógica, Visualização Física e Visualização de Aplicativos e Cargas de Trabalho do bloco Desempenho, este gráfico exibe estatísticas para o array de storage, volumes, grupos de volumes, pools, aplicativos e cargas de trabalho.

MiB/s é a abreviação de *mebibytes por segundo*, ou 1.048.576 bytes por segundo. Posicione o cursor sobre um ponto no gráfico para visualizar os seguintes valores para aquele ponto no tempo:

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

O que o gráfico de CPU mostra?

O gráfico da CPU exibe estatísticas de capacidade de processamento para cada controlador (controlador A e controlador B). CPU é uma abreviação de *central processing unit*. Na página inicial, este gráfico exibe estatísticas para o array de storage. Na guia Visualização Física do bloco Desempenho, este gráfico exibe estatísticas para o array de storage e as unidades.

O gráfico da CPU mostra a porcentagem da capacidade de processamento da CPU sendo utilizada em relação às operações no array. Mesmo quando nenhuma E/S externa está ocorrendo, a porcentagem de utilização de CPU pode ser diferente de zero, pois o sistema operacional de storage pode estar executando

operações em segundo plano e realizando monitoramento. Posicione o cursor sobre um ponto no gráfico para visualizar uma porcentagem da capacidade de processamento sendo utilizada naquele momento.

O que o gráfico Headroom mostra?

O gráfico de Headroom está relacionado à capacidade de desempenho restante para os controladores do array de storage. Este gráfico é visível na página inicial e na guia Visão Física do bloco Desempenho.

O gráfico de margem disponível mostra a capacidade de desempenho restante dos objetos físicos no sistema de storage. Posicione o cursor sobre um ponto no gráfico para visualizar 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 preferências de exibição?

Para obter informações sobre as opções de exibição disponíveis:

- Para saber mais sobre as unidades padrão para exibir os valores de capacidade, veja "Definir as unidades padrão para valores de capacidade".
- Para saber mais sobre o período de tempo padrão para exibir gráficos de desempenho, veja "Definir o período de tempo padrão para os gráficos de desempenho".

Pools e grupos de volume

Saiba mais sobre pools e grupos de volume no SANtricity System Manager

Você pode criar capacidade de storage lógica a partir de um subconjunto de unidades não atribuídas em seu array de storage. Essa capacidade lógica pode assumir a forma de um pool ou de um grupo de volume, dependendo das necessidades do seu ambiente.

O que são pools e grupos de volume?

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

Saiba mais:

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

Como você cria pools?

Você pode permitir que System Manager crie pools automaticamente quando detectar capacidade não atribuída em um array de storage. Como alternativa, quando a criação automática não conseguir determinar a melhor configuração, você pode criar pools manualmente em **Storage › Pools & Volume Groups**.

Saiba mais:

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

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

Como criar grupos de volume?

Você pode criar grupos de volumes no menu: Storage [Pools & Volume Groups].

Saiba mais:

- "Criar um grupo de volume"
- "Adicionar capacidade a um pool ou grupo de volume"

Informações relacionadas

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

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

Conceitos

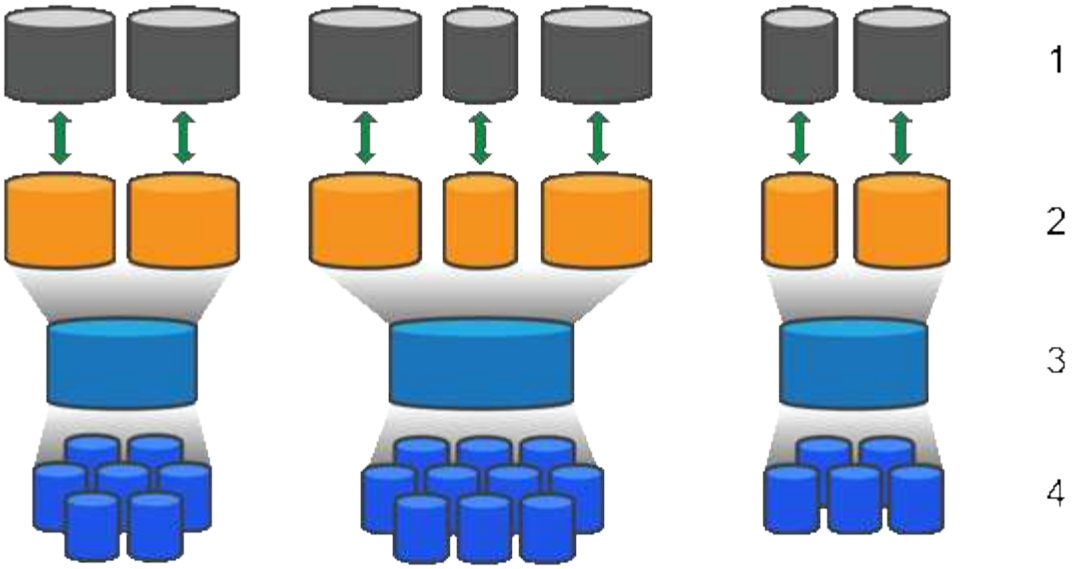
Como funcionam os pools e os grupos de volume no SANtricity software

Para provisionar armazenamento, você cria um pool ou grupo de volume que conterá os Hard Disk Drives (HDD) ou Solid State Disk (SSD) que deseja usar em seu array de storage.

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

- Pools
- Grupos de volumes RAID

Os pools e grupos de volumes são as unidades de armazenamento de nível superior em um array de storage: eles 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] LUNs do host; [2] Volumes; [3] Grupos de volumes ou pools; [4] Unidades de disco rígido (HDD) ou SSD

Quando um sistema de storage é implantado, o primeiro passo é apresentar a capacidade de unidade disponível aos diversos hosts por:

- Criando pools ou grupos de volume com capacidade suficiente
- Adicionar o número de unidades necessárias para atender aos requisitos de desempenho ao pool ou grupo de volume
- Selecionar o nível desejado de proteção RAID (caso utilize grupos de volume) para atender a requisitos específicos de negócios

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

Pools

Os pools são projetados para agregar discos rígidos físicos em um grande espaço de storage e fornecer proteção RAID aprimorada para ele. Um pool cria vários conjuntos RAID virtuais a partir do número total de discos atribuídos ao pool e distribui os dados uniformemente entre todos os discos participantes. Se um disco for perdido ou adicionado, System Manager reequilibra dinamicamente os dados em todos os discos ativos.

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 de unidade e tratamento de perda de unidade. System Manager define automaticamente o nível RAID como 6 em uma configuração 8+2 (oito discos de dados mais dois discos de paridade).

Correspondência de unidade

Você pode escolher entre HDD ou SSDs para uso em pools; no entanto, assim como nos grupos de volume, todas as unidades no pool devem usar a mesma tecnologia. Os controladores selecionam automaticamente quais unidades incluir, portanto, você deve garantir que tenha um número suficiente de unidades para a tecnologia que escolher.

Gerenciando unidades com falha

Os pools têm uma capacidade mínima de 11 discos; no entanto, a capacidade equivalente a um disco é reservada como capacidade de reserva no caso de falha de um disco. Essa capacidade de reserva é chamada de “preservation capacity.”

Ao criar pools, uma certa quantidade de capacidade é reservada para uso emergencial. Essa capacidade é expressa em termos de número de unidades no System Manager, mas a implementação real é distribuída por todo o pool de unidades. A quantidade padrão de capacidade reservada é baseada no número de unidades no pool.

Após a criação do pool, você pode alterar o valor da capacidade de preservação para mais ou menos capacidade, ou até mesmo defini-la como nenhuma capacidade de preservação (0 drive’s worth). A quantidade máxima de capacidade que pode ser preservada (expressa como número de drives) é 10, mas a capacidade disponível pode ser menor, dependendo do número total de drives no pool.

Grupos de volume

Os grupos de volumes definem como a capacidade é alocada no sistema de storage aos volumes. Os discos rígidos são organizados em grupos RAID e os volumes residem nos discos de um grupo RAID. Portanto, as configurações do grupo de volume identificam quais discos fazem parte do grupo e qual nível RAID é utilizado.

Ao criar um grupo de volume, 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 volume é o total do número de unidades que você selecionar, multiplicado pela capacidade delas.

Correspondência de unidade

Você deve combinar as unidades no grupo de volume em termos de tamanho e desempenho. Se houver unidades menores e maiores no grupo de volume, todas as unidades serão reconhecidas como o menor tamanho de capacidade. Se houver unidades mais lentas e mais rápidas no grupo de volume, todas as unidades serão 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 (HDD e SSD). RAID 3, 5 e 6 são limitados a um máximo de 30 unidades. RAID 1 e RAID 10 usam espelhamento, portanto esses grupos de volumes devem ter um número par de discos.

Gerenciando unidades com falha

Os grupos de volume utilizam hot spare drives como reserva em caso de falha de uma unidade em volumes RAID 1/10, RAID 3, RAID 5 ou RAID 6 contidos em um grupo de volume. Um hot spare drive não contém dados e adiciona outro nível de redundância ao seu array de storage.

Se uma unidade falhar no array de storage, a hot spare é automaticamente substituída pela unidade com falha, sem a necessidade de troca física. Se a hot spare estiver disponível quando uma unidade falhar, o controlador usa os dados de redundância para reconstruir os dados da unidade com falha na hot spare.

Aprenda sobre a terminologia de capacidade no SANtricity software

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

Objetos de armazenamento

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

Objeto de armazenamento	Descrição
Host	Um host é um servidor que envia I/O para um volume em um array de storage.
LUN	Um número de unidade lógica (LUN, na sigla em inglês) é o número atribuído ao espaço de endereçamento que um host usa para acessar um volume. O volume é apresentado ao host como capacidade na forma de um LUN. Cada host possui seu próprio espaço de endereçamento LUN. Portanto, o mesmo LUN pode ser usado por diferentes hosts para acessar volumes diferentes.
Grupo de consistência	Um grupo de consistência de espelhamento é um contêiner para um ou mais pares espelhados. Para operações de espelhamento assíncrono, você deve 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.
Pool	Um pool é um conjunto de unidades agrupadas 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 volume.)
Grupo de consistência Snapshot	Um grupo de consistência de snapshot é uma coleção de volumes que são tratados como uma única entidade quando uma imagem de snapshot é criada. Cada um desses volumes possui sua própria imagem de snapshot, mas todas as imagens são criadas no mesmo ponto no tempo.
Grupo de Snapshot	Um grupo de Snapshot é uma coleção de imagens de Snapshot de um único volume base.
Volume de Snapshot	Um volume de snapshot permite que o host acesse dados na imagem do snapshot. O volume de snapshot contém sua própria capacidade reservada, que salva quaisquer modificações no volume base sem afetar a imagem original do snapshot.
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 array de storage.
Grupo de volume	Um grupo de volume é um contêiner para volumes com características compartilhadas. Um grupo de volume tem uma capacidade definida e nível RAID. Você pode usar um grupo de volume para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um grupo de volume ou de um pool.)

Capacidade de armazenamento

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

Tipo de capacidade	Descrição
Capacidade alocada	A capacidade alocada é a capacidade física alocada das unidades em um pool ou grupo de volume. Você utiliza a capacidade alocada para criar volumes e para operações de copy services.
Capacidade livre	A capacidade livre é a capacidade disponível em um pool ou grupo de volume que ainda não foi alocada para criação de volumes, operações de serviços de cópia e objetos de storage.
Capacidade do pool ou grupo de volume	A capacidade de um pool, volume ou grupo de volume é a capacidade em um array de storage que foi atribuída a um pool ou grupo de volume. Essa capacidade é usada para criar volumes e atender às diversas necessidades de capacidade das operações de serviços de cópia e objetos de armazenamento.
Capacidade inutilizável do pool	A capacidade inutilizável do pool é o espaço em um pool que não pode ser usado devido a tamanhos incompatíveis de drives.
Capacidade de preservação	A capacidade de preservação é a quantidade de capacidade (número de drives) reservada em um pool para suportar possíveis falhas de drives.
Capacidade relatada	A capacidade reportada é a capacidade que é informada ao host e pode ser acessada pelo host.
Capacidade reservada	A capacidade reservada é a capacidade física alocada que é usada para qualquer operação de serviço de cópia e objeto de armazenamento. Ela não é diretamente legível pelo host.
Cache SSD	O cache SSD é um conjunto de unidades de estado sólido (SSD) que você agrupa logicamente em seu array de storage. O recurso de cache SSD armazena em cache os dados acessados com mais frequência ("dados quentes") em unidades SSD de menor latência para acelerar dinamicamente as cargas de trabalho dos aplicativos.
Capacidade não atribuída	A capacidade não atribuída é o espaço em um array de storage que **não** foi atribuído a um pool ou volume group.
Capacidade escrita	A capacidade de escrita é a quantidade de capacidade que foi escrita da capacidade reservada alocada para volumes finos.

Aprenda sobre pools e grupos de volume no software SANtricity

Você pode criar volumes usando um pool ou um grupo de volume. A melhor escolha depende principalmente dos principais requisitos de storage, como a carga de trabalho

de E/S esperada, os requisitos de desempenho e os requisitos de proteção de dados.

Razões para escolher um pool ou grupo de volume

Escolha um pool

- Se você precisa de reconstruções de unidades mais rápidas e administração de storage simplificada, requer volumes finos e/ou tem uma carga de trabalho altamente aleatória.
- Se você deseja distribuir os dados de cada volume aleatoriamente entre um conjunto de drives que compõem o pool.

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

Escolha um grupo de volume

- Se você precisa de largura de banda máxima do sistema, capacidade de ajustar as configurações de storage e uma carga de trabalho altamente sequencial.
- Se você deseja distribuir os dados entre as unidades com base em um nível RAID. Você pode especificar o nível RAID ao criar o grupo de volume.
- Se você deseja gravar os dados de cada volume sequencialmente no conjunto de drives que compõem o grupo de volume.

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

Diferenças de recursos entre pools e grupos de volume

A tabela a seguir apresenta uma comparação de recursos entre grupo de volume e pools.

Usar	Pool	Grupo de volume
Carga de trabalho aleatória	Melhor	Bom
Carga de trabalho sequencial	Bom	Melhor
Tempo de reconstrução da unidade	Mais rápido	Mais devagar
Desempenho (modo ideal)	Bom: melhor para blocos pequenos e cargas de trabalho aleatórias.	Bom: ideal para cargas de trabalho sequenciais com blocos grandes
Desempenho (modo de reconstrução de drive)	Melhor: geralmente melhor que RAID 6	Degradado: queda de até 40% no desempenho
Falhas múltiplas de unidade	Maior proteção de dados: reconstruções mais rápidas e priorizadas	Menos proteção de dados: reconstruções lentas, maior risco de perda de dados

Usar	Pool	Grupo de volume
Adicionando unidades	Mais rápido: adicione ao pool instantaneamente	Mais lento: requer operação de Expansão Dinâmica de Capacidade
Suporte para volumes finos	Sim	Não
Suporte para disco de estado sólido (SSD)	Sim	Sim
Administração simplificada	Sim: nenhum hot spare ou configuração de RAID para configurar	Não: é necessário alocar hot spares, configurar RAID
Desempenho ajustável	Não	Sim

Comparação funcional de pools e grupos de volume

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

A tabela a seguir ajuda você a decidir se um pool ou grupo de volume é o mais adequado às suas necessidades de storage.

Função	Pool	Grupo de volume
Diferentes níveis RAID suportados	Não. Sempre RAID 6 no System Manager.	Sim. RAID 0, 1, 10, 5 e 6 disponíveis.
Volumes finos suportados	Sim	Não
Suporte para criptografia de disco completo (FDE)	Sim	Sim
Data Assurance (DA) suportado	Sim	Sim
Proteção contra perda de shelf suportada	Sim	Sim
Proteção contra perda de gaveta suportada	Sim	Sim
Velocidades de drive mistas suportadas	Recomenda-se que sejam iguais, mas não é obrigatório. A unidade mais lenta determina a velocidade de todas as unidades.	Recomenda-se que sejam iguais, mas não é obrigatório. A unidade mais lenta determina a velocidade de todas as unidades.

Função	Pool	Grupo de volume
Capacidade de unidade mista suportada	Recomenda-se que sejam iguais, mas não é obrigatório. A menor unidade determina a capacidade de todas as unidades.	Recomenda-se que sejam iguais, mas não é obrigatório. 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 precisam de 2 (requer um número par). O mínimo para RAID 5 é 3. O mínimo para RAID 6 é 5.
Número máximo de unidades	Até o limite máximo para o array de storage	RAID 1 e 10—até o limite máximo do array de storage RAID 5, 6—30 discos
É possível escolher unidades individuais ao criar um volume	Não	Sim
É possível especificar o tamanho do segmento ao criar um volume	Sim. 128K suportado.	Sim
É possível especificar as características de E/S ao criar um volume	Não	Sim. Sistema de arquivos, banco de dados, multimídia e personalizados são suportados.
Proteção contra falha de drive	Utiliza a capacidade de preservação em cada unidade no pool, tornando a reconstrução mais rápida.	Utiliza um hot spare. A reconstrução é limitada pelos IOPs da unidade.
Aviso ao atingir o limite de capacidade	Sim. É possível configurar um alerta quando a capacidade utilizada atingir uma porcentagem da capacidade máxima.	Não
Migração para um array de storage diferente suportada	Não. É necessário migrar primeiro para um grupo de volume.	Sim
Tamanho dinâmico do segmento (DSS)	Não	Sim
É possível alterar o nível RAID	Não	Sim
Expansão de volume (aumento da capacidade)	Sim	Sim

Função	Pool	Grupo de volume
Expansão de capacidade (adicionar capacidade)	Sim	Sim
Redução de capacidade	Sim	Não

Tipos mistos de unidades (HDD, SSD) não são suportados para pools nem para grupos de volume.

Saiba mais sobre a criação automática versus manual de pools no SANtricity System Manager

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

Criação automática

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

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

- Pools não existem no array de storage, e há unidades semelhantes suficientes para criar um novo pool.
- Novos discos são adicionados a um array de storage que possui pelo menos um pool.

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

- Crie um único pool se houver um número suficiente de drives desses tipos.
- Crie vários pools se a capacidade não atribuída consistir de diferentes tipos de unidades.
- Adicione as unidades ao pool existente se um pool já estiver definido no array de storage, 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 diferentes.

Criação manual

Você pode querer criar um pool manualmente quando a criação automática não conseguir determinar a melhor configuração. Essa situação pode ocorrer por um dos seguintes motivos:

- Os novos discos rígidos podem ser adicionados a mais de um pool.
- Um ou mais dos novos candidatos a pool podem usar proteção contra perda de prateleira ou proteção contra perda de gaveta.
- Um ou mais dos candidatos atuais ao pool não conseguem manter seu status de proteção contra perda de prateleira ou perda de gaveta.

Você também pode querer criar um pool manualmente se tiver vários aplicativos em seu array de storage e não quiser que eles disputem os mesmos recursos de disco. Nesse caso, você pode considerar criar

manualmente um pool menor para um ou mais dos 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 nos quais distribuir os dados. Criar manualmente um pool separado dedicado à carga de trabalho de um aplicativo específico pode permitir que as operações do array de storage sejam executadas mais rapidamente, com menos contenção.

Configurar storage

Crie um pool automaticamente no SANtricity System Manager

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

Antes de começar

Você pode abrir a caixa de diálogo Pool Auto-Configuration quando uma destas condições for verdadeira:

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

Sobre esta tarefa

Tenha em mente o seguinte:

- Ao adicionar unidades a um array de storage, System Manager detecta 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 já tiverem sido definidos, System Manager automaticamente lhe oferecerá a opção de adicionar as unidades compatíveis a um pool existente. Quando novas unidades são adicionadas a um pool existente, System Manager redistribui automaticamente os dados pela nova capacidade, que agora inclui as novas unidades que você adicionou.
- Ao configurar um array de storage EF600 ou EF300, certifique-se de que cada controlador tenha 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 ambos os barramentos PCIe do lado das unidades de forma mais eficaz.

Você pode abrir a caixa de diálogo Pool Auto-Configuration usando qualquer um dos seguintes métodos:

- Quando é detectada capacidade não atribuída, a recomendação de Autoconfiguração do Pool aparece na página inicial, na área de Notificações. Clique em **Exibir Autoconfiguração do Pool** para abrir a caixa de diálogo.
- Você também pode abrir a caixa de diálogo de Autoconfiguração do Pool na página Pools e Volume Groups, conforme descrito na tarefa a seguir.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione o menu: mais [Iniciar configuração automática do pool].

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

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 capacidade semelhante.
- Cria vários pools se a capacidade não atribuída consistir em diferentes tipos de drives.
- Adiciona as unidades a um pool existente se um pool já estiver definido no array de storage e você adicionar novas unidades do mesmo tipo 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 diferentes.

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

   Informações sobre o tipo de unidade, capacidade de segurança, capacidade de garantia de dados (DA), proteção contra perda na prateleira e proteção contra perda na gaveta aparecem.

   Para os arrays de storage EF600 e EF300, as configurações de provisionamento de recursos e tamanhos de bloco de volume também são exibidas.

5. Clique em **Accept**.

Criar um pool manualmente no SANtricity System Manager

Você pode criar um pool manualmente (a partir de um conjunto de candidatos) se o recurso Pool Auto Configuration 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 no mínimo 11 unidades do mesmo tipo de unidade (HDD ou SSD).
- A proteção contra perda de prateleira exige que as unidades que compõem o pool estejam localizadas em pelo menos seis prateleiras de unidades diferentes e que não haja mais de duas unidades em uma única prateleira de unidades.
- A proteção contra perda de gavetas exige que as unidades que compõem o pool estejam localizadas em pelo menos cinco gavetas diferentes e que o pool inclua um número igual de prateleiras de unidades de cada gaveta.
- Ao configurar um EF600 ou EF300 array de storage, certifique-se de que cada controlador tenha 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 utilizarem ambos os barramentos PCIe do lado das unidades de forma mais eficiente. Atualmente System Manager permite a seleção de unidades no recurso Advanced ao criar um grupo de volume. Para a criação de pool, recomenda-se usar todas as unidades do array de storage.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Clique no menu: criar [Pool].

   A caixa de diálogo Create Pool é exibida.

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

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

5. Selecione o candidato do pool que deseja usar com base nas seguintes características e clique em **Criar**.

Característica	Usar
Capacidade livre	Mostra a capacidade livre do pool candidato em GiB. Selecione um pool candidato com capacidade para as necessidades de storage da sua aplicação. A capacidade de preservação (sobressalente) também é distribuída por todo o pool e não faz parte da quantidade de capacidade livre.
Total de drives	Mostra o número de unidades disponíveis no pool candidato. System Manager reserva automaticamente o máximo de unidades possível para capacidade de preservação (para cada seis unidades em um pool, System Manager reserva uma unidade para capacidade de preservação). Quando ocorre uma falha na unidade, a capacidade de preservação é usada para guardar os dados reconstruídos.
Tamanho do bloco de drive (somente EF300 e EF600)	Mostra o tamanho do bloco (tamanho do setor) que as unidades no pool podem gravar. Valores podem incluir: • 512 — tamanho do setor de 512 bytes. • 4K — tamanho do setor de 4.096 bytes.
Compatível com segurança	Indica se este candidato a conjunto de unidades é composto inteiramente por unidades com capacidade de segurança, que podem ser unidades Full Disk Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS). • Você pode proteger seu pool com o Drive Security, mas todas as unidades devem ser secure-capable para usar esse recurso. • Se você deseja criar um pool somente FDE, procure por **Sim - FDE** na coluna Secure-Capable. Se você deseja criar um pool somente FIPS, procure por **Sim - FIPS** ou **Sim - FIPS (Misto)**. "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 operará no nível de segurança mais baixo (140-2). • Você pode criar um pool composto por unidades que podem ou não ser compatíveis com segurança ou que tenham diferentes níveis de segurança. Se as unidades no pool incluírem unidades que não são compatíveis com segurança, você não poderá tornar o pool seguro.

Característica	Usar
Ativar segurança?	Oferece a opção de ativar o recurso de Drive Security com unidades compatíveis com segurança. Se o pool for compatível com segurança e você tiver criado uma chave de segurança, é possível ativar a segurança marcando a caixa de seleção. A única maneira de remover o Drive Security depois de ativado é excluir o pool e apagar as drives.
Compatível com DA	Indica se o Data Assurance (DA) está disponível para este candidato a pool. O DA verifica e corrige erros que possam ocorrer durante a transferência de dados pelos controladores até as unidades. DA é ativado se todas as unidades forem compatíveis com DA. DA pode ser desativado após a criação do volume selecionando **Storage › Volumes › View/Edit Settings › Advanced › Permanently disable data assurance**. Se DA for desativado em um volume, não poderá ser reativado.
Resource Provisioning Capable (somente EF300 e EF600)	Mostra se o Resource Provisioning está disponível para este pool candidato. Resource Provisioning é um recurso disponível nos EF300 e EF600 storage arrays, que permite que os volumes sejam colocados em uso imediatamente, sem processo de inicialização em segundo plano.
Proteção contra perda de shelf	Indica se a proteção contra perda de shelf está disponível. A proteção contra perda de compartimento garante acessibilidade aos dados nos volumes de um pool caso ocorra uma perda total de comunicação com uma unidade única de compartimento.
Proteção contra perda de gavetas	Indica se a proteção contra perda de gavetas está disponível, que só é oferecida se você estiver usando uma prateleira de unidades que contenha gavetas. A proteção contra perda de gaveta garante acessibilidade aos dados nos volumes de um pool caso ocorra uma perda total de comunicação com uma única gaveta em uma drive shelf.
Tamanhos de bloco de volume suportados (EF300 e EF600 only)	Mostra os tamanhos de bloco que podem ser criados para os volumes no pool: • 512n — 512 bytes nativo. • 512e — 512 bytes emulados. • 4K — 4.096 bytes.

Crie um grupo de volume no SANtricity System Manager

Você usa um grupo de volume para criar um ou mais volumes que são acessíveis ao host. Um grupo de volume é um contêiner para volumes com características

compartilhadas, como nível RAID e capacidade.

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

Antes de começar

Consulte estas diretrizes antes de criar um grupo de volume:

- Você precisa de pelo menos uma unidade não atribuída.
- Existem limites para o 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/prateleira, você deve criar um grupo de volume que utilize unidades localizadas em pelo menos três prateleiras ou gavetas, a menos que esteja usando RAID 1, onde duas prateleiras/gavetas são o mínimo.
- Se você possui um array de storage EF600 ou EF300 e planeja criar um grupo de volume manualmente, certifique-se de que cada controlador tenha 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 utilizarem ambos os barramentos PCIe do lado das unidades de forma mais eficaz. Atualmente, o System Manager permite a seleção de unidades no recurso Avançado ao criar um grupo de volume.
- Analise como a sua escolha de nível RAID afeta a capacidade resultante do grupo de volume:
  - Se você selecionar RAID 1, deverá adicionar duas unidades por vez para garantir que um par espelhado seja selecionado. O espelhamento e o striping (conhecido como RAID 10 ou RAID 1+0) são obtidos quando quatro ou mais unidades são selecionadas.
  - Se você selecionar RAID 5, deverá adicionar no mínimo três unidades para criar o grupo de volume.
  - Se você selecionar RAID 6, deverá adicionar no mínimo cinco unidades para criar o grupo de volume.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Clique no menu: criar [grupo de volume].

   A caixa de diálogo Criar grupo de volume é exibida.

3. Digite um nome para o grupo de volume.
4. Selecione o nível RAID que melhor atenda às suas necessidades de storage e proteção de dados.

   A tabela de grupos de volumes candidatos é exibida e mostra apenas os candidatos que suportam o nível RAID selecionado.

5. **Opcional:** se você tiver mais de um tipo de unidade em seu array de storage, selecione o tipo de unidade que deseja usar.

   A tabela de grupos de volumes candidatos é exibida e mostra apenas os candidatos que suportam o tipo de unidade selecionado e o nível RAID.

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

   Para selecionar unidades manualmente, clique no link **Selecionar unidades manualmente (avançado)**. Ao clicar, ele muda para **Selecionar unidades automaticamente (avançado)**.

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

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

7. Com base nas características da unidade exibidas, selecione as unidades que deseja usar no grupo de volume e clique em **Criar**.

   As características da unidade exibidas dependem se você selecionou o método automático ou o método manual.

Características da unidade do método automático

Característica	Usar
Capacidade livre	Mostra a capacidade disponível em GiB. Selecione um grupo de volume candidato com capacidade para as necessidades de storage da sua aplicação.
Total de drives	Mostra o número de unidades disponíveis para este grupo de volume. Selecione um candidato a grupo de volume com o número de unidades que você deseja.
Tamanho do bloco de drive (somente EF300 e EF600)	Mostra o tamanho do bloco (tamanho do setor) que as unidades no grupo podem gravar. Valores podem incluir: • 512 — tamanho do setor de 512 bytes. • 4K — tamanho do setor de 4.096 bytes.
Compatível com segurança	Indica se este grupo de volumes candidato é composto inteiramente por unidades com capacidade de segurança, que podem ser unidades Full Disk Encryption (FDE) ou Federal Information Processing Standard (FIPS). • Você pode proteger seu grupo de volume com Drive Security, mas todas as unidades devem ser compatíveis com segurança para usar esse recurso. • Se você deseja criar um grupo de volume somente FDE, procure por **Sim - FDE** na coluna Secure-Capable. Se você deseja criar um grupo de volume somente FIPS, procure por **Sim - FIPS** ou **Sim - FIPS (Misto)**. "Misto" indica uma mistura de unidades nível 140-2 e 140-3. Se você usar uma mistura desses níveis, esteja ciente de que o grupo de volume operará no nível de segurança mais baixo (140-2). • Você pode criar um grupo de volume composto por unidades que podem ou não ser compatíveis com segurança, ou que apresentem uma combinação de níveis de segurança. Se as unidades no grupo de volume incluírem unidades que não sejam compatíveis com segurança, você não poderá tornar o grupo de volume seguro.
Ativar segurança?	Oferece a opção de ativar o recurso Drive Security para unidades compatíveis com segurança. Se o grupo de volumes for compatível com segurança e você tiver configurado uma chave de segurança, você pode ativar o Drive Security marcando a caixa de seleção. ⓘ A única maneira de remover Drive Security depois de ativada é excluir o grupo de volume e apagar as unidades.

Característica	Usar
Compatível com DA	Indica se Data Assurance (DA) está disponível para este grupo. Data Assurance (DA) verifica e corrige erros que possam ocorrer durante a transferência de dados pelos controladores até as unidades de disco. Se você deseja usar o DA, selecione um grupo de volumes compatível com DA. (Para unidades compatíveis com DA, DA é ativado automaticamente nos volumes criados no pool.) Um grupo de volume pode conter unidades compatíveis com DA ou não compatíveis com DA, mas todas as unidades devem ser compatíveis com DA para que você possa usar esse recurso.
Resource Provisioning Capable (somente EF300 e EF600)	Mostra se o Resource Provisioning está disponível para este grupo. Resource Provisioning é um recurso disponível nos storage arrays EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente, sem processo de inicialização em segundo plano.
Proteção contra perda de shelf	Indica se a proteção contra perda de prateleira está disponível. A proteção contra perda de prateleira garante acessibilidade aos dados nos volumes de um grupo de volumes caso ocorra uma perda total de comunicação com a prateleira.
Proteção contra perda de gavetas	Indica se a proteção contra perda de gaveta está disponível, recurso fornecido apenas se você estiver usando um drive shelf que contém gavetas. A proteção contra perda de gaveta garante acessibilidade aos dados nos volumes de um grupo de volume caso ocorra uma perda total de comunicação com uma unidade única em um drive shelf.
Tamanhos de bloco de volume suportados (EF300 e EF600 only)	Mostra os tamanhos de bloco que podem ser criados para os volumes no grupo: • 512n — 512 bytes nativo. • 512e — 512 bytes emulados. • 4K — 4.096 bytes.

Características da unidade do método manual

Característica	Usar
Tipo de mídia	Indica o tipo de mídia. Os seguintes tipos de mídia são suportados: • Disco rígido • Unidade de estado sólido (SSD) Todas as unidades em um grupo de volume devem ser do mesmo tipo de mídia (todas SSDs ou todas hard drives). Grupos de volume não podem conter uma mistura de tipos de mídia ou tipos de interface.
Tamanho do bloco de drive (somente EF300 e EF600)	Mostra o tamanho do bloco (tamanho do setor) que as unidades no grupo podem gravar. Valores podem incluir: • 512 — tamanho do setor de 512 bytes. • 4K — tamanho do setor de 4.096 bytes.
Capacidade da unidade	Indica a capacidade da unidade. • Sempre que possível, selecione unidades que tenham uma capacidade igual às capacidades das unidades atuais no grupo de volume. • Se precisar adicionar unidades não atribuídas com capacidade menor, esteja ciente de que a capacidade utilizável de cada unidade atualmente no grupo de volume é reduzida. Portanto, a capacidade da unidade é a mesma em todo o grupo de volume. • Caso precise adicionar unidades não atribuídas com maior capacidade, esteja ciente de que a capacidade utilizável das unidades não atribuídas que você adicionar será reduzida para corresponder às capacidades atuais das unidades no grupo de volume.
Bandeja	Indica a localização da bandeja da unidade.
Slot	Indica a localização do slot da unidade.
Velocidade (rpm)	Indica a velocidade da unidade.
Tamanho do setor lógico	Indica o tamanho e o formato do setor.

Característica	Usar
Compatível com segurança	Indica se este grupo de volumes candidato é composto inteiramente por unidades com capacidade de segurança, que podem ser unidades Full Disk Encryption (FDE) ou Federal Information Processing Standard (FIPS). • Você pode proteger seu grupo de volume com Drive Security, mas todas as unidades devem ser compatíveis com segurança para usar esse recurso. • Se você deseja criar um grupo de volume somente FDE, procure por **Sim - FDE** na coluna Secure-Capable. Se você deseja criar um grupo de volume somente FIPS, procure por **Sim - FIPS** ou **Sim - FIPS (Misto)**. "Misto" indica uma mistura de unidades nível 140-2 e 140-3. Se você usar uma mistura desses níveis, esteja ciente de que o grupo de volume operará no nível de segurança mais baixo (140-2). • Você pode criar um grupo de volume composto por unidades que podem ou não ser compatíveis com segurança, ou que apresentem uma combinação de níveis de segurança. Se as unidades no grupo de volume incluírem unidades que não sejam compatíveis com segurança, você não poderá tornar o grupo de volume seguro.
Compatível com DA	Indica se o Data Assurance (DA) está disponível para este grupo. O Data Assurance (DA) verifica e corrige erros que possam ocorrer durante a comunicação de dados pelos controladores até as unidades de disco. Se você deseja usar o DA, selecione um grupo de volumes compatível com DA. (Para unidades compatíveis com DA, DA é ativado automaticamente nos volumes criados no pool.) Um grupo de volume pode conter unidades compatíveis com DA ou não compatíveis com DA, mas todas as unidades devem ser compatíveis com DA para que você possa usar esse recurso.
Tamanhos de bloco de volume suportados (EF300 e EF600 only)	Mostra os tamanhos de bloco que podem ser criados para os volumes no grupo: • 512n — 512 bytes nativo. • 512e — 512 bytes emulados. • 4K — 4.096 bytes.
Resource Provisioning Capable (somente EF300 e EF600)	Mostra se o Resource Provisioning está disponível para este grupo. Resource Provisioning é um recurso disponível nos storage arrays EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente, sem processo de inicialização em segundo plano.

Adicione capacidade a um pool ou grupo de volume no SANtricity System Manager

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

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

Antes de começar

- As unidades devem estar em status Ótimo.
- As unidades devem ter o mesmo tipo de unidade (HDD ou SSD).
- O pool ou grupo de volume deve estar em status Ótimo.
- O número máximo de volumes permitidos em um volume group é 256.
- O número máximo de volumes permitidos em um pool depende do modelo do sistema de storage:
  - 2.048 volumes (EF600 e E5700 series)
  - 1.024 volumes (EF300)
  - 512 volumes (E4000 e E2800 series)
- Se o pool ou grupo de volume contiver apenas unidades com capacidade de segurança, adicione somente unidades com capacidade de segurança para continuar usando os recursos de criptografia das unidades com capacidade de segurança.

  Unidades com capacidade de segurança podem ser unidades Full Disk Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS).

Sobre esta tarefa

Para pools, você pode adicionar no máximo 60 drives por vez. Para volume groups, você pode adicionar no máximo dois drives por vez. Se precisar adicionar mais do que o número máximo de drives, repita o procedimento. (Um pool não pode conter mais drives do que o limite máximo para um sistema de storage.)

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

Evite usar unidades com suporte a Data Assurance (DA) para adicionar capacidade a um pool ou grupo de volume que não seja DA capaz. O pool ou grupo de volume não pode aproveitar as capacidades da unidade DA capaz. Considere usar unidades que não sejam DA capazes nessa situação.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione o pool ou grupo de volume ao qual deseja adicionar unidades e clique em **Add Capacity**.

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

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

   O firmware do controlador organiza as unidades não atribuídas, exibindo as melhores opções no topo. A capacidade livre total que é adicionada ao pool ou grupo de volume aparece abaixo da lista em **Capacidade total selecionada**.

Detalhes do campo

Campo	Descrição
Compartimento	Indica a localização da unidade na prateleira.
Baía	Indica a localização da baia da unidade.
Capacidade (GiB)	Indica a capacidade da unidade. • Sempre que possível, selecione unidades que tenham uma capacidade igual às capacidades das unidades atuais no pool ou grupo de volume. • Se precisar adicionar unidades não atribuídas com capacidade menor, esteja ciente de que a capacidade utilizável de cada unidade atualmente no pool ou grupo de volume é reduzida. Portanto, a capacidade da unidade é a mesma em todo o pool ou grupo de volume. • Caso precise adicionar unidades não atribuídas com maior capacidade, esteja ciente de que a capacidade utilizável das unidades não atribuídas que você adicionar será reduzida para corresponder às capacidades atuais das unidades no pool ou grupo de volume.
Compatível com segurança	Indica se a unidade é compatível com segurança. • Para proteger seu pool ou grupo de volume com o recurso Drive Security, todas as unidades devem ser compatíveis com segurança. • É possível criar um pool ou grupo de volume com uma combinação de unidades com e sem capacidade de segurança, mas o recurso Drive Security não pode ser ativado. • Um pool ou grupo de volume com todas as unidades compatíveis com segurança não pode aceitar uma unidade não compatível com segurança para uso como reserva ou expansão, mesmo que a criptografia não esteja em uso. • Unidades de disco que são relatadas como compatíveis com segurança podem ser unidades Full Disk Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS). • Uma unidade FIPS pode ser de nível 140-2 ou 140-3, com o nível 140-3 sendo 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 volume operará no nível mais baixo de segurança (140-2).

Campo	Descrição
Compatível com DA	Indica se a unidade é compatível com Data Assurance (DA). • Não é recomendável usar unidades que não sejam compatíveis com Data Assurance (DA) para adicionar capacidade a um pool ou grupo de volume compatível com DA. O pool ou grupo de volume deixa de ter recursos de DA e você não tem mais a opção de habilitar DA em volumes recém-criados dentro do pool ou grupo de volume. • Não é recomendável usar unidades com capacidade Data Assurance (DA) para adicionar capacidade a um pool ou grupo de volume que não seja compatível com DA, pois esse pool ou grupo de volume não poderá aproveitar os recursos da unidade com DA (os atributos da unidade não correspondem). Considere usar unidades que não sejam compatíveis com DA nessa situação.
DULBE capaz	Indica se a unidade possui a opção de erro de bloco lógico desalocado ou não gravado (DULBE). DULBE é uma opção em unidades NVMe que permite que o array de storage EF300 ou EF600 suporte volumes com recursos provisionados.

4. Clique em **Add**.

   Se você estiver adicionando unidades a um pool ou grupo de volume, uma caixa de diálogo de confirmação aparecerá se você selecionar uma unidade que faça com que o pool ou grupo de volume deixe de ter um ou mais dos seguintes atributos:

   ◦ Proteção contra perda de shelf *
   ◦ Proteção contra perda de gaveta *
   ◦ Capacidade de criptografia de disco completo
   ◦ Capacidade de Data Assurance
   ◦ Capacidade DULBE

   * Atualmente, a caixa de diálogo de confirmação não é exibida ao adicionar unidades a um pool com shelf loss protection ou drawer loss protection.

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 volume, os dados em cada volume do pool ou grupo de volume são redistribuídos para incluir as unidades adicionais.

Gerenciar armazenamento

Verifique a redundância do volume no SANtricity System Manager

Com a orientação do suporte técnico ou conforme as instruções do Recovery Guru, você pode verificar a redundância de um volume em um pool ou grupo de volume para

determinar se os dados nesse volume são consistentes.

Os dados de redundância são usados para reconstruir rapidamente as informações em uma unidade de substituição caso uma das unidades no pool ou grupo de volume falhe.

Antes de começar

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

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

Sobre esta tarefa

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

- Analisa os blocos de dados em um volume RAID 3, RAID 5 ou RAID 6 e verifica as informações de redundância para cada bloco. (RAID 3 só pode ser atribuído a grupos de volume usando a interface de linha de comando.)
- Compara os blocos de dados em unidades RAID 1 espelhadas.
- 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 volume pode causar um erro. Para evitar esse problema, aguarde de um a dois minutos antes de executar outra verificação de redundância no mesmo pool ou grupo de volume.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione o menu: tarefas incomuns [Verificar redundância de volume].

   A caixa de diálogo Verificar redundância é exibida.

3. Selecione os volumes que deseja verificar e, em seguida, digite `check` para confirmar que deseja realizar esta operação.
4. Clique em **Check**.

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

   - O volume é selecionado na tabela de volumes.
   - O status da verificação de redundância é exibido na coluna **Status**.
   - A verificação é interrompida ao encontrar qualquer erro de mídia ou paridade e, em seguida, o erro é relatado.

Mais informações sobre o status da verificação de redundância

Status	Descrição
Pendente	Este é o primeiro volume a ser verificado e você ainda não clicou em Iniciar para iniciar a verificação de redundância. ou A operação de verificação de redundância está sendo realizada em outros volumes no pool ou grupo de volume.
Verificando	O volume está passando pela verificação de redundância.
Aprovado	O volume passou na verificação de redundância. Nenhuma inconsistência foi detectada nas informações de redundância.
Falha	O volume falhou na verificação de redundância. Foram detectadas inconsistências nas informações de redundância.
Erro de mídia	A mídia de armazenamento está defeituosa e ilegível. Siga as instruções exibidas no Recovery Guru.
Erro de paridade	A paridade não está correta para uma determinada parte dos dados. Um erro de paridade é potencialmente grave e pode causar perda permanente de dados.

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

Excluir um pool ou grupo de volume no SANtricity System Manager

Você pode excluir um pool ou grupo de volume para criar mais capacidade não atribuída, que você pode reconfigurar para atender às necessidades de armazenamento do seu aplicativo.

Antes de começar

- Você deve ter feito backup dos dados em todos os volumes no pool ou grupo de volume.
- Você deve ter interrompido todas as operações de entrada/saída (I/O).
- Você deve desmontar quaisquer sistemas de arquivos nos volumes.
- Você deve ter excluído quaisquer relacionamentos de espelhamento no pool ou grupo de volume.
- Você deve ter interrompido qualquer operação de cópia de volume em andamento para o pool ou grupo de volume.
- O pool ou grupo de volume não deve estar participando de uma operação de espelhamento assíncrono.
- As unidades no grupo de volume não devem ter uma reserva persistente.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione um pool ou grupo de volume da lista.

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

3. Selecione o menu: tarefas incomuns [Excluir] e confirme.

Resultados

System Manager executa as seguintes ações:

- Exclui todos os dados no pool ou grupo de volume.
- Exclui todas as unidades associadas ao pool ou grupo de volume.
- Remove a atribuição das unidades associadas, o que permite reutilizá-las em pools ou grupos de volume novos ou existentes.

Consolide a capacidade livre para um grupo de volume no SANtricity System Manager

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

Antes de começar

- O grupo de volume deve conter pelo menos uma área de capacidade livre.
- Todos os volumes do grupo de volume devem estar online e em status Ótimo.
- Operações de modificação de volume não devem estar em andamento, como a alteração do 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 abrir a caixa de diálogo Consolidate Free Capacity usando qualquer um dos seguintes métodos:

- Quando pelo menos uma área de capacidade livre é detectada para um grupo de volume, a recomendação "Consolidar capacidade livre" aparece na página inicial na área de Notificações. Clique no link **Consolidar capacidade livre** para abrir a caixa de diálogo.
- Você também pode abrir a caixa de diálogo Consolidate Free Capacity na página Pools & Volume Groups, conforme descrito na tarefa a seguir.

Mais informações sobre áreas de capacidade livre

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

Você consolida a capacidade livre em um grupo de volume para melhorar o desempenho de gravação. A capacidade livre do seu grupo de volume ficará fragmentada com o tempo, à medida que o host grava, modifica e exclui arquivos. Eventualmente, a capacidade disponível não estará localizada em um único bloco contíguo, mas estará espalhada em pequenos fragmentos por todo o grupo de volume. Isso causa ainda mais fragmentação de arquivos, já que o host precisa gravar novos arquivos como fragmentos para que caibam nos intervalos disponíveis de clusters livres.

Ao consolidar a capacidade livre em um grupo de volume selecionado, você notará uma melhoria no desempenho 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 o menu: Storage [Pools & Volume Groups].
2. Selecione o grupo de volume com capacidade livre que deseja consolidar e, em seguida, selecione **Tarefas incomuns › Consolidar capacidade livre do grupo de volume**.

   A caixa de diálogo Consolidate Free Capacity é exibida.

3. Digite `consolidate` para confirmar que deseja realizar esta operação.
4. Clique em **Consolidate**.

   System Manager começa a consolidar (desfragmentar) as áreas de capacidade livre do grupo de volume em uma quantidade contígua para tarefas subsequentes de configuração de storage.

Depois que você terminar

Selecione o menu: Home [View Operations in Progress] para visualizar o progresso da operação Consolidate Free Capacity. Esta operação pode ser demorada e pode afetar o desempenho do sistema.

Exportar/importar grupos de volume na interface de linha de comando do SANtricity

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

A função Exportar/Importar não é suportada na interface de usuário do SANtricity System Manager. Você deve usar a interface de linha de comando (CLI) para exportar/importar um grupo de volume para um array de storage.

Ative as luzes indicadoras em um pool, grupo de volume ou cache SSD no SANtricity System Manager

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

acende em cada unidade no pool, grupo de volume ou SSD Cache selecionado.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione o pool, grupo de volume ou SSD Cache que deseja localizar e clique em **More › Turn on locator lights**.

   Uma caixa de diálogo aparece indicando que as luzes das unidades que compõem o pool, grupo de volume ou cache SSD selecionado estão acesas.

3. Após localizar as unidades com sucesso, clique em **Turn Off**.

Remover capacidade de um pool ou SSD Cache no SANtricity System Manager

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

Após remover unidades, os dados em cada volume do pool ou SSD Cache são redistribuídos para as unidades restantes. As unidades removidas ficam desatribuídas e sua capacidade passa a fazer parte da capacidade livre total do array de storage.

Sobre esta tarefa

Siga estas orientações ao remover capacidade:

- Não é possível remover a última unidade em um SSD Cache sem primeiro excluir o SSD Cache.
- Não é possível reduzir o número de unidades em um pool para menos de 11 unidades.
- Você pode remover no máximo 12 unidades por 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 SSD Cache para armazenar os dados, quando esses dados forem redistribuídos para as unidades restantes no pool ou SSD Cache.

Leia sobre os possíveis impactos no desempenho

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

Leia sobre os impactos em drives com capacidade de segurança

- Se você remover a última unidade que não é compatível com segurança, o pool ficará apenas com unidades compatíveis com segurança. Nessa situação, você tem a opção de habilitar a segurança para o pool.
- Se você remover a última unidade que não é compatível com Data Assurance (DA), o pool ficará com todas as unidades compatíveis com DA.

> Qualquer novo volume que você criar no pool será compatível com DA. Se você quiser que volumes existentes sejam compatíveis com DA, você precisa excluir e então recriar o volume.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione o pool ou o SSD Cache e, em seguida, clique em **More › Remove capacity**.

   A caixa de diálogo Remover Capacity é exibida.
3. Selecione uma ou mais unidades na lista.

   Ao selecionar ou desmarcar unidades na lista, o campo **Capacidade total selecionada** é atualizado. Este campo mostra a capacidade total do pool ou SSD Cache que resulta após você remover as unidades selecionadas.
4. Clique em **Remover** e, em seguida, confirme que deseja remover as unidades.

   A capacidade recentemente reduzida do pool ou do cache SSD é refletida na visualização Pools e grupos de volume.

Modificar configurações de pool e grupo

Altere as configurações de um pool no SANtricity System Manager

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. System Manager configura automaticamente os pools como RAID 6.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione o pool que você deseja editar e clique em **Visualizar/Editar Configurações**.

   A caixa de diálogo Pool Setting é exibida.
3. Selecione a aba **Configurações** e, em seguida, edite as configurações do pool conforme apropriado.

Detalhes do campo

Configuração	Descrição
Nome	Você pode alterar o nome do pool fornecido pelo usuário. É obrigatório especificar um nome para o pool.
Alertas de capacidade	Você pode enviar notificações de alerta quando a capacidade livre em um pool atingir ou ultrapassar um limite especificado. Quando os dados armazenados no pool ultrapassam o limite especificado, System Manager envia uma mensagem, permitindo que você adicione mais espaço de storage ou exclua objetos desnecessários. Os alertas são exibidos na área de Notificações do Dashboard e podem ser enviados do servidor para os administradores por e-mail e mensagens SNMP trap. Você pode definir os seguintes alertas de capacidade: • **Alerta crítico** — Este alerta crítico notifica você quando a capacidade livre no pool atinge ou ultrapassa o limite especificado. Use os controles giratórios para ajustar a porcentagem do limite. Selecione a caixa de seleção para desativar esta notificação. • **Alerta antecipado** — Este alerta antecipado notifica você quando a capacidade livre em um pool está atingindo um limite especificado. Use os controles giratórios para ajustar a porcentagem do limite. Selecione a caixa de seleção para desativar esta notificação.

Configuração	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 rapidamente, mas pode diminuir o desempenho de I/O do host. Uma prioridade mais baixa faz com que as operações demorem mais, mas o desempenho de I/O do host é menos afetado. Você pode escolher entre cinco níveis de prioridade: lowest, low, medium, high e highest. Quanto maior o nível de prioridade, maior é o impacto nas operações de E/S do host e no desempenho do sistema. • **Prioridade crítica de reconstrução** — Esta barra deslizante determina a prioridade de uma operação de reconstrução de dados quando múltiplas falhas de unidade resultam em uma condição na qual alguns dados não possuem redundância e uma falha adicional de unidade pode resultar em perda de dados. • **Prioridade de reconstrução degradada** — Esta barra deslizante determina a prioridade da operação de reconstrução de dados quando ocorre uma falha na unidade, mas os dados ainda possuem redundância e uma falha adicional na unidade não resulta em perda de dados. • **Prioridade de operações em segundo plano** — Esta barra deslizante determina a prioridade das operações em segundo plano do pool que ocorrem enquanto o pool está em um estado ideal. Essas operações incluem Dynamic Volume Expansion (DVE), Instant Availability Format (IAF) e migração de dados para uma unidade substituída ou adicionada.

Configuração	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 suportar possíveis falhas de unidade. Quando ocorre uma falha de unidade, a capacidade de preservação é usada para armazenar os dados reconstruídos. Os pools usam a capacidade de preservação durante o processo de reconstrução de dados em vez de hot spare, que são usados em grupos de volume. Use os controles giratórios para ajustar o número de unidades. Com base no número de unidades, a capacidade de preservação no pool aparece ao lado da caixa do controle giratório. Tenha em mente as seguintes informações sobre capacidade de preservação. • Como a capacidade de preservação é subtraída da capacidade livre total de um pool, a quantidade de capacidade que você reserva afeta quanto de capacidade livre está disponível para criar volumes. Se você especificar 0 para a capacidade de preservação, toda a capacidade livre do pool é usada para a criação de volumes. • Se você diminuir a capacidade de preservação, aumentará a capacidade que pode ser usada para volumes do pool. **Capacidade de otimização adicional** (EF600 e EF300 arrays only) — Quando um pool é criado, uma capacidade de otimização recomendada é gerada, proporcionando um equilíbrio entre capacidade disponível versus desempenho e vida útil dos discos. Você pode ajustar esse equilíbrio movendo o controle deslizante para a direita para melhor desempenho e vida útil dos discos em detrimento de maior capacidade disponível, ou movendo-o para a esquerda para maior capacidade disponível em detrimento de melhor desempenho e vida útil dos discos. Unidades SSD terão uma vida útil mais longa e melhor desempenho máximo de gravação quando uma parte de sua capacidade estiver não alocada. Para unidades associadas a um pool, a capacidade não alocada é composta pela capacidade de preservação do pool, a capacidade livre (capacidade não usada pelos 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 ao reduzir a capacidade utilizável e, assim, não está disponível para criação de volumes.

4. Clique em **Salvar**.

Altere as configurações de um grupo de volume no SANtricity System Manager

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

Antes de começar

Se você estiver alterando o nível RAID para atender às necessidades de desempenho dos aplicativos que

acessam o grupo de volume, certifique-se de atender aos seguintes pré-requisitos:

- O grupo de volume deve estar em estado Ótimo.
- Você deve ter capacidade suficiente no grupo de volume para converter para o novo nível RAID.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione o grupo de volume que você 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, em seguida, edite as configurações do grupo de volume conforme apropriado.

Detalhes do campo

Configuração	Descrição
Nome	Você pode alterar o nome fornecido pelo usuário do grupo de volume. É obrigatório especificar um nome para um grupo de volume.
Nível RAID	Selecione o novo nível RAID no menu suspenso. • **RAID 0 striping** — Oferece alto desempenho, mas não fornece nenhuma redundância de dados. Se uma unidade única falhar no grupo de volume, todos os volumes associados falham e todos os dados são perdidos. Um grupo RAID de striping combina duas ou mais unidades em uma única unidade lógica grande. • **RAID 1 espelhamento** — Oferece alto desempenho e a melhor disponibilidade de dados, sendo ideal para armazenar dados confidenciais em nível corporativo ou pessoal. Protege seus dados espelhando automaticamente o conteúdo de uma unidade para a segunda unidade no par espelhado. Isso proporciona proteção em caso de falha de uma unidade única. • **RAID 10 striping/espelhamento** — Oferece uma combinação de RAID 0 (striping) e RAID 1 (espelhamento), e é obtido quando quatro ou mais drives são selecionados. RAID 10 é adequado para aplicações de alto volume de transações, como um banco de dados, que exigem alto desempenho e tolerância de falhas. • **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. • **RAID 6** — Ideal para ambientes que exigem proteção de redundância além do RAID 5, mas que não necessitam de alto desempenho de gravação. RAID 3 só pode ser atribuído a grupos de volume usando a interface de linha de comando (CLI). Ao alterar o nível RAID, você não pode cancelar essa operação depois que ela começa. Durante a alteração, seus dados permanecem disponíveis.

Configuração	Descrição
Capacidade de otimização (apenas arrays EF600)	Quando um grupo de volume é criado, uma capacidade de otimização recomendada é gerada que proporciona um equilíbrio entre a capacidade disponível, o desempenho e a vida útil da unidade. Você pode ajustar esse equilíbrio movendo o controle deslizante para a direita para obter melhor desempenho e maior vida útil da unidade, em detrimento de maior capacidade disponível, ou movendo-o para a esquerda para obter maior capacidade disponível, em detrimento de melhor desempenho e vida útil da unidade. Unidades SSD terão uma vida útil mais longa e melhor desempenho máximo de gravação quando uma parte de sua capacidade estiver não alocada. Para unidades associadas a um grupo de volume, a capacidade não alocada é composta pela capacidade livre do grupo (capacidade não usada pelos 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 ao reduzir a capacidade utilizável e, assim, não está disponível para criação de volumes.

4. Clique em **Salvar**.

   Uma caixa de diálogo de confirmação será exibida se a capacidade for reduzida, a redundância do volume for perdida ou a proteção contra perda de prateleira/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 de um grupo de volume, System Manager altera os níveis RAID de todos os volumes que compõem o grupo de volume. O desempenho pode ser ligeiramente afetado durante a operação.

Ative ou desative o provisionamento de recursos em grupos de volume e pools existentes no SANtricity System Manager

Para qualquer unidade compatível com DULBE, você pode ativar ou desativar o provisionamento de recursos em um volume existente em um pool ou grupo de volume.

O provisionamento de recursos é um recurso disponível nos arrays de storage EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente, sem processo de inicialização em segundo plano. Todos os blocos de disco atribuídos ao volume são desalocados (desmapeados), o que pode melhorar a vida útil do SSD e aumentar o desempenho máximo de gravação.

Por padrão, o provisionamento de recursos está habilitado em sistemas onde as unidades suportam DULBE. Não é necessário habilitar o provisionamento de recursos, a menos que você o tenha desabilitado anteriormente.

Antes de começar

- Você precisa ter um array de storage EF300 ou EF600.

  DULBE não é suportado nos arrays de storage EF300C ou EF600C neste momento.

- Você deve ter grupos ou pools de volumes SSD, onde todas as unidades suportem a capacidade de recuperação de erros NVMe Deallocated or Unwritten Logical Block Error Enable (DULBE). Caso contrário, a opção de provisionamento de recursos não estará disponível.

Sobre esta tarefa

Ao habilitar o provisionamento de recursos para grupos de volumes e pools existentes, todos os volumes no grupo de volume ou pool selecionado são alterados para permitir que os blocos sejam desalocados. Esse processo pode envolver uma operação em segundo plano para garantir alocação consistente na granularidade de unmap. Essa operação não desmapeia nenhum espaço. Após a conclusão da operação em segundo plano, o sistema operacional precisa desmapear quaisquer blocos não utilizados para criar espaço livre.

Ao desativar o provisionamento de recursos para grupos de volume ou pools 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 volume ou pool.

> Para novos grupos de volumes e pools, você pode ativar ou desativar o provisionamento de recursos no **Settings › Sistema › Configurações adicionais › Ativar/Desativar volumes com recursos provisionados**.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione um pool ou grupo de volume da lista.

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

3. Selecione **Tarefas incomuns** e, em seguida, **Ativar provisionamento de recurso** ou **Desativar provisionamento de recurso**.
4. Na caixa de diálogo, confirme a operação.

> **Se você reativou o DULBE** — Após a conclusão da operação em segundo plano, talvez seja necessário reinicializar o host para que ele detecte as alterações de configuração do DULBE e, em seguida, remontar todos os filesystems.

Ativar ou desativar o provisionamento de recursos para novos grupos de volumes ou pools no SANtricity System Manager

Se você desativou anteriormente o recurso padrão de provisionamento de recursos, pode reativá-lo para quaisquer novos grupos ou pools de volumes SSD que você criar. Você também pode desativar a configuração novamente.

O provisionamento de recursos é um recurso disponível nos arrays de storage EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente, sem processo de inicialização em segundo plano. Todos os blocos de disco atribuídos ao volume são desalocados (desmapeados), 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 array de storage EF300 ou EF600.
- Você precisa ter grupos ou pools de volumes SSD, onde todas as unidades suportam a capacidade de recuperação de erros NVMe Deallocated or Unwritten Logical Block Error Enable (DULBE).

> DULBE não é suportado nos arrays de storage EF300C ou EF600C neste momento.

Sobre esta tarefa

Ao reativar o provisionamento de recursos para novos grupos de volumes ou pools, somente os grupos de volumes e pools recém-criados serão afetados. Quaisquer grupos de volumes e pools existentes com o provisionamento de recursos ativado permanecerão inalterados.

Passos

1. Selecione o menu: configurações [Sistema].
2. Desça até **Configurações adicionais** e clique em **Ativar/Desativar volumes provisionados por recurso**.

   A descrição da configuração indica se o provisionamento de recursos está atualmente ativado ou desativado.

3. Na caixa de diálogo, confirme a operação.

Resultados

Habilitar ou desabilitar o provisionamento de recursos afeta apenas novos pools de SSD ou grupos de volumes que você criar. Pools ou grupos de volumes existentes permanecem inalterados.

Habilite a segurança para um pool ou grupo de volume no SANtricity System Manager

Você pode habilitar a Segurança de Unidade para um pool ou grupo de volume para impedir o acesso não autorizado aos dados nas unidades contidas no pool ou grupo de volume. O acesso de leitura e gravação às unidades só está disponível por meio de um controlador configurado com uma chave de segurança.

Antes de começar

- O recurso Drive Security deve estar ativado.
- Uma chave de segurança deve ser criada.
- O pool ou grupo de volume deve estar em estado Ótimo.
- Todas as unidades no pool ou grupo de volume devem ser unidades secure-capable.

Sobre esta tarefa

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

Após ativar a segurança, você só poderá removê-la excluindo o pool ou grupo de volume e, em seguida, apagando as unidades.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione o pool ou grupo de volume no qual deseja ativar a segurança e clique em **More › Enable security**.

   A caixa de diálogo Confirm Enable Security é exibida.

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

Gerenciar cache SSD

Como o cache SSD funciona no software SANtricity

O recurso SSD Cache é uma solução baseada no controlador que armazena em cache os dados acessados com mais frequência ("dados quentes") em unidades de estado sólido (SSDs) de menor latência para acelerar dinamicamente o desempenho do sistema. SSD Cache é usado exclusivamente para leituras do host.

Cache SSD versus cache primário

O cache SSD é um cache secundário usado em conjunto com o cache primário na memória dinâmica de acesso aleatório (DRAM) do controlador.

O cache SSD funciona de forma diferente do cache primário:

- Para o cache primário, cada operação de E/S deve passar os dados pelo cache para realizar a operação.

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

- O cache SSD é usado somente se for benéfico colocar os dados em cache para melhorar o desempenho geral do sistema.

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

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

Como o SSD Cache é utilizado

Armazenamento em cache coloca dados em uma unidade de menor latência, para que as respostas a solicitações futuras desses dados possam ocorrer muito mais rapidamente. Se um programa solicitar dados que estão no cache (chamado de "acerto do cache"), então a unidade de menor latência pode atender a essa transação. Caso contrário, ocorre um "erro de cache" e os dados precisam ser acessados da unidade original, mais lenta. À medida que mais acertos do cache ocorrem, o desempenho geral melhora.

Quando um programa host acessa as unidades do array de storage, os dados são armazenados no SSD Cache. Quando os mesmos dados são acessados novamente pelo programa host, eles são lidos do SSD Cache em vez dos discos rígidos. Os dados acessados com frequência são armazenados no SSD Cache. Os discos rígidos são acessados somente quando os dados não podem ser lidos do SSD Cache.

O cache SSD é utilizado apenas quando é benéfico colocar os dados em cache para melhorar o desempenho geral do sistema.

Quando a CPU precisa processar dados de leitura, ela segue os passos abaixo:

1. Verifique o cache DRAM.
2. Se não for encontrado no cache DRAM, então verifique o 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, então copie para o cache SSD.

Desempenho aprimorado

Copiar os dados mais acessados (hot spot) para o cache SSD permite uma operação mais eficiente do disco rígido, redução da latência e velocidades de leitura e gravação aceleradas. Usar SSDs de alto desempenho para armazenar em cache dados 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 SSD Cache. Depois que os dados são armazenados em cache e salvos nos SSDs, as leituras subsequentes desses dados são realizadas no SSD Cache, eliminando assim a necessidade de acessar o volume do HDD.

Cache SSD e o recurso Drive Security

Para usar o Cache SSD em um volume que também utiliza Drive Security (está com a segurança ativada), os recursos de Drive Security do volume e do Cache SSD devem corresponder. Se eles não corresponderem, o volume não terá a segurança ativada.

Implementar SSD Cache

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 armazenamento em cache SSD de leitura.

> Qualquer volume atribuído ao uso do SSD Cache de um controlador não é elegível para transferência automática de load balance.

Saiba mais sobre as restrições de cache SSD no software SANtricity

Saiba mais sobre as restrições ao usar o SSD Cache em seu array de storage.

Restrições

- Qualquer volume atribuído ao uso do SSD Cache de um controlador não é elegível para transferência automática de load balance.
- Atualmente, apenas um SSD Cache é suportado por array de storage.
- A capacidade máxima utilizável de SSD Cache em um array de storage é de 10 TB.
- O SSD Cache não é compatível com imagens de snapshot.
- Se você importar ou exportar volumes que estão com SSD Cache ativado ou desativado, os dados em cache não serão importados ou exportados.
- Não é possível remover a última unidade em um SSD Cache sem primeiro excluir o SSD Cache.

Restrições com Drive Security

- Você só pode habilitar a segurança no SSD Cache ao criar o SSD Cache. Você não pode habilitar a segurança posteriormente, como pode em um volume.
- Se você misturar unidades com capacidade de segurança com unidades sem capacidade de segurança no SSD Cache, não poderá ativar a Drive Security para essas unidades.
- Os volumes com segurança habilitada devem ter um SSD Cache com segurança habilitada.

Criar um SSD Cache no SANtricity System Manager

Para acelerar dinamicamente o desempenho do sistema, você pode usar o recurso SSD Cache para armazenar em cache os dados acessados com mais frequência ("dados quentes") em Solid State Drives (SSDs) de menor latência. SSD Cache é usado exclusivamente para leituras do host.

Antes de começar

Seu array de storage deve conter algumas unidades SSD.

Sobre esta tarefa

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

Siga estas orientações ao criar um novo SSD Cache.

- Você pode habilitar a segurança no cache SSD somente ao criá-lo, não depois.
- Apenas um SSD Cache é suportado por array de storage.
- Se apenas um volume tiver o cache SSD ativado, todo o cache SSD será atribuído ao controlador proprietário desse volume.
- A capacidade máxima de SSD Cache utilizável em um array de storage depende da capacidade do cache primário do controlador.
- O SSD Cache não é compatível com imagens de snapshot.
- Se você importar ou exportar volumes que estão com SSD Cache ativado ou desativado, os dados em cache não serão importados ou exportados.
- Qualquer volume atribuído ao uso do SSD Cache de um controlador não é elegível para transferência automática de load balance.
- Se os volumes associados tiverem a segurança habilitada, crie um SSD Cache com segurança habilitada.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Clique no menu: criar [Cache SSD].

   A caixa de diálogo Criar SSD Cache é exibida.

3. Digite um nome para o SSD Cache.
4. Selecione o candidato a SSD Cache que deseja usar com base nas seguintes características.

Característica	Usar
Capacidade	Exibe a capacidade disponível em GiB. Selecione a capacidade para as necessidades de storage da sua aplicação. A capacidade máxima do SSD Cache depende da capacidade do cache primário do controlador. Se você alocar mais do que o máximo para o SSD Cache, qualquer capacidade extra ficará inutilizável. A capacidade do SSD Cache conta para a sua capacidade total alocada.
Total de drives	Mostra o número de unidades disponíveis para este cache SSD. Selecione o candidato a SSD com o número de unidades que você deseja.
Compatível com segurança	Indica se o candidato a cache SSD é composto inteiramente de unidades com capacidade de segurança, que podem ser unidades Full Disk Encryption (FDE) ou Federal Information Processing Standard (FIPS). Se você deseja criar um cache SSD com segurança habilitada, procure por **Sim - FDE** ou **Sim - FIPS** na coluna Secure-capable.
Ativar segurança?	Oferece a opção de ativar o recurso de Segurança da Unidade em unidades compatíveis com segurança. Se você deseja criar um SSD Cache com segurança ativada, selecione a caixa de seleção Enable Security. Uma vez ativada, a segurança não pode ser desativada. Você pode ativar a segurança no SSD Cache somente ao criá-lo, não depois.
Compatível com DA	Indica se o Data Assurance (DA) está disponível para este candidato a SSD Cache. O Data Assurance (DA) verifica e corrige erros que possam ocorrer durante a transferência de dados pelos controladores até as unidades. Se você deseja usar DA, selecione um candidato a cache SSD que seja compatível com DA. Essa opção está disponível somente quando o recurso DA foi ativado. O cache SSD pode conter unidades compatíveis com DA e unidades não compatíveis com DA, mas todas as unidades devem ser compatíveis com DA para que você possa usar DA.

5. Associe o SSD Cache aos volumes para os quais você deseja implementar o armazenamento em cache de leitura SSD. Para habilitar o SSD Cache em volumes compatíveis imediatamente, selecione a caixa de seleção **Habilitar SSD Cache em volumes compatíveis existentes que estão mapeados para hosts**.

   Os volumes são compatíveis se compartilharem os mesmos recursos de Drive Security e DA.

6. Clique em **Create**.

Alterar as configurações de cache SSD no SANtricity System Manager

Você pode editar o nome do SSD Cache e visualizar seu status, capacidade máxima e atual, status de Drive Security e Data Assurance, além de seus volumes e unidades associados.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione o SSD Cache que deseja editar e clique em **Exibir/Editar configurações**.

   A caixa de diálogo Configurações de cache do SSD é exibida.

3. Revise ou edite as configurações de armazenamento em cache do SSD conforme necessário.

Detalhes do campo

Configuração	Descrição
Nome	Exibe o nome do cache SSD, que você pode alterar. Um nome para o cache SSD é necessário.
Características	Exibe o status do cache SSD. Status possíveis incluem: • Ideal • Desconhecido • Degradado • Falha (um estado de falha resulta em um evento MEL crítico.) • Suspenso
Capacidades	Mostra a capacidade atual e a capacidade máxima permitida para o SSD Cache. A capacidade máxima permitida para o cache SSD depende do tamanho do cache primário do controlador: • Até 1 GiB • 1 GiB a 2 GiB • 2 GiB a 4 GiB • Mais de 4 GiB
Segurança e DA	Exibe o status de segurança da unidade e garantia de dados para o SSD Cache. • **Compatível com segurança** — Indica se o cache SSD é composto inteiramente por unidades compatíveis com segurança. Uma unidade compatível com segurança é uma unidade com criptografia automática que pode proteger seus dados contra acesso não autorizado. • **Secure-enabled** — Indica se a segurança está ativada no cache SSD. • **Compatível com DA** — Indica se o cache SSD é composto inteiramente por unidades compatíveis com DA. Uma unidade compatível com DA pode verificar e corrigir erros que possam ocorrer durante a comunicação de dados entre o host e o array de storage.
Objetos associados	Exibe os volumes e drives associados ao cache SSD.

4. Clique em **Salvar**.

Visualize estatísticas de cache SSD no SANtricity System Manager

Você pode visualizar estatísticas do cache SSD, como leituras, gravações, acerto do

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

As estatísticas nominais, que são um subconjunto das estatísticas detalhadas, são exibidas na caixa de diálogo Exibir Estatísticas do Cache SSD. Você pode visualizar as estatísticas detalhadas do Cache SSD somente ao exportar todas as estatísticas do SSD para um arquivo `.csv`.

Ao analisar e interpretar as estatísticas, lembre-se de que algumas interpretações são derivadas pela análise de uma combinação de estatísticas.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione o cache SSD para o qual deseja visualizar estatísticas e clique em **Mais › Visualizar estatísticas do cache SSD**.

   A caixa de diálogo Exibir Estatísticas do Cache SSD é exibida e exibe as estatísticas nominais do cache SSD selecionado.

Detalhes do campo

Configurações	Descrição
Leituras	Mostra o número total de leituras do host nos volumes com SSD Cache ativado. Quanto maior a proporção de leituras para gravações, melhor é a operação do cache.
Gravações	O número total de gravações do host nos volumes com SSD Cache ativado. Quanto maior a proporção entre leituras e gravações, melhor é a operação do cache.
Acertos do cache	Mostra o número de acertos do cache.
Acertos do cache %	Mostra a porcentagem de acerto do cache. Esse número é derivado de acerto do cache / (leituras + gravações). A porcentagem de acerto do cache deve ser superior a 50 por cento para uma operação eficaz do SSD Cache.
Alocação %	Mostra a porcentagem do armazenamento em cache SSD que está alocada, expressa como uma porcentagem do armazenamento em cache SSD disponível para este controlador e é derivada de bytes alocados / bytes disponíveis.
Utilização do cache %	Mostra a porcentagem do armazenamento em cache SSD que contém dados de volumes habilitados, expressa como uma porcentagem do armazenamento em cache SSD alocado. Esse valor representa a utilização ou densidade do SSD Cache. Derivado de bytes alocados / bytes disponíveis.
Exportar tudo	Exporta todas as estatísticas do SSD Cache para o formato CSV. O arquivo exportado contém todas as estatísticas disponíveis para o SSD Cache (tanto nominais quanto detalhadas).

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

Gerenciar capacidade reservada

Como funciona a capacidade reservada no SANtricity software

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

A finalidade da capacidade reservada é armazenar as alterações de dados nesses volumes, caso algo dê errado. Assim como os 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 Snapshot
- Volumes Snapshot de leitura/gravação
- Volumes de membros do grupo de consistência
- Volumes de pares espelhados

Ao criar ou expandir esses objetos de serviço de cópia, você deve criar nova capacidade reservada a partir de um pool ou grupo de volume. A capacidade reservada geralmente corresponde a 40 por cento do volume base para operações de Snapshot e 20 por cento do volume base para operações de espelhamento assíncrono. No entanto, a capacidade reservada varia dependendo do número de alterações nos dados originais.

Volumes finos e capacidade reservada

Para um volume fino, se a capacidade máxima relatada de 256 TiB for atingida, você não poderá aumentar sua capacidade. Certifique-se de que a capacidade reservada do volume fino esteja definida para um tamanho maior que a capacidade máxima relatada. (Um volume fino é sempre thinly-provisioned, o que significa que a capacidade é alocada à medida que os dados são 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 thin falhar, o próprio volume thin não entrará automaticamente no estado Failed. No entanto, como todas as operações de E/S em um volume thin exigem acesso ao volume de capacidade reservada, as operações de E/S sempre resultarão em uma Check Condition sendo retornada ao host solicitante. Se o problema subjacente com o volume de capacidade reservada puder ser resolvido, o volume de capacidade reservada retornará ao estado Optimal e o volume thin voltará a funcionar.
- Se você usar um volume fino existente para concluir um par espelhado assíncrono, esse volume fino será reinicializado com um novo volume de capacidade reservada. Somente os blocos provisionados no lado primário são transferidos durante o processo de sincronização inicial.

Alertas de capacidade

O objeto de serviço de cópia possui um aviso e limite de alerta de capacidade configurável, 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 limite de preenchimento, um alerta é emitido para o usuário. Por padrão, esse alerta é emitido quando o volume de capacidade reservada está 75 por cento cheio; no entanto, você pode ajustar esse ponto de alerta para cima ou para baixo conforme necessário. Se você receber esse alerta, pode aumentar a capacidade do volume de capacidade reservada nesse momento. Cada objeto de serviço de cópia pode ser configurado independentemente nesse aspecto.

Volumes de capacidade reservada órfãos

Um volume de capacidade reservada órfão é um volume que não armazena mais dados para operações do 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 deveria ter sido excluído. No entanto, o volume de capacidade reservada não foi excluído.

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 órfão para que você possa usar sua capacidade para outras operações.

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

Características da capacidade reservada

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

Aumentar a capacidade reservada no SANtricity System Manager

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

Para operações de Snapshot, normalmente é 40 por cento do volume base; para operações de espelhamento assíncrono, normalmente é 20 por cento 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 volume deve ter um status Ótimo e não deve estar em nenhum estado de modificação.
- Deve haver capacidade livre no pool ou volume group que você deseja usar para aumentar a capacidade.

  Se não houver capacidade livre em nenhum pool ou grupo de volume, você pode adicionar capacidade não atribuída na forma de drives não utilizados a um pool ou grupo de volume.

Sobre esta tarefa

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

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

Use uma porcentagem alta se você acredita que o volume principal sofrerá muitas alterações ou se a vida útil de uma determinada operação de serviço de cópia for muito longa.

Não é possível aumentar a capacidade reservada para um volume de snapshot que seja somente leitura. Apenas volumes de snapshot que sejam de leitura e gravação requerem capacidade reservada.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione a guia **Capacidade Reservada**.
3. Selecione o objeto de storage para o qual deseja aumentar a capacidade reservada e clique em **Aumentar capacidade**.

   A caixa de diálogo Increase Reserved Capacity é exibida.

4. Use a caixa de rotação para ajustar a porcentagem de capacidade.

   Se não houver capacidade livre no pool ou grupo de volume que contém o objeto de armazenamento selecionado, e o array de storage tiver capacidade não atribuída, você pode criar um novo pool ou grupo de volume. Você pode então tentar novamente esta operação usando a nova capacidade livre nesse pool ou grupo de volume.

5. Clique em **Increase**.

Resultados

System Manager executa as seguintes ações:

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

Diminuir a capacidade reservada no SANtricity System Manager

Você usa a opção Diminuir Capacidade para diminuir a capacidade reservada dos seguintes objetos de storage: grupo de snapshot, volume de snapshot e volume membro de grupo de consistência. Você só pode diminuir a capacidade reservada pela(s) mesma(s) quantidade(s) que usou para aumentá-la.

Antes de começar

- O objeto de armazenamento deve conter mais de um volume de capacidade reservada.
- O objeto de armazenamento não deve ser um volume de par espelhado.
- Se o objeto de armazenamento for um volume de snapshot, então ele deve ser um volume de snapshot desativado.
- Se o objeto de armazenamento for um grupo de instantâneos, então ele não deve conter nenhuma imagem de instantâneo associada.

Sobre esta tarefa

Revise as seguintes diretrizes:

- Você pode remover volumes de capacidade reservada apenas na ordem inversa em que foram adicionados.
- Não é possível diminuir a capacidade reservada para um volume de snapshot que seja somente leitura porque ele não possui nenhuma capacidade reservada associada. Somente volumes de snapshot que

sejam de leitura e gravação requerem capacidade reservada.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Clique na guia **Capacidade Reservada**.
3. Selecione o objeto de storage para o qual deseja diminuir a capacidade reservada e clique em **Diminuir capacidade**.

   A caixa de diálogo Diminuir Capacidade Reservada é exibida.

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

Resultados

System Manager executa as seguintes ações:

- Atualiza a capacidade do objeto de storage.
- Exibe a capacidade reservada recém-atualizada para o objeto de storage.
- Ao diminuir a capacidade de um volume de snapshot, System Manager automaticamente faz a transição do volume de snapshot para o estado Desativado. Desativado significa que o volume de snapshot não está atualmente associado a uma imagem de snapshot e, portanto, não pode ser atribuído a um host para E/S.

Altere as configurações de capacidade reservada para um grupo de Snapshot no SANtricity System Manager

Você pode alterar as configurações de um grupo de Snapshot para alterar seu nome, as configurações de exclusão automática, o número máximo de imagens de Snapshot permitidas, o ponto percentual em que o SANtricity System Manager envia uma notificação de alerta de capacidade reservada ou a política a ser usada quando a capacidade reservada atingir sua porcentagem máxima definida.

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

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Clique na guia **Capacidade Reservada**.
3. Selecione o grupo de Snapshot que deseja editar e clique em **Exibir/Editar configurações**.

   A caixa de diálogo Snapshot Group Settings é exibida.

4. Altere as configurações do grupo de Snapshot conforme necessário.

Detalhes do campo

Configuração	Descrição
Configurações do grupo de Snapshot	Nome
O nome do grupo de Snapshot. É obrigatório especificar um nome para o grupo de Snapshot.	Exclusão automática
Uma configuração que mantém o número total de imagens de Snapshot no grupo igual ou inferior a um máximo definido pelo usuário. Quando esta opção está ativada, System Manager exclui automaticamente a imagem de Snapshot mais antiga do grupo sempre que um novo Snapshot é criado, para respeitar o número máximo de imagens de Snapshot permitidas para o grupo.	Limite de imagens do Snapshot
Um valor configurável que especifica o número máximo de imagens de Snapshot permitidas para um grupo de Snapshot.	Agendamento do Snapshot
Em caso afirmativo, um agendamento é definido para criar Snapshots automaticamente.	**Configurações de capacidade reservada**

Configuração	Descrição
Avise-me quando…	Use o controle de rotação para ajustar o ponto percentual em que System Manager envia uma notificação de alerta quando a capacidade reservada para um grupo de Snapshot estiver quase cheia. Quando a capacidade reservada para o grupo de Snapshot excede o limite especificado, System Manager envia um alerta, permitindo que você aumente a capacidade reservada ou exclua objetos desnecessários.
Política para capacidade totalmente reservada	Você pode escolher uma das seguintes políticas: • **Excluir imagem de snapshot mais antiga** — System Manager exclui automaticamente a imagem de snapshot mais antiga no grupo de snapshots, o que libera a capacidade reservada da imagem de snapshot para reutilização dentro do grupo. • **Rejeitar gravações no volume base** — Quando a capacidade reservada atinge a porcentagem máxima definida, 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 usado para o grupo. Um volume base é a origem a partir da qual uma imagem de Snapshot é criada. Pode ser um volume espesso ou fino e normalmente é atribuído a um host. O volume base pode residir em um grupo de volume ou em um pool de discos.	Imagens de Snapshot

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

Altere as configurações de capacidade reservada para um volume de Snapshot no SANtricity System Manager

Você pode alterar as configurações de um volume de snapshot para ajustar a porcentagem em que o sistema envia uma notificação de alerta quando a capacidade reservada para um volume de snapshot estiver quase cheia.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].

2. Clique na guia **Capacidade Reservada**.
3. Selecione o volume de Snapshot que você deseja editar e clique em **View/Edit Settings**.

   A caixa de diálogo Snapshot Volume Reserved Capacity Settings é exibida.

4. Altere as configurações de capacidade reservada para o volume de Snapshot conforme necessário.

   Detalhes do campo

Configuração	Descrição
Avise-me quando…	Use o seletor para ajustar o ponto percentual em que o sistema envia uma notificação de alerta quando a capacidade reservada para um volume de membro estiver quase cheia. Quando a capacidade reservada para o volume de Snapshot excede o limite especificado, o sistema envia um alerta, permitindo que você aumente a capacidade reservada ou exclua objetos desnecessários.

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

Altere as configurações de capacidade reservada para um volume membro de grupo de consistência no SANtricity System Manager

Você pode alterar as configurações de um volume membro de grupo de consistência para ajustar a porcentagem em que o SANtricity System Manager envia uma notificação de alerta quando a capacidade reservada para um volume 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 de membro associados a um grupo de consistência.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Clique na guia **Capacidade Reservada**.
3. Selecione o volume 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 de membro conforme apropriado.

Detalhes do campo

Configuração	Descrição
Avise-me quando…	Use o seletor giratório para ajustar o ponto percentual em que System Manager envia uma notificação de alerta quando a capacidade reservada para um volume de membro estiver quase cheia. Quando a capacidade reservada para o volume do membro excede o limite especificado, System Manager envia um alerta, permitindo que você aumente a capacidade reservada ou exclua objetos desnecessários. Alterar a configuração de alerta para um volume membro alterará para *todos* os volumes membros que pertencem ao mesmo grupo de consistência.
Política para capacidade totalmente reservada	Você pode escolher uma das seguintes políticas: • **Excluir imagem de Snapshot mais antiga** — System Manager exclui automaticamente a imagem de Snapshot mais antiga no grupo de consistência, o que libera a capacidade reservada do membro para reutilização dentro do grupo. • **Rejeitar gravações no volume base** — Quando a capacidade reservada atinge a porcentagem máxima definida, 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

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

Altere as configurações de capacidade reservada para um volume de par espelhado no SANtricity System Manager

Você pode alterar as configurações de um volume de par espelhado para ajustar o ponto percentual em que SANtricity System Manager envia uma notificação de alerta quando a capacidade reservada para um volume de par espelhado está quase cheia.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione a guia **Capacidade Reservada**.
3. Selecione o par de volumes espelhados que deseja editar e clique em **Visualizar/Editar Settings**.

   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

Configuração	Descrição
Avise-me quando…	Use o seletor giratório para ajustar o ponto percentual em que System Manager envia uma notificação de alerta quando a capacidade reservada para um par espelhado estiver quase cheia. Quando a capacidade reservada para o par espelhado excede o limite especificado, System Manager envia um alerta, permitindo que você aumente a capacidade reservada. Alterar a configuração de alerta para um par espelhado altera a configuração de alerta para todos os pares espelhados que pertencem ao mesmo grupo de consistência de espelhamento.

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

Cancelar uma imagem de Snapshot pendente no SANtricity System Manager

Você pode cancelar uma imagem de snapshot pendente antes que ela seja concluída. Os snapshots ocorrem de forma assíncrona e o status do snapshot é pendente até que o snapshot seja concluído. A imagem do snapshot é concluída assim que a operação de sincronização é concluída.

Sobre esta tarefa

Uma imagem de Snapshot está em estado Pendente devido às seguintes condições simultâneas:

- O volume base para um grupo de snapshot ou um ou mais volumes membros de um grupo de consistência que contém esta imagem de snapshot é membro de um grupo de espelhamento assíncrono.
- O(s) volume(s) encontra(m)-se atualmente em uma operação de sincronização de espelhamento assíncrono.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Clique na guia **Capacidade Reservada**.
3. Selecione o grupo de snapshot para o qual deseja cancelar uma imagem de snapshot pendente e clique em **Tarefas incomuns › Cancelar imagem de snapshot pendente**.
4. Clique em **Sim** para confirmar que deseja cancelar a imagem de snapshot pendente.

Excluir um grupo de Snapshot no SANtricity System Manager

Você exclui um grupo de snapshot quando deseja excluir permanentemente seus dados e removê-lo do sistema. Excluir um grupo de snapshot libera a capacidade reservada para reutilização no pool ou grupo de volume.

Sobre esta tarefa

Quando um grupo de Snapshot é excluído, todas as imagens de Snapshot do grupo também são excluídas.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Clique na guia **Capacidade Reservada**.
3. Selecione o grupo de snapshot que você deseja excluir e clique em **Uncommon Tasks › Delete snapshot group**.

   A caixa de diálogo Confirmar Exclusão do Snapshot Group é exibida.

4. Digite `delete` para confirmar.

Resultados

System Manager executa as seguintes ações:

- Exclui todas as imagens de Snapshot associadas ao grupo de Snapshot.
- Desativa quaisquer volumes de snapshot associados às imagens do grupo de snapshot.
- Exclui a capacidade reservada que existe para o grupo de snapshot.

Perguntas frequentes sobre pools e grupos de volume para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

O que é um grupo de volume?

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

O que é um pool?

Um pool é um conjunto de unidades agrupadas 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 volume.)

Os pools podem eliminar a necessidade de os administradores monitorarem o uso em cada host para determinar quando é provável que fiquem sem espaço de storage e evitar interrupções convencionais para redimensionamento de discos. Quando um pool se aproxima do esgotamento, unidades adicionais podem ser adicionadas ao pool sem interrupção 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 de reserva por todo o pool, cada unidade no pool pode ser usada para reconstruir uma unidade com falha. Essa abordagem não utiliza unidades hot spare dedicadas; em vez disso, a capacidade de preservação (reserva) é reservada em todo o pool. Quando uma unidade falha, os segmentos em outras unidades são lidos para recriar os dados. Uma nova unidade é então 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 capacidade reservada?

A capacidade reservada é a capacidade fisicamente alocada que armazena dados para objetos do serviço de cópia, como imagens de instantâneo, volumes de membros de 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 um grupo de volume. Você cria capacidade reservada a partir de um pool ou grupo de volume.

O que é segurança FDE/FIPS?

A segurança FDE/FIPS refere-se a unidades com recursos de segurança que criptografam os dados durante as gravações e descriptografam os dados durante as leituras, utilizando uma chave de criptografia exclusiva. Essas unidades com recursos de segurança impedem o acesso não autorizado aos dados em uma unidade que esteja fisicamente removida do array de storage.

Unidades com recursos de segurança podem ser unidades com criptografia de disco completa (FDE) ou unidades Federal Information Processing Standard (FIPS). Unidades FIPS passaram por testes de certificação.

> Para volumes que exigem suporte FIPS, use somente unidades FIPS. Misturar unidades FIPS e FDE em um grupo de volume ou pool fará com que todas as unidades sejam tratadas como unidades FDE. Além disso, uma unidade FDE não pode ser adicionada ou usada como hot spare em um grupo de volume ou pool totalmente FIPS.

O que é verificação de redundância?

Uma verificação de redundância determina se os dados em um volume de um pool ou grupo de volume são consistentes. Os dados de redundância são usados para reconstruir rapidamente as informações em uma unidade de substituição caso uma das unidades do pool ou grupo de volume falhe.

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

- Analisa 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. (RAID 3 só pode ser atribuído a grupos de volume usando a interface de linha de comando.)
- Compara os blocos de dados em unidades RAID 1 espelhadas.
- 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 volume pode causar um erro. Para evitar esse problema, aguarde de 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 volume groups?

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, diferentemente dos dados em um grupo de volume, que são armazenados no mesmo conjunto de unidades.
- Um pool apresenta menor degradação de desempenho quando uma unidade falha e leva menos tempo

para ser reconstruído.

- Um pool possui 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 iria querer configurar um pool manualmente?

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

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

  Você pode atribuir apenas um ou dois volumes em vez de atribuir a carga de trabalho a um pool grande que tem muitos volumes nos quais distribuir os dados. Criar manualmente um pool separado dedicado à carga de trabalho de um aplicativo específico pode permitir que as operações do array de storage sejam executadas mais rapidamente, com menos contenção.

  Para criar um pool manualmente: selecione **Armazenamento** e, em seguida, selecione **Pools & Volume Groups**. Na guia All Capacity, clique em **Create › Pool**.

- Se houver vários pools do mesmo tipo de unidade, uma mensagem será exibida indicando que 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 unidades manualmente a um pool existente: na página Pools & Volume Groups, selecione o pool e clique em **Adicionar Capacidade**.

Por que os alertas de capacidade são importantes?

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

Você define essa porcentagem ao criar um pool usando a opção **Configuração automática do pool** ou a opção **Criar pool**. Se escolher a opção automática, as configurações padrão determinam automaticamente quando você recebe notificações de alerta. Se optar por criar o pool manualmente, você pode definir as configurações de notificação de alerta; ou, se preferir, pode aceitar as configurações padrão. Você pode ajustar essas configurações depois em **Configurações › Alertas**.

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

Por que não posso aumentar minha capacidade de preservação?

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

A capacidade de preservação é a quantidade de capacidade (número de unidades) reservada em um pool para suportar possíveis falhas de unidades. 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 criou volumes em toda a capacidade utilizável disponível, não poderá aumentar a capacidade de preservação sem adicionar capacidade ao pool, seja adicionando unidades ou excluindo volumes.

Você pode alterar a capacidade de preservação em **Pools & Volume Groups**. Selecione o pool que você deseja editar. Clique em **View/Edit Settings** e, em seguida, selecione a guia **Settings**.

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

Existe um limite para o número de unidades que posso remover de um pool?

SANtricity 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 menos de 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 forem redistribuídos para as unidades restantes no pool.
- Você pode remover no máximo 60 unidades por 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?

Os seguintes tipos de mídia são suportados: Hard Disk Drive (HDD) e Solid State Disk (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 volume.

As unidades não são elegíveis por nenhum dos seguintes motivos:

- A unidade deve estar desatribuída e não habilitada para segurança. Unidades que já fazem parte de outro pool, outro grupo de volume ou que estejam configuradas como hot spare não são elegíveis. Se uma unidade estiver desatribuída, mas estiver habilitada para segurança, você deverá apagá-la manualmente para que se torne elegível.
- Uma unidade que está em um estado não ideal não é elegível.
- Se a capacidade de uma unidade for muito pequena, ela não será elegível.
- O tipo de mídia da unidade deve corresponder dentro de um pool ou grupo de volume. Você não pode misturar o seguinte:
  - Unidades de disco rígido (HDDs) com Solid State Disks (SSDs)
  - NVMe com unidades SAS
  - Unidades com tamanhos de bloco de volume de 512 bytes e 4KiB
- Se um pool ou grupo de volume contiver apenas unidades com capacidade de segurança, as unidades sem capacidade de segurança não serão listadas.
- Se um pool ou grupo de volume contiver todas as unidades Federal Information Processing Standards (FIPS), as unidades não FIPS não serão listadas.
- Se um pool ou grupo de volume contiver todas as unidades compatíveis com Data Assurance (DA) e houver pelo menos um volume com DA habilitado nesse pool ou grupo de volume, uma unidade que não

seja compatível com DA não será elegível, portanto, não poderá ser adicionada a esse pool ou grupo de volume. No entanto, se não houver nenhum volume com DA habilitado no pool ou grupo de volume, uma unidade que não seja compatível com DA pode ser adicionada a esse pool ou grupo de volume. Se você decidir misturar essas unidades, lembre-se de que não poderá criar nenhum volume com DA habilitado.

A capacidade pode ser aumentada no seu array de storage 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 perdas em prateleiras/gavetas para um pool ou grupo de volume, utilize os critérios especificados na tabela a seguir.

Nível	Critérios para proteção contra perda de prateleira/gaveta	Número mínimo de prateleiras/gavetas necessárias
Pool	Para prateleiras, o pool não deve conter mais de duas unidades em uma única prateleira. Para gavetas, o pool deve incluir um número igual de unidades de cada gaveta.	6 para prateleiras 5 para gavetas
RAID 6	O grupo de volume contém no máximo duas unidades em uma única shelf ou drawer.	3
RAID 3 ou RAID 5	Cada unidade no grupo de volume está localizada em uma prateleira ou gaveta separada.	3
RAID 1	Cada unidade em um par espelhado deve estar localizada em uma prateleira ou gaveta separada.	2
RAID 0	Não é possível obter proteção contra perda de shelf/drawer.	Não aplicável

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

Qual é o posicionamento ideal das unidades para pools e grupos de volume?

Ao criar pools e grupos de volume, certifique-se de equilibrar a seleção de unidades entre os slots de unidade superiores e inferiores.

Nos controladores EF600 e EF300, os slots de unidade 0 a 11 estão conectados a uma ponte PCI, enquanto os slots 12 a 23 estão conectados a outra ponte PCI. Para desempenho ideal, você deve equilibrar a seleção

das unidades para incluir um número aproximadamente igual de unidades nos slots superiores e inferiores. Esse posicionamento garante que seus volumes não atinjam um limite de largura de banda antes do necessário.

Qual nível RAID é o melhor para minha aplicação?

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

Níveis RAID e desempenho do aplicativo

RAID utiliza uma série de configurações, chamadas de *níveis*, para determinar como os dados do usuário e os dados de redundância são gravados e recuperados das unidades. Cada nível RAID oferece diferentes recursos de desempenho. Aplicativos com alta porcentagem de leitura terão um bom desempenho usando volumes RAID 5 ou volumes RAID 6 devido ao excelente desempenho de leitura das configurações RAID 5 e RAID 6.

Aplicações com baixa porcentagem de leitura (uso intensivo de escrita) não apresentam o mesmo desempenho em volumes RAID 5 ou volumes RAID 6. A degradação de desempenho resulta da forma como o controlador grava dados e dados de redundância nas unidades em um grupo de volume RAID 5 ou um grupo de volume RAID 6.

Selecione um nível RAID com base nas seguintes informações.

RAID 0

- **Descrição**
  - Não redundante, modo de striping.
- **Como funciona**
  - RAID 0 distribui os dados por todas as unidades do grupo de volume.
- **Recursos de proteção de dados**
  - RAID 0 não é recomendado para necessidades de alta disponibilidade. RAID 0 é mais adequado para dados não críticos.
  - Se uma unidade única falhar no grupo de volume, todos os volumes associados falham e todos os dados são perdidos.
- **Requisitos de número de unidades**
  - É necessário no mínimo um disco rígido para o nível RAID 0.
  - Grupos de volume RAID 0 podem ter mais de 30 unidades.
  - Você pode criar um grupo de volume que inclua todas as unidades no storage array.

RAID 1 ou RAID 10

- **Descrição**
  - Modo striping/espelhamento.
- **Como funciona**
  - RAID 1 utiliza espelhamento de disco para gravar dados em dois discos duplicados simultaneamente.
  - RAID 10 usa o striping de unidades para distribuir os dados entre 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 o 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 array de storage pode alternar instantaneamente para a outra unidade sem qualquer perda de dados ou serviço.
  - A falha de uma unidade única faz com que os volumes associados fiquem degradados. A unidade espelhada permite o acesso aos dados.
  - A falha de um par de unidades em um grupo de volume causa a falha de todos os volumes associados, e pode ocorrer perda de dados.
- **Requisitos de número de unidades**
  - É necessário um mínimo de duas unidades para RAID 1: uma unidade para os dados de usuário e uma unidade para os dados espelhados.
  - Se você selecionar quatro ou mais unidades, RAID 10 é configurado automaticamente em todo o grupo de volume: duas unidades para dados de usuário e duas unidades para os dados espelhados.
  - Você precisa ter um número par de unidades no grupo de volume. Se você não tiver um número par de unidades e ainda tiver algumas unidades não atribuídas, acesse **Pools & Volume Groups** para adicionar unidades adicionais ao grupo de volume e tente a operação novamente.
  - Os grupos de volume RAID 1 e RAID 10 podem ter mais de 30 unidades. Um grupo de volume pode ser criado que inclua todas as unidades no array de storage.

RAID 5

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

RAID 6

- **Descrição**
  - Modo de alta E/S.
- **Como funciona**
  - Os dados de 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 volume 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 volume RAID 6, todos os volumes associados falharão e todos os dados serão perdidos.
- **Requisitos de número de unidades**
  - Você deve ter no mínimo cinco drives no grupo de volume.
  - Normalmente, você está limitado a um máximo de 30 drives no grupo de volume.

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

Níveis RAID e proteção de dados

RAID 1, RAID 5 e RAID 6 gravam dados de redundância na mídia do disco para tolerância de 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 um disco de substituição caso um disco falhe.

Você configura um único nível RAID em um único grupo de volume. Todos os dados de redundância para esse grupo de volume são armazenados dentro do grupo de volume. A capacidade do grupo de volume 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 utilizado.

O que é Data Assurance?

A Garantia de Dados (DA) implementa o padrão T10 Protection Information (PI), que aumenta a integridade de dados ao verificar e corrigir erros que possam ocorrer durante a transferência de dados ao longo do caminho de E/S.

O uso típico do recurso Data Assurance consiste em verificar a porção do caminho de E/S entre os controladores e as unidades. Os recursos de DA são apresentados nos níveis de pool e grupo de volume.

Quando esse recurso está habilitado, o array de storage anexa códigos de verificação de erros (também conhecidos como verificações de redundância cíclica ou CRCs) a cada bloco de dados no volume. Após a movimentação de um bloco de dados, o array de storage usa esses códigos CRC para determinar se ocorreram erros durante a transmissão. Dados potencialmente corrompidos não são gravados em disco nem retornados ao host. Se você deseja usar o recurso DA, selecione um pool ou grupo de volume compatível com DA ao criar um novo volume (procure por "Sim" ao lado de "DA" na tabela de candidatos de pool e grupo de volumes).

Certifique-se de atribuir esses volumes habilitados para DA a um host usando uma interface de E/S compatível com DA. Interfaces de E/S compatíveis com DA incluem Fibre Channel, SAS, iSCSI sobre TCP/IP, NVMe/FC, NVMe/IB, NVMe/RoCE e iSER sobre InfiniBand (iSCSI Extensions for RDMA/IB). DA não é compatível com SRP sobre InfiniBand.

O que é secure-capable (Drive Security)?

A Segurança de Unidade é um recurso que impede o acesso não autorizado a dados em unidades com segurança habilitada quando removidas do array de storage. Essas unidades podem ser unidades Full Disk

Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS).

O que preciso saber sobre o aumento da capacidade reservada?

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

- Você deve ter capacidade livre suficiente no pool ou grupo de volume para que ele possa ser expandido se necessário.

  Se não houver capacidade livre em nenhum pool ou grupo de volume, você pode adicionar capacidade não atribuída na forma de drives não utilizados a um pool ou grupo de volume.

- O volume no pool ou grupo de volume deve ter um status Ótimo e não deve estar em nenhum estado de modificação.
- Deve haver capacidade livre no pool ou volume group que você deseja usar para aumentar a capacidade.
- Não é possível aumentar a capacidade reservada para um volume de snapshot que seja somente leitura. Apenas volumes de snapshot que sejam de leitura e gravação requerem capacidade reservada.

Para operações de snapshot, a capacidade reservada normalmente corresponde a 40% do volume base. Para operações de espelhamento assíncrono, a capacidade reservada normalmente corresponde a 20% do volume base. Use uma porcentagem maior se você acredita que o volume base sofrerá muitas alterações ou se a expectativa de vida útil da operação de serviço de cópia de um objeto de storage for muito longa.

Por que não posso escolher outro valor para diminuir?

Você só pode diminuir a capacidade reservada na mesma proporção em que a aumentou. A capacidade reservada para volumes de membros só pode ser removida na ordem inversa em que foram adicionados.

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

- Se o objeto de armazenamento for um volume de par espelhado.
- Se o objeto de armazenamento contiver apenas um volume para capacidade reservada. O objeto de armazenamento deve conter pelo menos dois volumes para capacidade reservada.
- Se o objeto de armazenamento for um volume de snapshot desativado.
- Se o objeto de armazenamento contiver uma ou mais imagens de snapshot 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 de snapshot que seja somente leitura porque ele não possui nenhuma capacidade reservada associada. Somente volumes de snapshot que sejam de leitura e gravação requerem capacidade reservada.

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

Cada volume 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 membro designado como leitura/gravação.

Uma imagem de snapshot de grupo de consistência não é diretamente acessível para leitura ou gravação pelos hosts. Em vez disso, a imagem de snapshot é usada para salvar apenas os dados capturados do

volume base.

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

Como faço para visualizar e interpretar todas as estatísticas do SSD Cache?

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

As estatísticas detalhadas só podem ser visualizadas ao exportar todas as estatísticas de SSD para um `.csv` arquivo. Ao analisar e interpretar as estatísticas, lembre-se de que algumas interpretações são derivadas da análise de uma combinação de estatísticas.

Estatísticas nominais

Para visualizar as estatísticas do SSD Cache, selecione **Storage › Pools & Volume Groups**. Selecione o SSD Cache para o qual deseja visualizar as estatísticas e, em seguida, selecione **More › View Statistics**. As estatísticas nominais são exibidas na caixa de diálogo Exibir Estatísticas do SSD Cache.

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

Estatística nominal	Descrição
Leituras/Gravações	O número total de leituras do host ou gravações do host nos volumes com SSD Cache ativado. Compare as leituras em relação às gravações. As leituras precisam ser maiores que as gravações para uma operação eficaz do SSD Cache. Quanto maior a proporção de leituras para gravações, melhor a operação do cache.
Acertos do cache	Uma contagem do número de acertos do cache.
Acertos do cache (%)	Derivado de acerto do cache / (leituras + gravações). A porcentagem de acerto do cache deve ser superior a 50 por cento para uma operação eficaz do cache SSD. Um número baixo pode indicar várias coisas: • A proporção de leituras para gravações é muito baixa • As leituras não são repetidas • A capacidade do cache é muito pequena
Alocação de cache (%)	A quantidade de armazenamento de cache SSD que está alocada, expressa como uma porcentagem do armazenamento de cache SSD que está disponível para este controlador. Derivada de bytes alocados / bytes disponíveis. A porcentagem de alocação de cache normalmente é exibida como 100 por cento. Se esse número for menor que 100 por cento, significa que o cache não foi aquecido ou que a capacidade do cache SSD é maior do que todos os dados acessados. No último caso, uma capacidade menor de cache SSD pode fornecer o mesmo nível de desempenho. Observe que isso não indica que os dados em cache foram colocados no cache SSD; é simplesmente uma etapa de preparação antes que os dados possam ser colocados no cache SSD.

Estatística nominal	Descrição
Utilização do cache (%)	A quantidade de armazenamento SSD Cache que contém dados de volumes habilitados, expressa como uma porcentagem do armazenamento SSD Cache que está alocado. Esse valor representa a utilização ou densidade do SSD Cache derivada da proporção de bytes de dados de usuário / bytes alocados. A porcentagem de utilização do cache normalmente é inferior a 100 por cento, podendo ser bem menor. Esse número mostra a porcentagem da capacidade do SSD Cache que está preenchida com dados de cache. Esse número é inferior a 100 por cento porque cada unidade de alocação do SSD Cache, o bloco do SSD Cache, é dividida em unidades menores chamadas sub-blocos, que são preenchidas de forma relativamente 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, além de estatísticas adicionais. Essas estatísticas adicionais são salvas juntamente com as estatísticas nominais, mas, diferentemente das estatísticas nominais, não são exibidas na caixa de diálogo Exibir Estatísticas do Cache SSD. Você pode visualizar as estatísticas detalhadas somente após exportar as estatísticas para um arquivo `.csv`.

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

Estatísticas detalhadas	Descrição
Blocos de leitura	O número de blocos em leituras do host.
Blocos de escrita	O número de blocos em gravações do host.
Blocos de acerto total	O número de blocos em acertos do cache. Os blocos de acerto completo indicam o número de blocos que foram lidos inteiramente do SSD Cache. O SSD Cache só é benéfico para o desempenho para aquelas operações que são acertos completos do cache.
Acertos parciais	O número de leituras do host em que pelo menos um bloco, mas não todos os blocos, estavam no SSD Cache. Um acerto parcial é um **miss** no SSD Cache, onde as leituras foram atendidas a partir do volume base.
Acertos Parciais - Blocos	O número de blocos em acertos parciais. Acertos parciais do cache e blocos de acerto parcial do cache resultam de uma operação que possui apenas uma parte de seus dados no SSD Cache. Nesse caso, a operação precisa obter os dados do volume do disco rígido (HDD) em cache. O SSD Cache não oferece nenhum benefício de desempenho para esse tipo de acerto. Se a contagem de blocos de acerto parcial do cache for maior que a de blocos de acerto completo do cache, um tipo diferente de característica de E/S (sistema de arquivos, banco de dados ou servidor web) poderia melhorar o desempenho. Espera-se que haja um número maior de acertos e falhas parciais em comparação com acertos de cache enquanto o SSD Cache estiver aquecendo.

Estatísticas detalhadas	Descrição
Perdas	O número de leituras do host em que nenhum dos blocos estava no SSD Cache. Uma falha de SSD Cache ocorre quando as leituras foram atendidas a partir do volume base. Espera-se que haja um número maior de acertos e falhas parciais em comparação com os acertos do cache enquanto o SSD Cache estiver aquecendo.
Perdas - Blocos	O número de blocos em Misses.
Ações de preenchimento (leituras do host)	O número de leituras do host em que os dados foram copiados do volume base para o SSD Cache.
Preencher ações (leituras do host) - blocos	O número de blocos em Populate Actions (Host Reads).
Ações de preenchimento (escritas do host)	O número de gravações do host em que os dados foram copiados do volume base para o SSD Cache. A contagem de Populate Actions (Host Writes) pode ser zero para as configurações de cache que não preenchem o cache como resultado de uma operação de gravação de E/S.
Ações de preenchimento (Host Writes) - Blocos	O número de blocos em Populate Actions (Host Writes).
Invalidar ações	Número de vezes que os dados foram invalidados ou removidos do SSD Cache. Uma operação de invalidação de cache é realizada para cada solicitação de gravação do host, cada solicitação de leitura do host com Forced Unit Access (FUA), cada solicitação de verificação e em algumas outras circunstâncias.
Ações de reciclagem	O número de vezes que o bloco de 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 for próximo ao número combinado de leituras e gravações, o SSD Cache está apresentando thrashing. A capacidade do cache precisa ser aumentada ou a carga de trabalho não é adequada para uso com SSD Cache.
Bytes disponíveis	O número de bytes disponíveis no SSD Cache para uso por este controlador.
Bytes alocados	O número de bytes alocados do SSD Cache por este controlador. Os bytes alocados do SSD Cache podem estar vazios ou podem conter dados de volumes base.
Bytes de dados de usuário	O número de bytes alocados no cache SSD que contêm dados dos volumes base. Os bytes disponíveis, os bytes alocados e os bytes de dados de usuário são usados para calcular a porcentagem de alocação de cache e a porcentagem de utilização de cache.

O que é capacidade de otimização para pools?

Unidades SSD terão vida útil mais longa e melhor desempenho máximo de gravação quando uma parte de sua capacidade estiver não alocada.

Para unidades associadas a um pool, a capacidade não alocada é composta pela capacidade de preservação do pool, a capacidade livre (capacidade não utilizada pelos volumes) e uma porção da capacidade utilizável reservada como capacidade de otimização adicional. A capacidade de otimização adicional garante um nível mínimo de capacidade de otimização ao reduzir a capacidade utilizável e, assim, não está disponível para criação de volumes.

Ao criar um pool, é gerada uma capacidade de otimização recomendada que proporciona um equilíbrio entre desempenho, vida útil da unidade 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. Ajustar o controle deslizante proporciona melhor desempenho e vida útil da unidade à custa da capacidade disponível, ou capacidade disponível adicional à custa do desempenho e da vida útil da unidade.

> O controle deslizante de Capacidade de Otimização Adicional está disponível apenas para os sistemas de storage EF600 e EF300.

Qual é a capacidade de otimização para grupos de volume?

Unidades SSD terão vida útil mais longa e melhor desempenho máximo de gravação quando uma parte de sua capacidade estiver não alocada.

Para unidades associadas a um grupo de volume, a capacidade não alocada é composta pela capacidade livre do grupo de volume (capacidade não utilizada pelos volumes) e por uma porção da capacidade utilizável reservada como capacidade de otimização. A capacidade de otimização adicional garante um nível mínimo de capacidade de otimização ao reduzir a capacidade utilizável e, assim, não está disponível para criação de volumes.

Quando um grupo de volume é criado, uma capacidade de otimização recomendada é gerada que oferece um equilíbrio entre desempenho, vida útil do disco 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. Ajustar o controle deslizante proporciona melhor desempenho e vida útil do disco à custa da capacidade disponível, ou capacidade disponível adicional à custa do desempenho e da vida útil do disco.

> O controle deslizante de Capacidade de Otimização Adicional está disponível apenas para os sistemas de storage EF600 e EF300.

O que o provisionamento de recursos é capaz de fazer?

O Resource Provisioning é um recurso disponível nos sistemas de storage EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente, sem processo de inicialização em segundo plano.

Um volume com recursos provisionados é um volume espesso em um grupo de volume SSD ou pool, onde a capacidade do disco é alocada (atribuída ao volume) quando o volume é criado, mas os blocos do disco são desalocados (desmapeados). Em comparação, em um volume espesso tradicional, todos os blocos do disco são mapeados ou alocados durante uma operação de inicialização do volume em segundo plano para 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 com recursos provisionados, não há inicialização em segundo plano com limite de tempo. Em vez disso, cada faixa RAID é inicializada na primeira gravação em um bloco de volume na faixa.

Volumes provisionados por recurso são suportados apenas em grupos de volumes SSD e pools, onde todas as unidades no grupo ou pool suportam a capacidade de recuperação de erros NVMe Deallocated or Unwritten Logical Block Error Enable (DULBE). Quando um volume provisionado por recurso é criado, todos os blocos de unidade atribuídos ao volume são desalocados (desmapeados). Além disso, hosts podem desalocar blocos lógicos no volume usando o comando NVMe Dataset Management ou o comando SCSI Unmap. Desalocar blocos pode melhorar a vida útil do SSD e aumentar o desempenho máximo de gravação. A melhoria varia com cada modelo de unidade e capacidade.

DULBE não é suportado nos arrays de storage EF300C ou EF600C neste momento.

O que preciso saber sobre o recurso de volumes provisionados por recurso?

O Resource Provisioning é um recurso disponível nos sistemas de storage EF300 e EF600, que permite que os volumes sejam colocados em uso imediatamente, sem processo de inicialização em segundo plano.

Um volume com recursos provisionados é um volume espesso em um grupo de volume SSD ou pool, onde a capacidade do disco é alocada (atribuída ao volume) quando o volume é criado, mas os blocos do disco são desalocados (desmapeados). Em comparação, em um volume espesso tradicional, todos os blocos do disco são mapeados ou alocados durante uma operação de inicialização do volume em segundo plano para 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 com recursos provisionados, não há inicialização em segundo plano com limite de tempo. Em vez disso, cada faixa RAID é inicializada na primeira gravação em um bloco de volume na faixa.

Volumes provisionados por recurso são suportados apenas em grupos de volumes SSD e pools, onde todas as unidades no grupo ou pool suportam a capacidade de recuperação de erros NVMe Deallocated or Unwritten Logical Block Error Enable (DULBE). Quando um volume provisionado por recurso é criado, todos os blocos de unidade atribuídos ao volume são desalocados (desmapeados). Além disso, hosts podem desalocar blocos lógicos no volume usando o comando NVMe Dataset Management ou o comando SCSI Unmap. Desalocar blocos pode melhorar a vida útil do SSD e aumentar o desempenho máximo de gravação. A melhoria varia com cada modelo de unidade e capacidade.

O provisionamento de recursos está ativado por padrão em sistemas onde as unidades suportam DULBE. Você pode desativar essa configuração padrão em **Pools & Grupos de Volume**.

DULBE não é suportado nos arrays de storage EF300C ou EF600C neste momento.

Volumes e cargas de trabalho

Saiba mais sobre volumes e cargas de trabalho no SANtricity System Manager

Você pode criar um volume como um contêiner 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 array de storage para um aplicativo específico.

O que são volumes e cargas de trabalho?

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 único componente lógico para o host. Depois que um volume é definido, você pode adicioná-lo a uma carga de trabalho. Uma carga de trabalho 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 funcionam os volumes"
- "Como funcionam as cargas de trabalho"
- "Terminologia de volume"
- "Como a capacidade é alocada para volumes"
- "Ações que você pode executar em volumes"

Como você cria volumes e cargas de trabalho?

Primeiro, você cria uma carga de trabalho. Vá para o **Storage › Volumes** e abra um assistente que o guiará pelas etapas. Em seguida, você cria um volume a partir da capacidade disponível em um pool ou em um grupo de volume e, em seguida, atribui a carga de trabalho que você criou.

Saiba mais:

- "Fluxo de trabalho para criação de volumes"
- "Criar workloads"
- "Criar volumes"
- "Adicionar volumes à carga de trabalho"

Informações relacionadas

Saiba mais sobre conceitos relacionados a volumes:

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

Conceitos

Como funcionam os volumes no SANtricity software

Os volumes são contêineres de dados que gerenciam e organizam o espaço de storage no seu array de storage.

Você cria volumes a partir da capacidade de storage disponível em seu array de storage e facilita a organização e o uso dos recursos do seu sistema. Esse 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 unidades lógicas (LUNs), que são visíveis para os hosts. Os LUNs armazenam os dados de usuário que são acessíveis usando um ou mais dos protocolos de acesso do host suportados pelo array de storage, incluindo FC, iSCSI e SAS.

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

Os volumes obtêm sua capacidade de pools ou grupos de volume. Você pode criar os seguintes tipos de

volumes a partir dos pools ou grupos de volume existentes em seu array de storage.

- **A partir de pools** — Você pode criar volumes a partir de um pool como *volumes totalmente provisionados (thick)* ou *volumes com thin provisioning (thin).*

  > A interface do System Manager não oferece uma opção para criar volumes thin. Se você deseja criar volumes thin, use a Command Line Interface (CLI).

- **A partir de grupos de volume** — Você pode criar volumes a partir de um grupo de volume somente como *volumes totalmente provisionados (espessos)*.

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

- A capacidade para um volume thick 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 custos iniciais de storage para as empresas. No entanto, o full provisioning tem a vantagem de menor latência, pois todo o storage é alocado de uma só vez quando thick volumes são criados.

> Os sistemas de storage EF600/EF600C e EF300/EF300C não suportam thin provisioning.

Características dos volumes

Cada volume em um pool ou grupo de volume pode ter suas próprias características individuais com base no tipo de dados que serão armazenados nele. Algumas dessas características incluem:

- **Tamanho do segmento** — Um segmento é a quantidade de dados em kilobytes (KiB) armazenada em uma unidade antes que o array de storage passe para a próxima unidade na faixa (grupo RAID). O tamanho do segmento é igual ou menor que a 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 livre disponível em um pool ou grupo de volume. Antes de criar um volume, o pool ou grupo de volume já deve existir e deve ter capacidade livre suficiente para criar o volume.
- **Propriedade do controlador** — Todos os arrays de storage podem ter um ou dois controladores. Em um array com um único controlador, a carga de trabalho de um volume é gerenciada por um único controlador. Em um array com controladora dupla, um volume terá um controlador preferencial (A ou B) que "possui" o volume. Em uma configuração com controladora dupla, a propriedade do volume é ajustada automaticamente usando o recurso de Automatic Load Balancing para corrigir quaisquer problemas de balanceamento de carga quando as cargas de trabalho são transferidas entre os controladores. O Automatic Load Balancing fornece balanceamento automático da carga de E/S e garante que o tráfego de E/S de entrada dos hosts seja gerenciado e balanceado dinamicamente entre os dois controladores.
- **Atribuição de volume** — Você pode conceder acesso a um volume a hosts, seja no momento da criação do volume ou posteriormente. Todo o acesso dos hosts é gerenciado por meio de um número de unidade lógica (LUN). Os hosts detectam os LUNs que, por sua vez, são atribuídos aos volumes. Se você estiver atribuindo um volume a vários hosts, use clustering para garantir que o volume esteja disponível para todos os hosts.

  O tipo de host pode ter limites específicos quanto ao número de volumes que o host pode acessar. Leve essa limitação em consideração ao criar volumes para uso por um host específico.

- **Nome descritivo** — Você pode nomear um volume como quiser, mas recomendamos que o nome seja

descritivo.

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

Como funcionam as cargas de trabalho no SANtricity software

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

Uma carga de trabalho é um objeto de storage que suporta uma aplicação. Você pode definir uma ou mais cargas de trabalho, ou instâncias, por aplicação. Para algumas aplicações, o sistema configura a carga de trabalho para conter volumes com características subjacentes semelhantes. Essas características de volume são otimizadas com base no tipo de aplicação que a carga de trabalho suporta. Por exemplo, se você criar uma carga de trabalho que suporte uma aplicação Microsoft SQL Server e, posteriormente, criar volumes para essa carga de trabalho, as características subjacentes do volume serão otimizadas para suportar Microsoft SQL Server.

Durante a criação de volumes, o sistema solicita que você responda a perguntas sobre o uso da carga de trabalho. Por exemplo, se você estiver criando volumes para Microsoft Exchange, você será perguntado quantas caixas de correio precisa, quais são os requisitos médios de capacidade de cada 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 ignorar esta etapa na sequência de criação de volumes.

Tipos de cargas de trabalho

Você pode criar dois tipos de cargas de trabalho: application-specific e outras.

- **Específico da aplicação**. Ao criar volumes usando uma carga de trabalho específica da aplicação, o sistema pode recomendar uma configuração de volume otimizada para minimizar a disputa entre a E/S da carga de trabalho da aplicação e outros tráfegos da sua instância da aplicação. Características do volume, como tipo de E/S, tamanho do segmento, propriedade do controlador e cache de leitura e gravação, são automaticamente recomendadas e otimizadas para cargas de trabalho criadas para os seguintes tipos de aplicação.
  - Microsoft® SQL Server™
  - Microsoft® Exchange Server™
  - Aplicações de video surveillance
  - VMware ESXi™ (para volumes a serem usados com Virtual Machine File System)

    Você pode revisar a configuração de volume recomendada e editar, adicionar ou excluir os volumes e características recomendados pelo sistema usando a caixa de diálogo Add/Edit Volumes.
- **Outros** (ou aplicações sem suporte específico para criação de volumes). Outras cargas de trabalho utilizam uma configuração de volume que você deve especificar manualmente quando quiser criar uma carga de trabalho que não está associada a uma aplicação específica ou se o sistema não tiver otimização incorporada para a aplicação que você pretende usar no array de storage. Você deve especificar manualmente a configuração de volume usando a caixa de diálogo Adicionar/Editar Volumes.

Visualizações de aplicativos e cargas de trabalho

Para visualizar aplicativos e cargas de trabalho, inicie SANtricity System Manager. Nessa interface, você pode visualizar informações associadas a uma carga de trabalho específica de um aplicativo de algumas maneiras diferentes:

- Você pode selecionar a guia **Aplicações e Cargas de Trabalho** no bloco Volumes para visualizar os volumes do array de storage agrupados por carga de trabalho e pelo tipo de aplicação ao qual a carga de trabalho está associada.
- Você pode selecionar a guia **Applications & Workloads** no bloco Desempenho para visualizar métricas de desempenho (latência, IOPS e MBs) para objetos lógicos. Os objetos são agrupados por aplicação e carga de trabalho associada. Ao coletar esses dados de desempenho em intervalos regulares, você pode estabelecer medições de referência e analisar tendências, o que pode ajudar enquanto você investiga problemas relacionados ao desempenho de I/O.

Aprenda sobre a terminologia de volume no software SANtricity

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

Todos os tipos de volume

Termo	Descrição
Capacidade alocada	Você utiliza a capacidade alocada para criar volumes e para operações de copy services. A capacidade alocada e a capacidade reportada são as mesmas para volumes espessos, mas são diferentes para volumes finos. Para um volume espesso, o espaço fisicamente alocado é igual ao espaço que é reportado ao host. Para um volume fino, a capacidade reportada é a capacidade que é reportada aos hosts, enquanto a capacidade alocada é a quantidade de espaço em disco que está atualmente alocada para gravação de dados.
Aplicativo	Um aplicativo é um software como SQL Server ou Exchange. Você define uma ou mais cargas de trabalho para suportar cada aplicativo. Para alguns aplicativos, o sistema recomenda automaticamente uma configuração de volume que otimiza o storage. Características 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 qual controlador é designado como proprietário, ou controlador primário, do volume. Um volume pode ter um controlador preferencial (A ou B) que "possui" o volume. A propriedade do volume é ajustada automaticamente usando o recurso de Balanceamento Automático de Carga para corrigir quaisquer problemas de balanceamento de carga quando as cargas de trabalho são distribuídas entre os controladores. O Balanceamento Automático de Carga fornece balanceamento automático de carga de E/S e garante que o tráfego de E/S proveniente dos hosts seja gerenciado e balanceado dinamicamente entre ambos os controladores.

Termo	Descrição
Pré-busca de leitura de cache dinâmico	O pré-carregamento dinâmico de leitura em cache permite que o controlador copie blocos de dados sequenciais adicionais para o cache enquanto lê blocos de dados de uma unidade para o cache. Esse armazenamento em cache aumenta a chance de que solicitações futuras de dados possam ser atendidas pelo cache. O pré-carregamento dinâmico de leitura em cache é importante para aplicativos multimídia que usam E/S sequencial. A taxa e a quantidade de dados pré-carregados no cache se ajustam automaticamente com base na taxa e no tamanho das solicitações de leitura do host. O acesso aleatório não faz com que dados sejam pré-carregados no cache. Esse recurso não se aplica quando o armazenamento em cache está desativado. Para um volume fino, a pré-busca de leitura em cache dinâmica está sempre desativada e não pode ser alterada.
Área de capacidade livre	Uma área de capacidade livre é a capacidade livre que pode resultar da exclusão de um volume ou do não uso de toda a capacidade livre disponível durante a criação do volume. Ao criar um volume em um grupo de volume que possui uma ou mais áreas de capacidade livre, a capacidade do volume é limitada à maior área de capacidade livre nesse grupo de volume. Por exemplo, se um grupo de volume tiver um total de 15 GiB de capacidade livre e a maior área de capacidade livre for 10 GiB, o maior volume que você pode criar é 10 GiB. Ao consolidar a capacidade livre, 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 I/O para um volume em um array de storage.
Cluster de hosts	Um cluster de hosts é um grupo de hosts. Você cria um cluster de hosts para facilitar a atribuição dos mesmos volumes a vários hosts.
Drive hot spare	Hot spare são suportados apenas com grupos de volume. Uma unidade hot spare não contém dados e atua como reserva caso uma unidade falhe em volumes RAID 1, RAID 3, RAID 5 ou RAID 6 contidos em um grupo de volume. A unidade hot spare adiciona mais um nível de redundância ao seu array de storage.
LUN	Um número de unidade lógica (LUN, na sigla em inglês) é o número atribuído ao espaço de endereçamento que um host usa para acessar um volume. O volume é apresentado ao host como capacidade na forma de um LUN. Cada host possui seu próprio espaço de endereçamento LUN. Portanto, o mesmo LUN pode ser usado por diferentes hosts para acessar volumes diferentes.
Verificação de mídia	Uma verificação de mídia permite detectar erros na mídia da unidade antes que sejam encontrados durante uma leitura ou gravação normal nas unidades. Uma verificação de mídia é executada como uma operação em segundo plano e examina todos os dados e informações de redundância em volumes de usuário definidos.

Termo	Descrição
Espaço de nomes	Um namespace é um storage NVM formatado para acesso em bloco. É análogo a uma unidade lógica em SCSI, que se relaciona a um volume no array de storage.
Pool	Um pool é um conjunto de unidades agrupadas 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 volume.)
Capacidade do pool ou grupo de volume	A capacidade de um pool, volume ou grupo de volume é a capacidade em um array de storage que foi atribuída a um pool ou grupo de volume. Essa capacidade é usada para criar volumes e atender às diversas necessidades de capacidade das operações de serviços de cópia e objetos de armazenamento.
Cache de leitura	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 serem liberados.
Capacidade relatada	A capacidade reportada é a capacidade que é informada ao host e pode ser acessada pelo host. A capacidade reportada e a capacidade alocada são as mesmas para volumes espessos, mas são diferentes para volumes finos. Para um volume espesso, o espaço fisicamente alocado é igual ao espaço reportado ao host. Para um volume fino, a capacidade reportada é a capacidade que é reportada aos hosts, enquanto a capacidade alocada é a quantidade de espaço em disco que está atualmente alocada para gravação de dados.
Tamanho do segmento	Um segmento é a quantidade de dados em kilobytes (KiB) armazenada em uma unidade antes que o array de storage passe para a próxima unidade na faixa (grupo RAID). O tamanho do segmento é igual ou menor que a capacidade do grupo de volume. O tamanho do segmento é fixo e não pode ser alterado para pools.
Distribuição	O striping é uma forma de armazenar dados no array de storage. O striping divide o fluxo de dados em blocos de um determinado tamanho (chamado de "tamanho do bloco") e, em seguida, grava esses blocos nas unidades uma a uma. Essa forma de armazenamento de dados é usada para distribuir e armazenar dados em várias unidades físicas. O striping é sinônimo de RAID 0 e distribui 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 array de storage.
Atribuição de volume	A atribuição de volume é como os LUNs do host são atribuídos a um volume.

Termo	Descrição
Nome do volume	O nome de um volume é uma sequência de caracteres atribuída ao volume no momento de sua criação. Você pode aceitar o nome padrão ou fornecer um nome mais descritivo que indique o tipo de dados armazenados no volume.
Grupo de volume	Um grupo de volume é um contêiner para volumes com características compartilhadas. Um grupo de volume tem uma capacidade definida e nível RAID. Você pode usar um grupo de volume para criar um ou mais volumes acessíveis a um host. (Você cria volumes a partir de um grupo de volume ou de um pool.)
Carga de trabalho	Uma carga de trabalho é um objeto de storage que suporta uma aplicação. Você pode definir uma ou mais cargas de trabalho, ou instâncias, por aplicação. Para algumas aplicações, o sistema configura a carga de trabalho para conter volumes com características subjacentes semelhantes. Essas características de volume são otimizadas com base no tipo de aplicação que a carga de trabalho suporta. Por exemplo, se você criar uma carga de trabalho que suporte uma aplicação Microsoft SQL Server e, posteriormente, criar volumes para essa carga de trabalho, as características subjacentes do volume serão otimizadas para suportar Microsoft SQL Server.
Cache de gravação	O cache de gravação é um buffer que armazena dados do host que ainda não foram gravados nos discos. Os dados permanecem no cache de gravação até serem gravados nos discos. O armazenamento em cache pode aumentar o desempenho 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 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 está disponível somente se o armazenamento em cache de gravação estiver habilitado e houver dois controladores. O armazenamento em cache com espelhamento é a configuração padrão na criação do volume.
Armazenamento em cache sem baterias	A configuração de armazenamento em cache de gravação sem baterias permite que o armazenamento em cache continue mesmo quando as baterias estão ausentes, com defeito, completamente descarregadas ou não totalmente carregadas. Escolher armazenamento em cache de gravação sem baterias geralmente não é recomendado, pois os dados podem ser perdidos se houver uma queda de energia. Normalmente, o armazenamento em cache é desativado temporariamente pelo controlador até que as baterias sejam carregadas ou uma bateria com defeito seja substituída.

Específico para volumes finos

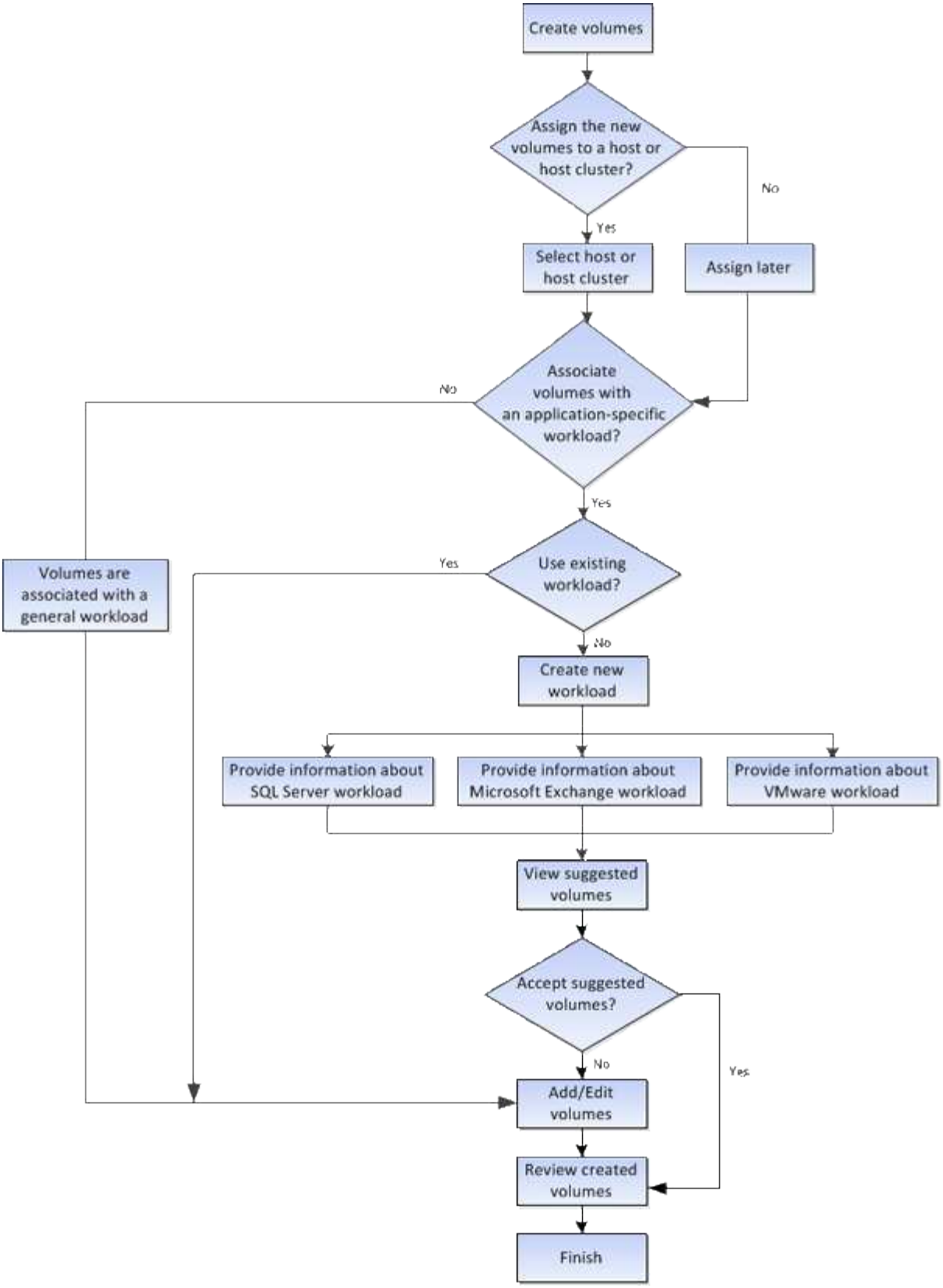
System Manager não oferece uma opção para criar volumes finos. Se você deseja criar volumes finos, use a interface de linha de comando (CLI).

Volumes finos não estão disponíveis nos sistemas de storage EF600/EF600C ou EF300/EF300C.

Termo	Descrição
Limite de capacidade alocada	O limite de capacidade alocada é o teto de quanto a capacidade física alocada para um volume fino pode crescer.
Capacidade escrita	A capacidade de escrita é a quantidade de capacidade que foi escrita da capacidade reservada alocada para volumes finos.
Limiar de alerta	Você pode definir um limite de alerta para ser emitido quando a capacidade alocada para um volume fino atingir a porcentagem de preenchimento (o limite de alerta).

Como funciona a criação de volumes no SANtricity System Manager

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



Aprenda sobre integridade de dados e segurança de dados para volumes no software SANtricity

Você pode habilitar volumes para usar o recurso Data Assurance (DA) e o recurso Drive Security. Esses recursos são apresentados no nível do pool e do grupo de volumes.

Garantia de dados

O Data Assurance (DA) implementa o padrão T10 Protection Information (PI), que aumenta a integridade de dados ao verificar e corrigir erros que possam ocorrer durante a transferência de dados ao longo do caminho de E/S. O uso típico do recurso Data Assurance verifica a porção do caminho de E/S entre os controladores e as unidades. Os recursos do DA são apresentados nos níveis de pool e grupo de volume.

Quando esse recurso está habilitado, o array de storage anexa códigos de verificação de erros (também conhecidos como verificações de redundância cíclica ou CRCs) a cada bloco de dados no volume. Após a movimentação de um bloco de dados, o array de storage usa esses códigos CRC para determinar se ocorreram erros durante a transmissão. Dados potencialmente corrompidos não são gravados em disco nem retornados ao host. Se você deseja usar o recurso DA, selecione um pool ou grupo de volume compatível com DA ao criar um novo volume (procure por "Sim" ao lado de "DA" na tabela de candidatos de pool e grupo de volumes).

Segurança da unidade

A Segurança de Unidade é um recurso que impede o acesso não autorizado a dados em unidades com segurança habilitada quando removidas do array de storage. Essas unidades podem ser unidades com Full Disk Encryption (FDE) ou unidades certificadas para atender ao Federal Information Processing Standards 140-2 nível 2 (unidades FIPS).

Como o Drive Security funciona no nível da unidade

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

Como o Drive Security funciona no nível de volume

Ao criar um pool ou grupo de volume a partir de drives secure-capable, você também pode habilitar Drive Security para esses pools ou grupos de volume. A opção Drive Security torna os drives e os grupos de volume e pools associados secure-enabled. Um pool ou grupo de volume pode conter tanto drives secure-capable quanto drives não secure-capable, mas todos os drives devem ser secure-capable para usar seus recursos de criptografia.

Como implementar Drive Security

Para implementar a Segurança do Drive, execute as seguintes etapas.

1. Equipe seu array de storage com unidades compatíveis com segurança, sejam elas FDE drives ou FIPS drives. (Para volumes que exigem suporte a FIPS, use somente FIPS drives. Misturar FIPS drives e FDE drives em um grupo de volume ou pool fará com que todas as unidades sejam tratadas como FDE drives. Além disso, um FDE drive não pode ser adicionado ou usado como reserva em um grupo de volume ou pool composto apenas por FIPS drives.)
2. Crie uma chave de segurança, que é uma sequência de caracteres compartilhada pelo controlador e pelas unidades para acesso de leitura/gravação. Você pode criar uma chave interna a partir da memória persistente do controlador ou uma chave externa a partir 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 de unidade para pools e grupos de volume:
    - Crie um pool ou grupo de volume (procure por **Sim** na coluna **Secure-capable** na tabela Candidates).

◦ Selecione um pool ou grupo de volume ao criar um novo volume (procure por **Sim** ao lado de **Compatível com segurança** na tabela de candidatos a pool e grupo de volume).

Com o recurso Drive Security, você cria uma chave de segurança que é compartilhada entre as unidades habilitadas para segurança e os controladores em um array de storage. Sempre que a energia das unidades for desligada e ligada, as unidades habilitadas para segurança mudam para o estado Security Locked até que o controlador aplique a chave de segurança.

Saiba mais sobre cache SSD e volumes no software SANtricity

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

Volumes

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

O cache SSD é um cache secundário usado em conjunto com o cache primário na memória dinâmica de acesso aleatório (DRAM) do controlador.

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

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

Qualquer volume atribuído ao uso do SSD Cache de um controlador não é elegível para transferência automática de load balance.

Recurso de segurança da unidade

Para usar o Cache SSD em um volume que também utiliza Drive Security (está com a segurança ativada), os recursos de Drive Security do volume e do Cache SSD devem corresponder. Se eles não corresponderem, o volume não terá a segurança ativada.

Ações que você pode executar em volumes no SANtricity System Manager

Você pode executar diversas ações diferentes em um volume: aumentar a capacidade, excluir, copiar, inicializar, redistribuir, alterar a propriedade, alterar as configurações de armazenamento em cache e alterar as configurações de verificação de mídia.

Aumentar capacidade

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

- Utilize a capacidade livre que está disponível no pool ou grupo de volume.

Você adiciona capacidade a um volume selecionando **Storage › Pools and Volume Groups › Add Capacity**.

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

  Você adiciona capacidade não atribuída ao pool ou grupo de volume selecionando **Storage › Pools and Volume Groups › Add Capacity**.

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

Após expandir a capacidade do volume, você deve aumentar manualmente o tamanho do sistema de arquivos para que corresponda. Como fazer isso depende do sistema de arquivos que você está usando. Consulte a documentação do seu sistema operacional para obter detalhes.

Excluir

Normalmente, você exclui volumes se eles foram criados com parâmetros ou capacidade incorretos, não atendem mais às necessidades de configuração de storage ou são imagens de 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 volume.

A exclusão de volumes causa a perda de todos os dados nesses volumes. A exclusão de um volume também excluirá quaisquer imagens de snapshot, agendamentos e volumes de snapshot associados e removerá quaisquer relações de espelhamento.

Copiar

Ao copiar volumes, você cria uma cópia pontual de dois volumes separados, o volume de origem e o volume de destino, no mesmo array de storage. Você pode copiar volumes selecionando **Storage › Volumes › Copy Services › Copy volume**.

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 um volume manualmente para se recuperar de determinadas condições de falha. Ao inicializar um volume, o volume mantém seu WWN, atribuições de host, capacidade alocada e configurações de capacidade reservada. Ele também mantém as mesmas configurações de Data Assurance (DA) e configurações de segurança.

Você pode inicializar volumes selecionando **Storage › Volumes › More › Initialize volumes**.

Redistribuir

Você redistribui volumes para movê-los de volta aos seus controladores proprietários preferenciais. Normalmente, os drivers de multipath movem volumes de seus controladores proprietários preferenciais quando ocorre um problema no caminho de dados entre o host e o array de storage.

A maioria dos drivers de multipath do host tenta acessar cada volume em um caminho até o controlador proprietário preferencial. No entanto, se esse caminho preferencial ficar indisponível, o driver de multipath no host alterna 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 controlador proprietário preferencial, mas, em alguns casos, pode ser necessário redistribuir os volumes manualmente.

Você pode redistribuir volumes selecionando **Storage › Volumes › More › Redistribute volumes**.

Alterar propriedade do volume

Alterar a propriedade de um volume altera a propriedade de controlador preferencial do volume. O proprietário de controlador preferencial de um volume é listado em **Storage › Volumes › View/Edit Settings › Advanced tab**.

Você pode alterar a propriedade de um volume selecionando **Storage › Volumes › More › Change ownership**.

Espelhamento e propriedade de volume

Se o volume primário do par espelhado pertencer ao controlador A, então o volume secundário também será de propriedade do controlador A do array de storage remoto. Alterar o proprietário do volume primário alterará automaticamente o proprietário do volume secundário para garantir que ambos os volumes pertençam ao mesmo controlador. As alterações de propriedade atuais no lado primário se propagam automaticamente para as alterações de propriedade atuais correspondentes no lado secundário.

Se um grupo de consistência de espelhamento contiver um volume secundário local e a propriedade do controlador for alterada, o volume secundário será automaticamente transferido de volta para o proprietário original do controlador na primeira operação de gravação. Você não pode alterar a propriedade do controlador de um volume secundário usando a opção **Change ownership**.

Cópia de volume e propriedade do volume

Durante uma operação de cópia de volume, o mesmo controlador deve ser o proprietário tanto do volume de origem quanto do volume de destino. Às vezes, ambos os volumes não possuem o mesmo controlador preferencial quando a operação de cópia de volume é iniciada. Portanto, a propriedade do volume de destino é automaticamente transferida para o controlador preferencial do volume de origem. Quando a cópia de volume é concluída ou interrompida, a propriedade do volume de destino é restaurada ao seu controlador preferencial.

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

Alterar configurações de cache

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

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

Selecione o **Storage › Volumes › More › Change cache settings** para alterar as seguintes configurações de cache:

- **Armazenamento em 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 serem liberados.

  O cache de gravação é um buffer que armazena dados do host que ainda não foram gravados nos discos. Os dados permanecem no cache de gravação até serem gravados nos discos. O armazenamento em cache pode aumentar o desempenho de E/S.

- **Armazenamento em cache com espelhamento** — armazenamento em cache com espelhamento ocorre quando os dados gravados na memória cache de um controlador também são gravados na memória 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 está disponível somente se o armazenamento em cache de gravação estiver habilitado e houver dois controladores. O armazenamento em cache com espelhamento é a configuração padrão na criação do volume.
- **Armazenamento em cache de gravação sem baterias** — A configuração de armazenamento em cache de gravação sem baterias permite que o armazenamento em cache continue mesmo quando as baterias estão ausentes, com defeito, completamente descarregadas ou não totalmente carregadas. Escolher armazenamento em cache de gravação sem baterias geralmente não é recomendado, pois os dados podem ser perdidos se houver uma queda de energia. Normalmente, o armazenamento em cache de gravação é desativado temporariamente pelo controlador até que as baterias sejam carregadas ou uma bateria com defeito seja substituída.

  Essa configuração só está disponível se você tiver habilitado o armazenamento em cache de gravação. Essa configuração não está disponível para volumes finos.

- **Pré-busca dinâmica de leitura em cache** — A pré-busca dinâmica de leitura em cache permite que o controlador copie blocos de dados sequenciais adicionais para o cache enquanto lê blocos de dados de uma unidade para o cache. Esse armazenamento em cache aumenta a chance de que solicitações futuras de dados possam ser atendidas pelo cache. A pré-busca dinâmica de leitura em cache é importante para aplicativos multimídia que usam E/S sequencial. A taxa e a quantidade de dados pré-buscados para o cache se ajustam automaticamente com base na taxa e no tamanho da solicitação de leitura do host. O acesso aleatório não faz com que dados sejam pré-buscados para o cache. Esse recurso não se aplica quando o armazenamento em cache está desativado.

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

Alterar configurações de varredura de mídia

A verificação de mídia detecta e corrige erros em blocos de disco que são lidos com pouca frequência pelos aplicativos. Essa verificação pode evitar perda de dados caso outras unidades no pool ou grupo de volume falhem, pois os dados das unidades com falha são reconstruídos usando informações de redundância e dados de outras unidades no pool ou grupo de volume.

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

Você pode ativar e definir a duração da verificação de mídia selecionando **Storage › Volumes › More ›**

Change media scan settings.

Um volume é verificado somente quando a opção de verificação de mídia está habilitada para o array de storage e para esse volume. Se a verificação de redundância também estiver habilitada para esse volume, as informações de redundância no volume serão verificadas quanto à consistência com os dados, desde que o volume possua redundância. A verificação de mídia com verificação de redundância é habilitada por padrão para cada volume quando ele é criado.

Se um erro de mídia irrecuperável for encontrado durante a verificação, os dados serão reparados usando informações de redundância, se disponíveis. Por exemplo, informações de redundância estão disponíveis em volumes RAID 5 otimizados ou em volumes RAID 6 que estão otimizados ou têm apenas 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 setores ilegíveis. Tanto erros de mídia corrigíveis quanto irrecuperáveis são relatados ao log de eventos.

Se a verificação de redundância encontrar uma inconsistência entre os dados e as informações de redundância, isso será relatado no registro de eventos.

Como a capacidade é alocada para volumes no SANtricity System Manager

Os discos do seu array de storage fornecem a capacidade de storage físico para seus dados. Antes de começar a armazenar dados, você deve configurar a capacidade alocada em componentes lógicos conhecidos como pools ou grupo de volume. Você usa esses objetos de storage para configurar, armazenar, manter e preservar dados no seu array de storage.

Usando a capacidade para criar e expandir volumes

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

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

Após expandir a capacidade do volume, você deve aumentar manualmente o tamanho do sistema de arquivos para que corresponda. Como fazer isso depende do sistema de arquivos que você está usando. Consulte a documentação do seu sistema operacional para obter detalhes.

Tipos de capacidade para volumes espessos e volumes finos

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

- Para um volume espesso, a capacidade reportada do volume é igual à quantidade de storage físico alocada. Toda a capacidade de storage físico deve estar presente. O espaço fisicamente alocado é igual ao espaço reportado ao host.

  Normalmente, você define a capacidade reportada do volume espesso como a capacidade máxima que você prevê que o volume atingirá. Os volumes espessos oferecem alto desempenho e previsibilidade para seus aplicativos, principalmente porque toda a capacidade do usuário é reservada e alocada no momento da criação.

- Para um volume fino, a capacidade relatada é a capacidade que é informada aos hosts, enquanto a capacidade alocada é a quantidade de espaço em disco que está atualmente alocada para gravação de dados.

  A capacidade reportada pode ser maior do que a capacidade alocada no array de storage. Volumes thin podem ser dimensionados para acomodar o crescimento sem levar em consideração os recursos atualmente disponíveis.

> SANtricity System Manager não oferece uma opção para criar volumes thin. Se você deseja criar volumes thin, use o Command Line Interface (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 drives no pool ou grupo de volume.

Ao aumentar a capacidade declarada para um volume espesso, tenha em mente as seguintes diretrizes:

- Você pode especificar até três casas decimais (por exemplo, 65.375 GiB).
- A capacidade deve ser menor (ou igual) à máxima disponível no grupo de volume.

  Ao criar um volume, uma capacidade adicional é pré-alocada para a migração de Dynamic Segment Size (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 (a capacidade máxima relatada é determinada pelo sistema operacional). Na verdade, alguns sistemas operacionais suportam volumes de até 128 TiB. Consulte a documentação do seu sistema operacional para obter mais detalhes.

Limites de capacidade para volumes finos

É possível criar volumes thin com uma grande capacidade reportada e uma capacidade alocada relativamente pequena, o que é benéfico para a utilização do storage e eficiência. Os volumes thin podem ajudar a simplificar a administração do storage, pois a capacidade alocada pode aumentar conforme as necessidades do aplicativo mudam, sem interromper o aplicativo, permitindo uma melhor utilização do storage.

Além da capacidade reportada e da capacidade alocada, os volumes thin também contêm capacidade escrita. A capacidade escrita é a quantidade de capacidade que foi escrita a partir da capacidade reservada alocada para volumes thin.

A tabela a seguir lista os limites de capacidade para um volume fino.

Tipo de capacidade	Tamanho mínimo	Tamanho máximo
Denunciado	32 MiB	256 TiB
Alocado	4 MiB	64 TiB

Para um volume fino, se a capacidade máxima relatada de 256 TiB for atingida, você não poderá aumentar sua capacidade. Certifique-se de que a capacidade reservada do volume fino esteja definida para um tamanho maior que a capacidade máxima relatada.

O sistema expande automaticamente a capacidade alocada com base no limite de capacidade alocada. O limite de capacidade alocada permite limitar o crescimento automático do thin volume a um valor inferior à 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 menu:Storage [Volumes > guia Thin Volume Monitoring > Change Limit].

Como System Manager não aloca a capacidade total ao criar um volume fino, pode haver capacidade livre insuficiente no pool. A falta de espaço 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 realizar operações de leitura no pool. Se essa situação ocorrer, você receberá um aviso de limite de alerta.

Saiba mais sobre o monitoramento de volumes thin no software SANtricity

Você pode monitorar volumes thin para espaço e gerar alertas apropriados para evitar condições de falta de capacidade.

Ambientes com provisionamento dinâmico podem alocar mais espaço lógico do que possuem de storage físico. Você pode selecionar **Storage › Volumes › Thin Volume Monitoring** para monitorar quanto crescimento seus volumes dinâmicos têm antes de atingirem o limite máximo de capacidade alocada.

Você pode usar a visualização de Thin Monitoring para executar as seguintes ações:

- Defina o limite que restringe a capacidade alocada à qual um volume fino pode expandir automaticamente.
- Defina a porcentagem a partir da qual um alerta (limite de aviso excedido) é enviado para a área de Notificações na página inicial quando um volume thin estiver próximo do limite máximo de capacidade alocada.

Para aumentar a capacidade de um volume fino, aumente sua capacidade declarada.

System Manager não oferece uma opção para criar thin volumes. Se você deseja criar thin volumes, use a command line interface (CLI).

Volumes finos não estão disponíveis nos sistemas de storage EF600/EF600C ou EF300/EF300C.

Aprenda sobre volumes espessos e finos no software SANtricity

Um volume espesso é sempre totalmente provisionado, o que significa que toda a capacidade é alocada quando o volume é criado. Um volume fino é sempre com thin provisioning, o que significa que a capacidade é alocada à medida que os dados são gravados no volume.

System Manager não oferece uma opção para criar thin volumes. Se você deseja criar thin volumes, use a command line interface (CLI).

Tipo de volume	Descrição
Volumes espessos	• Volumes thick são criados a partir de um pool ou grupo de volume. • Com volumes espessos, uma grande quantidade de espaço de storage é fornecida antecipadamente em antecipação às necessidades futuras de storage. • Volumes espessos são criados com todo o tamanho do volume pré-alocado no storage físico no momento em que o volume é criado. Essa pré-alocação significa que criar um volume de 100 GiB realmente consome 100 GiB de capacidade alocada em seus discos. No entanto, o espaço pode permanecer não utilizado, causando subutilização da capacidade de storage. • Ao criar volumes espessos, certifique-se de não alocar capacidade em excesso para um único volume. Alocar capacidade em excesso para um único volume pode consumir rapidamente todo o storage físico do seu sistema. • Lembre-se de que capacidade de storage também é necessária para serviços de cópia (imagens de Snapshot, volumes de Snapshot, cópias de volume e espelhamento assíncrono), portanto, não aloque toda a capacidade para volumes thick. Espaço insuficiente pode bloquear gravações no pool ou grupo de volume. Você recebe um aviso de limite de capacidade livre se essa situação ocorrer.
Volumes com thin provisioning	• Volumes com thin provisioning são criados apenas a partir de um pool, não de um grupo de volume. • Os volumes thin devem ser RAID 6. • Volumes finos não estão disponíveis nos sistemas de storage EF600/EF600C ou EF300/EF300C. • Você deve usar a CLI para criar volumes com thin provisioning. • 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. • Um volume com thin provisioning permite que você superaloque seu tamanho. Ou seja, você pode atribuir um tamanho de LUN maior do que o tamanho do volume. Você pode então expandir o volume conforme necessário (se necessário, adicionando unidades no processo) sem expandir o tamanho do LUN e, portanto, sem desconectar os usuários. • Você pode usar thin provisioning exigência de espaço (UNMAP) para recuperar blocos de um volume com thin provisioning no array de storage por meio de um comando SCSI UNMAP emitido pelo host. Um array de storage que suporta thin provisioning pode reaproveitar o espaço recuperado para atender solicitações de alocação de outro volume com thin provisioning dentro do mesmo array de storage, o que permite um melhor relatório do consumo de espaço de disco e um uso mais eficiente dos recursos.

Restrições de thin volume

Volumes com thin provisioning suportam todas as operações que volumes espessos suportam, com as seguintes exceções:

- Não é possível alterar o tamanho do segmento de um volume com thin provisioning.
- Não é possível ativar a verificação de redundância de pré-leitura para um volume com thin provisioning.
- Não é possível usar um volume com thin provisioning como volume de destino em uma operação de Copy Volume.
- Você pode alterar o limite de capacidade alocada e o limite de aviso de um volume com thin provisioning apenas no lado primário de um par espelhado assíncrono. Quaisquer alterações nesses parâmetros no lado primário são propagadas automaticamente para o lado secundário.

Configurar storage

Crie cargas de trabalho no SANtricity System Manager

Você pode criar cargas de trabalho para qualquer tipo de aplicação.

Sobre esta tarefa

Uma carga de trabalho é um objeto de storage que dá suporte a um aplicativo. Você pode definir uma ou mais cargas de trabalho, ou instâncias, por aplicativo.

Passos

1. Selecione o menu: storage [Volumes].
2. Selecione o menu: criar [Workload].

   A caixa de diálogo Criar Carga de Trabalho do Aplicativo é exibida.

3. Use a lista suspensa para selecionar o tipo de aplicativo para o qual deseja criar a carga de trabalho e, em seguida, digite um nome de carga de trabalho.
4. Clique em **Create**.

Depois que você terminar

Você está pronto para adicionar capacidade de storage à carga de trabalho que criou. Use a opção **Criar Volume** para criar um ou mais volumes para um aplicativo e alocar quantidades específicas de capacidade para cada volume.

Crie volumes no SANtricity System Manager

Você cria volumes para adicionar capacidade de storage a uma carga de trabalho específica de um aplicativo e para tornar os volumes criados visíveis para um host ou cluster de hosts específico. Além disso, a sequência de criação de volumes oferece opções para alocar quantidades específicas de capacidade a cada volume que você deseja criar.

Sobre esta tarefa

A maioria dos tipos de aplicativos utiliza, por padrão, uma configuração de volume definida pelo usuário. Alguns tipos de aplicativos possuem uma configuração inteligente aplicada durante a criação do volume. Por exemplo, se você estiver criando volumes para o aplicativo 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 você deseja. 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 o host para um volume

Você cria volumes para adicionar capacidade de storage a uma carga de trabalho específica de um aplicativo e para tornar os volumes criados visíveis para um host ou cluster de hosts específico. Além disso, a sequência de criação de volumes oferece opções para alocar quantidades específicas de capacidade a cada volume que você deseja criar.

Antes de começar

- Hosts ou clusters de hosts válidos existem no bloco Hosts.
- Os identificadores de porta do host foram definidos para o host.
- Antes de criar um volume com DA habilitado, a conexão de host que você pretende usar deve ser compatível com DA. Se alguma das conexões de host nos controladores do seu array de storage não for compatível com DA, os hosts associados não poderão acessar dados nos volumes com DA habilitado.

Sobre esta tarefa

Tenha em mente estas diretrizes ao atribuir volumes:

- O sistema operacional de um host pode ter limites específicos quanto ao número de volumes que o host pode acessar. Leve essa limitação em consideração ao criar volumes para uso por um host específico.
- Você pode definir uma atribuição para cada volume no array de storage.
- Os volumes atribuídos são compartilhados entre os controladores no array de storage.
- O mesmo número de unidade lógica (LUN) não pode ser usado duas vezes por um host ou um cluster de hosts para acessar um volume. Você deve usar um LUN exclusivo.
- Se você deseja acelerar o processo de criação de volumes, pode ignorar a etapa de atribuição de 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 hosts que entre em conflito com uma atribuição já estabelecida para um host nos clusters de hosts.

Passos

1. Selecione o menu: storage [Volumes].
2. Selecione o menu: criar [Volume].

   A caixa de diálogo Create Volumes é exibida.

3. Na lista suspensa, selecione um host ou cluster de hosts específico ao qual deseja atribuir volumes ou escolha atribuir o host ou cluster de hosts posteriormente.
4. Para continuar a sequência de criação de volume para o host ou cluster de hosts selecionado, clique em **Avançar** e vá para Etapa 2: selecione uma carga de trabalho para um volume.

   A caixa de diálogo Select Workload é exibida.

Etapa 2: selecione uma carga de trabalho para um volume

Selecione uma carga de trabalho para personalizar a configuração do array de storage 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 pretende usar neste array de storage não estiver listado.

Sobre esta tarefa

Esta tarefa descreve como criar volumes para uma carga de trabalho existente.

- Ao criar volumes usando uma carga de trabalho específica de aplicativo, o sistema pode recomendar uma configuração de volume otimizada para minimizar a disputa entre a E/S da carga de trabalho do aplicativo e outro tráfego da sua instância de aplicativo. Você pode revisar a configuração de volume recomendada e editar, adicionar ou excluir os volumes e características recomendados pelo sistema usando a caixa de diálogo Adicionar/Editar Volumes.
- *Ao criar volumes usando "Other"* aplicativos (ou aplicativos sem suporte específico para criação de volumes), você especifica manualmente a configuração do volume usando a caixa de diálogo Adicionar/Editar Volumes.

Passos

1. Faça uma das seguintes ações:
   - Selecione a opção **Create volumes for an existing workload** 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 opções "Other" se o aplicativo que você pretende usar neste array de storage não estiver listado.

     - Insira um nome para a carga de trabalho que você deseja criar.
2. Clique em **Next**.
3. Se sua carga de trabalho estiver associada a um tipo de aplicativo compatível, insira as informações solicitadas; caso contrário, vá para Etapa 3: adicionar ou editar volumes.

Etapa 3: adicionar ou editar volumes

System Manager pode sugerir uma configuração de volume com base no aplicativo ou carga de trabalho que você selecionou. Essa configuração de volume é otimizada com base no tipo de aplicativo que a carga de trabalho suporta. Você pode aceitar a configuração de volume recomendada ou pode editá-la conforme necessário. Se você selecionou um dos aplicativos "Outros", deverá especificar manualmente os volumes e as características que deseja criar.

Antes de começar

- Os pools ou grupos de volume devem ter capacidade livre suficiente.
- O número máximo de volumes permitidos em um volume group é 256.
- O número máximo de volumes permitidos em um pool depende do modelo do sistema de storage:
  - 2.048 volumes (EF600, EF600C e E5700 series)
  - 1.024 volumes (EF300 and EF300C)
  - 512 volumes (E4000 e E2800 series)
- Para criar um volume com Data Assurance (DA) ativado, a conexão de host que você pretende usar deve ser compatível com DA.

Selecionando um pool ou grupo de volume com recursos de segurança

Se você deseja criar um volume habilitado para DA, selecione um pool ou grupo de volume que seja compatível com DA (procure por **Sim** ao lado de "DA" na tabela de candidatos de pool e grupo de volume).

Os recursos de DA são apresentados no nível do pool e do grupo de volume no System Manager. A proteção de DA verifica e corrige erros que possam ocorrer durante a transferência de dados pelos controladores até as unidades. Selecionar um pool ou grupo de volume com suporte a DA para o novo volume garante que quaisquer erros sejam detectados e corrigidos.

Se alguma das conexões de host nos controladores em seu array de storage não suportar DA, os hosts associados não poderão acessar dados em volumes com DA habilitado.

- Para criar um volume com segurança habilitada, uma chave de segurança deve ser criada para o array de storage.

Selecionando um pool ou grupo de volume com recursos de segurança

Se você deseja criar um volume com segurança habilitada, selecione um pool ou grupo de volume que seja secure capable (procure por **Yes** ao lado de "Secure-capable" na tabela de candidatos de pool e grupo de volume).

Os recursos de segurança das unidades são apresentados no nível do pool e do grupo de volume no System Manager. Unidades com recursos de segurança impedem o acesso não autorizado aos dados em uma unidade que foi fisicamente removida do array de storage. Uma unidade com segurança habilitada criptografa os dados durante as gravações e os descriptografa durante as leituras usando uma chave de criptografia exclusiva.

Um pool ou grupo de volume pode conter tanto unidades com capacidade de segurança quanto unidades sem capacidade de segurança, mas todas as unidades devem ter capacidade de segurança para usar seus recursos de criptografia.

- Para criar um volume com recursos provisionados, todas as unidades devem ser unidades NVMe com a opção Deallocated or Unwritten Logical Block Error (DULBE).

Sobre esta tarefa

Você cria volumes a partir de pools ou grupos de volume. A caixa de diálogo Adicionar/Editar Volumes mostra todos os pools e grupos de volume elegíveis no array de storage. Para cada pool e grupo de volume elegível, o número de unidades disponíveis e a capacidade livre total são exibidos.

Para algumas cargas de trabalho específicas de aplicativos, cada pool ou grupo de volume exibe a capacidade proposta com base na configuração de volume sugerida e mostra a capacidade livre restante em GiB. Para outras cargas de trabalho, a capacidade proposta aparece à medida que você adiciona volumes a um pool ou grupo de volume e especifica a capacidade relatada.

Passos

1. Escolha uma destas ações com base em ter selecionado Outro ou uma carga de trabalho específica da aplicação:
   - **Other** — Clique em **Adicionar novo volume** em cada pool ou grupo de volume 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 do volume. Você pode aceitar o nome padrão ou fornecer um nome mais descritivo, indicando o tipo de dados armazenados no volume.
Capacidade relatada	Defina a capacidade do novo volume e as unidades de capacidade a serem usadas (MiB, GiB ou TiB). Para volumes Thick, a capacidade mínima é 1 MiB e a capacidade máxima é determinada pelo número e capacidade das unidades no pool ou grupo de volume. Lembre-se de que capacidade de storage também é necessária para serviços de cópia (imagens de snapshot, volumes de snapshot, cópias de volume e espelhos remotos); portanto, não aloque toda a capacidade para volumes padrão. 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 seja utilizável, especifique a capacidade em incrementos de 4-GiB ou 8-GiB. Se houver capacidade inutilizável, a única maneira de recuperá-la é aumentar a capacidade do volume.
Tamanho do bloco de volume (EF300 e EF600 only)	Mostra os tamanhos de bloco que podem ser criados para o volume: • 512 — 512 bytes • 4K — 4.096 bytes

Campo	Descrição
Tamanho do segmento	Exibe a configuração de dimensionamento de segmento, que só aparece para volumes em um grupo de volume. Você pode alterar o tamanho do segmento para otimizar o desempenho. **Transições de tamanho de segmento permitidas** — System Manager determina as transições de tamanho de segmento permitidas. Tamanhos de segmento que representam transições inadequadas em relação ao tamanho atual não estão disponíveis na lista suspensa. Transições permitidas geralmente são o dobro ou a 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 é permitido. **Volumes com SSD Cache habilitado** — Você pode especificar um tamanho de segmento de 4 KiB para volumes com SSD Cache habilitado. Certifique-se de selecionar o tamanho de segmento de 4 KiB somente para volumes com SSD Cache habilitado que lidam com operações de E/S de blocos pequenos (por exemplo, tamanhos de bloco de E/S de 16 KiB ou menores). O desempenho pode ser afetado se você selecionar 4 KiB como tamanho de segmento para volumes com SSD Cache habilitado que lidam com operações sequenciais de blocos grandes. **Tempo necessário para alterar o tamanho do segmento** — O tempo necessário para alterar o tamanho do segmento de um volume depende destas variáveis: • A carga de E/S do host • A prioridade de modificação do volume • O número de unidades no grupo de volume • O número de canais de drive • O poder de processamento dos controladores do array de storage Ao alterar o tamanho do segmento de um volume, o desempenho de I/O é afetado, mas seus dados permanecem disponíveis.
Compatível com segurança	**Sim** aparece ao lado de "Secure-capable" somente se as unidades no pool ou grupo de volume forem secure-capable. A Segurança de Unidade impede o acesso não autorizado aos dados em uma unidade que foi fisicamente removida do array de storage. Essa opção está disponível somente quando o recurso Segurança de Unidade estiver ativado e uma chave de segurança estiver configurada para o array de storage. Um pool ou grupo de volume pode conter tanto unidades com capacidade de segurança quanto unidades sem capacidade de segurança, mas todas as unidades devem ter capacidade de segurança para usar seus recursos de criptografia.

Campo	Descrição
DA	**Sim** aparece ao lado de "DA" somente se as unidades no pool ou grupo de volume suportarem Data Assurance (DA). O DA aumenta a integridade de dados em todo o sistema de storage. O DA permite que o array de storage verifique se há erros que possam ocorrer à medida que os dados são transferidos pelos controladores até os discos. Usar o DA para o novo volume garante que quaisquer erros sejam detectados.
Recurso provisionado (EF300 e EF600 somente)	**Sim** aparece ao lado de "Resource provisioned" somente se as unidades suportarem essa opção. Resource Provisioning é um recurso disponível nos arrays de storage 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 **Avançar** para aceitar os volumes e características recomendados pelo sistema para a carga de trabalho selecionada, ou clique em **Editar volumes** para alterar, adicionar ou excluir os volumes e características 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 do volume. Você pode aceitar o nome padrão ou fornecer um nome mais descritivo, indicando o tipo de dados armazenados no volume.
Capacidade relatada	Defina a capacidade do novo volume e as unidades de capacidade a serem usadas (MiB, GiB ou TiB). Para volumes Thick, a capacidade mínima é 1 MiB e a capacidade máxima é determinada pelo número e capacidade das unidades no pool ou grupo de volume. Lembre-se de que capacidade de storage também é necessária para serviços de cópia (imagens de snapshot, volumes de snapshot, cópias de volume e espelhos remotos); portanto, não aloque toda a capacidade para volumes padrão. 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 seja utilizável, especifique a capacidade em incrementos de 4-GiB ou 8-GiB. Se houver capacidade inutilizável, a única maneira de recuperá-la é aumentar a capacidade do volume.
Tipo de volume	O tipo de volume indica o tipo de volume que foi criado para uma carga de trabalho específica de aplicação.
Tamanho do bloco de volume (EF300 e EF600 only)	Mostra os tamanhos de bloco que podem ser criados para o volume: • 512 — 512 bytes • 4K — 4.096 bytes

Campo	Descrição
Tamanho do segmento	Exibe a configuração de dimensionamento de segmento, que só aparece para volumes em um grupo de volume. Você pode alterar o tamanho do segmento para otimizar o desempenho. **Transições de tamanho de segmento permitidas** — System Manager determina as transições de tamanho de segmento permitidas. Tamanhos de segmento que representam transições inadequadas em relação ao tamanho atual não estão disponíveis na lista suspensa. Transições permitidas geralmente são o dobro ou a 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 é permitido. **Volumes com SSD Cache habilitado** — Você pode especificar um tamanho de segmento de 4 KiB para volumes com SSD Cache habilitado. Certifique-se de selecionar o tamanho de segmento de 4 KiB somente para volumes com SSD Cache habilitado que lidam com operações de E/S de blocos pequenos (por exemplo, tamanhos de bloco de E/S de 16 KiB ou menores). O desempenho pode ser afetado se você selecionar 4 KiB como tamanho de segmento para volumes com SSD Cache habilitado que lidam com operações sequenciais de blocos grandes. **Tempo necessário para alterar o tamanho do segmento** — O tempo necessário para alterar o tamanho do segmento de um volume depende destas variáveis: • A carga de E/S do host • A prioridade de modificação do volume • O número de unidades no grupo de volume • O número de canais de drive • O poder de processamento dos controladores do array de storage. Ao alterar o tamanho do segmento de um volume, o desempenho de E/S é afetado, mas seus dados permanecem disponíveis.

Campo	Descrição
Compatível com segurança	**Sim** aparece ao lado de "Secure-capable" somente se as unidades no pool ou grupo de volume forem secure-capable. A segurança da unidade impede o acesso não autorizado aos dados em uma unidade que foi fisicamente removida do array de storage. Essa opção está disponível somente quando o recurso de segurança da unidade estiver ativado e uma chave de segurança estiver configurada para o array de storage. Um pool ou grupo de volume pode conter tanto unidades com capacidade de segurança quanto unidades sem capacidade de segurança, mas todas as unidades devem ter capacidade de segurança para usar seus recursos de criptografia.
DA	**Sim** aparece ao lado de "DA" somente se as unidades no pool ou grupo de volume suportarem Data Assurance (DA). O DA aumenta a integridade de dados em todo o sistema de storage. O DA permite que o array de storage verifique se há erros que possam ocorrer à medida que os dados são transferidos pelos controladores até os discos. Usar o DA para o novo volume garante que quaisquer erros sejam detectados.
Recurso provisionado (EF300 e EF600 somente)	**Sim** aparece ao lado de "Resource Provisioned" somente se as unidades suportarem essa opção. Resource Provisioning é um recurso disponível nos arrays de storage 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 o aplicativo selecionado, clique em **Avançar** e vá para Etapa 4: revisar a configuração do volume.

Etapa 4: revisar a configuração do volume

Analise um resumo dos volumes que pretende criar e faça as alterações necessárias.

Passos

1. Revise os volumes que deseja criar. Clique em **Voltar** para fazer alterações.
2. Quando estiver satisfeito com sua configuração de volume, clique em **Concluir**.

Resultados

System Manager cria os novos volumes nos pools e grupos de volume selecionados e, em seguida, exibe os novos volumes na tabela All Volumes.

Depois que você terminar

- Execute todas as modificações necessárias no sistema operacional do host da aplicação para que as aplicações possam usar o volume.
- Execute o utilitário específico do sistema operacional (disponível em um fornecedor terceiro) e, em seguida, execute o comando SMcli `-identifyDevices` para correlacionar os nomes dos volumes com os nomes dos arrays de storage do host.

  O SMcli está disponível diretamente através do SANtricity System Manager. Esta versão para download do SMcli está disponível nos controladores E4000, EF600, EF600C, EF300, EF300C, E5700, EF570, E2800 e EF280. Para baixar o SMcli dentro do SANtricity System Manager, selecione **Configurações** > **Sistema** e **Complementos** > **Interface de Linha de Comando**.

Adicionar volumes a uma carga de trabalho no SANtricity System Manager

Você pode adicionar um ou mais volumes a uma carga de trabalho existente ou nova para volumes que não estejam atualmente associados a uma carga de trabalho.

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 array de storage diferente.

Passos

1. Selecione o menu: storage [Volumes].
2. Selecione a guia **Applications & Workloads**.

   A visualização Applications & Workloads é exibida.

3. Selecione **Add to Workload**.

   A caixa de diálogo Select Workload 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 à carga de trabalho é atribuído aos volumes que você adiciona a essa carga de trabalho.

   - **Adicionar volumes a uma nova carga de trabalho** — Selecione esta opção para definir uma nova carga de trabalho para um tipo de aplicação e adicionar volumes à nova carga de trabalho.
5. Selecione **Avançar** para continuar com a sequência de adição à workload.

   A caixa de diálogo Selecionar Volumes é exibida.

6. Selecione os volumes que deseja adicionar à carga de trabalho.
7. Analise os volumes que você deseja adicionar à carga de trabalho selecionada.

8. Quando estiver satisfeito com a configuração da sua carga de trabalho, clique em **Finish**.

Gerenciar volumes

Aumentar a capacidade de um volume no SANtricity System Manager

Você pode aumentar a capacidade relatada (a capacidade relatada aos hosts) de um volume usando a capacidade livre disponível no pool ou volume group.

Antes de começar

- Existe capacidade livre suficiente disponível no pool ou grupo de volume associado do volume.
- O volume está ótimo e não se encontra em nenhum estado de modificação.
- A capacidade máxima relatada de 256 TiB não foi atingida para thin volumes.
- Não há hot spare em uso no volume. (Aplica-se somente a volumes em grupos de volumes.)

Você só pode expandir a capacidade de volume até 128 TiB de cada vez.

Sobre esta tarefa

Leve em consideração quaisquer requisitos futuros de capacidade que você possa ter para outros volumes neste pool ou grupo de volume. Certifique-se de reservar capacidade livre suficiente para criar imagens de snapshot, volumes de snapshot ou espelhos remotos.

Aumentar a capacidade de um volume só é compatível com determinados sistemas operacionais. Se você aumentar a capacidade do volume em um sistema operacional que não seja compatível, a capacidade expandida ficará inutilizável e você não poderá restaurar a capacidade original do volume.

Passos

1. Selecione o menu: storage [Volumes].
2. Selecione o volume para o qual deseja aumentar a capacidade e, em seguida, selecione **Increase Capacity**.

   A caixa de diálogo Confirm Increase Capacity é exibida.

3. Selecione **Yes** para continuar.

   A caixa de diálogo Aumentar a capacidade relatada é exibida.

   Esta caixa de diálogo exibe a capacidade atual relatada do volume e a capacidade livre disponível no pool ou grupo de volume associado ao volume.

4. Use a caixa **Aumentar a capacidade relatada adicionando…** para adicionar capacidade à capacidade relatada disponível atualmente. Você pode alterar o valor da capacidade para exibir em mebibytes (MiB), gibibytes (GiB) ou tebibytes (TiB).
5. Clique em **Increase**.

Resultados

- System Manager aumenta a capacidade do volume com base na sua seleção.
- Selecione o menu: Home[View Operations in Progress] para visualizar o progresso da operação de

aumento de capacidade que está sendo executada para o volume selecionado. Essa operação pode ser demorada e pode afetar o desempenho do sistema.

Depois que você terminar

Após expandir a capacidade do volume, você deve aumentar manualmente o tamanho do sistema de arquivos para que corresponda. Como fazer isso depende do sistema de arquivos que você está usando. Consulte a documentação do seu sistema operacional para obter detalhes.

Inicializar volumes no SANtricity System Manager

Um volume é inicializado automaticamente quando é criado pela primeira vez. No entanto, o Recovery Guru pode recomendar que você inicialize manualmente um volume para se recuperar de determinadas condições de falha. Use esta opção somente sob a orientação do suporte técnico. Você pode selecionar um ou mais volumes para inicializar.

Antes de começar

- Todas as operações de entrada/saída foram interrompidas.
- Quaisquer dispositivos ou file systems nos volumes que você deseja inicializar devem ser desmontados.
- O volume está em status ideal e nenhuma operação de modificação está em andamento no volume.

> Não é possível cancelar a operação após o início. Todos os dados do volume são apagados. Não tente esta operação a menos que o Recovery Guru aconselhe você a fazê-lo. Entre em contato com o suporte técnico antes de iniciar este procedimento.

Sobre esta tarefa

Ao inicializar um volume, o volume mantém seu WWN, atribuições de host, capacidade alocada e configurações de capacidade reservada. Ele também mantém as mesmas configurações de Data Assurance (DA) e configurações de segurança.

Os seguintes tipos de volumes *não podem* ser inicializados:

- Volume base de um volume de snapshot
- Volume primário em uma relação de espelhamento
- Volume secundário em uma relação de espelhamento
- Volume de origem em uma cópia de volume
- Volume de destino em uma cópia de volume
- Volume que já possui uma inicialização em andamento

Este tópico aplica-se apenas a volumes padrão criados a partir de pools ou volume groups.

Passos

1. Selecione o menu: storage [Volumes].
2. Selecione qualquer volume e, em seguida, selecione **More › Initialize volumes**.

   A caixa de diálogo Inicializar Volumes é exibida. Todos os volumes no array de storage aparecem nesta caixa de diálogo.

3. Selecione um ou mais volumes que você deseja inicializar e confirme que deseja realizar a operação.

Resultados

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 gravados sejam lidos como se estivessem preenchidos com zeros (o volume aparece como completamente vazio).

Selecione o **Home › Exibir operações em andamento** para visualizar o progresso da operação de inicialização que está sendo executada para o volume selecionado. Essa operação pode ser demorada e pode afetar o desempenho do sistema.

Redistribuir volumes no SANtricity System Manager

Você redistribui volumes para movê-los de volta aos seus controladores proprietários preferenciais. Normalmente, os drivers de multipath movem volumes de seus controladores proprietários preferenciais quando ocorre um problema no caminho de dados entre o host e o array de storage.

Antes de começar

- Os volumes que você deseja redistribuir não estão em uso ou ocorrerão erros de E/S.
- Um driver multipath deve estar instalado em todos os hosts que utilizam os volumes que você deseja redistribuir, ou ocorrerão erros de E/S.

  Se você deseja redistribuir volumes sem um driver multipath nos hosts, toda a atividade de E/S para os volumes *enquanto a operação de redistribuição estiver em andamento* deve ser interrompida para evitar erros de aplicativo.

Sobre esta tarefa

A maioria dos drivers de multipath do host tenta acessar cada volume em um caminho até o controlador proprietário preferencial. No entanto, se esse caminho preferencial ficar indisponível, o driver de multipath no host alterna 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 controlador proprietário preferencial, mas, em alguns casos, pode ser necessário redistribuir os volumes manualmente.

Passos

1. Selecione o menu: storage [Volumes].
2. Selecione o menu: mais [Redistribuir volumes].

   A caixa de diálogo Redistribuir Volumes é exibida. Todos os volumes no array de storage cujo controlador proprietário preferencial não corresponde ao proprietário atual aparecem nesta caixa de diálogo.

3. Selecione um ou mais volumes que você deseja redistribuir e confirme que deseja realizar a operação.

Resultados

System Manager move os volumes selecionados para seus controladores proprietários preferenciais ou você pode ver uma caixa de diálogo Redistribuir Volumes Desnecessários.

Altere a propriedade do controlador de um volume no SANtricity System Manager

Você pode alterar a propriedade do controlador preferencial de um volume, para que a E/S dos aplicativos do host seja direcionada pelo novo caminho.

Antes de começar

Se você não usar um driver multipath, todos os aplicativos do host que estiverem usando o volume deverão ser encerrados. Essa ação evita erros de aplicativo quando o caminho de E/S for alterado.

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 o menu: storage [Volumes].
2. Selecione qualquer volume e, em seguida, selecione **More › Change ownership**.

   A caixa de diálogo Alterar propriedade do volume é exibida. Todos os volumes no array de storage aparecem nesta caixa de diálogo.

3. Use a lista suspensa **Preferred Owner** para alterar o controlador preferencial de cada volume que deseja modificar e confirme que deseja realizar a operação.

Resultados

- System Manager altera a propriedade do controlador do volume. A entrada/saída (E/S) para o volume agora é direcionada por meio desse caminho de E/S.
- O volume pode não usar o novo caminho de E/S até que o multipath driver se reconfigure para reconhecer o novo caminho. Essa ação geralmente leva menos de cinco minutos.

Excluir um volume no SANtricity System Manager

Normalmente, você exclui volumes se eles foram criados com parâmetros ou capacidade incorretos, não atendem mais às necessidades de configuração de storage ou são imagens de snapshot que não são mais necessárias para backup ou teste de aplicativos.

A exclusão de um volume aumenta a capacidade livre no pool ou volume group. Você pode selecionar um ou mais volumes para excluir.

Antes de começar

Nos volumes que você planeja excluir, certifique-se do seguinte:

- Todos os dados estão em backup.
- Todas as operações de entrada/saída (E/S) são interrompidas.
- Todos os dispositivos e sistemas de arquivos estão desmontados.

Sobre esta tarefa

Não é possível excluir um volume que apresente uma destas condições:

- O volume está sendo inicializado.
- O volume está sendo reconstruído.

- O volume faz parte de um grupo de volume que contém uma unidade que está passando por uma operação de copyback.
- O volume está passando por uma operação de modificação, como uma alteração no tamanho do segmento, a menos que o volume esteja agora no status Failed.
- O volume está mantendo qualquer tipo de reserva persistente.
- O volume é um volume de origem ou um volume de destino em uma cópia de volume que possui o 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 realizada em segundo plano e o espaço liberado pode não estar disponível imediatamente.

Passos

1. Selecione o menu: storage [Volumes].
2. Clique em **Delete**.

   A caixa de diálogo Excluir Volumes é exibida.

3. Selecione um ou mais volumes que você deseja excluir e confirme que deseja realizar a operação.
4. Clique em **Delete**.

Resultados

System Manager executa as seguintes ações:

- Exclui quaisquer imagens de Snapshot, agendamentos e volumes de Snapshot associados.
- Remove quaisquer relações de espelhamento.
- Aumenta a capacidade livre no pool ou grupo de volume.

Altere o limite de capacidade alocada para um volume fino no SANtricity System Manager

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 expandir automaticamente.

Você também pode alterar a porcentagem a partir da qual um alerta (limite de aviso excedido) é enviado para a área de Notificações na página inicial quando um volume thin está próximo do limite de capacidade alocada. Você pode optar por ativar ou desativar essa notificação de alerta.

Este recurso não está disponível nos sistemas de storage EF600/EF600C ou EF300/EF300C.

O sistema expande automaticamente a capacidade alocada com base no limite de capacidade alocada. O limite de capacidade alocada permite limitar o crescimento automático do thin volume a um valor inferior à 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 consideração o espaço a ser consumido tanto pelos dados de usuário do volume quanto pelos dados dos

serviços de cópia.

Passos

1. Selecione o menu: storage [Volumes].
2. Selecione a guia **Thin Volume Monitoring**.

   A visualização de Monitoramento de Thin Volume é exibida.

3. Selecione o volume fino que deseja alterar e, em seguida, selecione **Change Limit**.

   A caixa de diálogo Alterar Limite é exibida. O limite de capacidade alocada e a configuração do limite de aviso para o volume fino selecionado são exibidos nesta caixa de diálogo.

4. Altere o limite de capacidade alocada e o limite de aviso conforme necessário.

   Detalhes do campo

Configuração	Descrição
Alterar o limite de capacidade alocada para…	O limite a partir do qual as gravações falham, impedindo que o volume fino consuma recursos adicionais. Esse limite é uma porcentagem do tamanho da capacidade relatada do volume.
Avise-me quando… (limiar de aviso)	Selecione a caixa de seleção se desejar que o sistema gere um alerta quando um volume fino estiver próximo do limite de capacidade alocada. O alerta é enviado para a área de Notificações na página inicial. Esse limite é uma porcentagem do tamanho da capacidade relatada do volume. Desmarque a caixa de seleção para desativar a notificação de alerta de limiar de aviso.

5. Clique em **Salvar**.

Gerenciar configurações

Altere as configurações de um volume no SANtricity System Manager

Você pode alterar as configurações de um volume, como seu nome, atribuição de host, tamanho do segmento, prioridade de modificação, armazenamento em cache e assim por diante.

Antes de começar

O volume que você deseja alterar está no status Ótimo.

Algumas operações podem estar indisponíveis enquanto as alterações nas configurações do volume estiverem em andamento

Passos

1. Selecione o menu: storage [Volumes].

2. Selecione o volume que você deseja alterar e, em seguida, selecione **View/Edit Settings**.

   A caixa de diálogo Configurações de Volume é exibida. As configurações do volume que você selecionou aparecem nessa caixa de diálogo.

3. Selecione a guia **Básico** para alterar o nome do volume e a atribuição do host.

Detalhes do campo

Configuração	Descrição
Nome	Exibe o nome do volume. Altere o nome de um volume quando o nome atual não for mais significativo ou aplicável.
Capacidades	Exibe a capacidade reportada e alocada para o volume selecionado. A capacidade reportada e a capacidade alocada são as mesmas para volumes espessos, mas são diferentes para volumes finos. Para um volume espesso, o espaço fisicamente alocado é igual ao espaço reportado ao host. Para um volume fino, a capacidade reportada é a capacidade que é reportada aos hosts, enquanto a capacidade alocada é a quantidade de espaço em disco que está atualmente alocada para gravação de dados.
Pool / grupo de volume	Exibe o nome e o nível RAID do pool ou grupo de volume. Indica se o pool ou grupo de volume é compatível com segurança e se está com a segurança habilitada.
Host	Exibe a atribuição de volume. Você atribui um volume a um host ou cluster de hosts para que ele possa ser acessado para operações de E/S. Essa atribuição concede a um host ou cluster de hosts acesso a um volume específico ou a vários volumes em um array de storage. • **Atribuído a** — Identifica o host ou cluster de hosts que tem acesso ao volume selecionado. • **LUN** — Um número de unidade lógica (LUN) é o número atribuído ao espaço de endereçamento 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 endereçamento LUN. Portanto, o mesmo LUN pode ser usado por diferentes hosts para acessar volumes diferentes. Para interfaces NVMe, esta coluna exibe o Namespace ID. Um namespace é um armazenamento NVM formatado para acesso em bloco. É análogo a uma unidade lógica em SCSI, que se relaciona a um volume no array de storage. O Namespace ID é o identificador exclusivo do controlador NVMe para o namespace e pode ser definido com um valor entre 1 e 255. É análogo a um número de unidade lógica (LUN) em SCSI.

Configuração	Descrição
Identificadores	Exibe os identificadores do volume selecionado. • **Identificador mundial (WWID)** — um identificador hexadecimal único para o volume. • **Identificador único estendido (EUI)** — Um identificador EUI-64 para o volume. • **Identificador de subsistema (SSID)** — O identificador do subsistema do array de storage de um volume.

4. Selecione a guia **Advanced** para alterar configurações adicionais de um volume em um pool ou em um grupo de volume.

Detalhes do campo

Configuração	Descrição
Informações sobre aplicativo e carga de trabalho	Durante a criação de volume, você pode criar cargas de trabalho específicas para aplicativos ou outras cargas de trabalho. Se aplicável, o nome da carga de trabalho, o tipo de aplicativo e o tipo de volume aparecem para o volume selecionado. Você pode alterar o nome da carga de trabalho se desejar.
Configurações de qualidade de serviço	**Desativar permanentemente data assurance** — Esta configuração só aparece se o volume tiver data assurance (DA) ativada. DA verifica e corrige erros que podem ocorrer durante a transferência de dados pelos controladores até as unidades. Use esta opção para desativar permanentemente DA no volume selecionado. Quando desativada, DA não poderá ser reativada neste volume. **Habilitar verificação de redundância pré-leitura** — Esta configuração só aparece se o volume for um volume espesso. As verificações de redundância pré-leitura determinam se os dados em um volume são consistentes sempre que uma leitura é realizada. Um volume com este recurso habilitado retorna erros de leitura se os dados forem considerados inconsistentes pelo firmware do controlador.
Propriedade do controlador	Define o controlador que é designado para ser o proprietário ou controlador principal do volume. A gestão dos controladores é muito importante e deve ser planejada cuidadosamente. Os controladores devem ser distribuídos da forma mais equilibrada possível para o total de I/Os.

Configuração	Descrição
Dimensionamento de segmentos	Exibe a configuração de dimensionamento de segmento, que aparece apenas para volumes em um grupo de volume. Você pode alterar o tamanho do segmento para otimizar o desempenho. **Transições de tamanho de segmento permitidas** — System Manager determina as transições de tamanho de segmento permitidas. Tamanhos de segmento que representam transições inadequadas em relação ao tamanho atual não estão disponíveis na lista suspensa. Transições permitidas geralmente são o dobro ou a 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 é permitido. **Volumes com SSD Cache habilitado** — Você pode especificar um tamanho de segmento de 4 KiB para volumes com SSD Cache habilitado. Certifique-se de selecionar o tamanho de segmento de 4 KiB somente para volumes com SSD Cache habilitado que lidam com operações de E/S de blocos pequenos (por exemplo, tamanhos de bloco de E/S de 16 KiB ou menores). O desempenho pode ser afetado se você selecionar 4 KiB como tamanho de segmento para volumes com SSD Cache habilitado que lidam com operações sequenciais de blocos grandes. **Tempo necessário para alterar o tamanho do segmento** — O tempo necessário para alterar o tamanho do segmento de um volume depende destas variáveis: • A carga de E/S do host • A prioridade de modificação do volume • O número de unidades no grupo de volume • O número de canais de drive • O poder de processamento dos controladores do array de storage. Ao alterar o tamanho do segmento de um volume, o desempenho de E/S é afetado, mas seus dados permanecem disponíveis.
Prioridade de modificação	Mostra a configuração de prioridade de modificação, que só aparece para volumes em um grupo de volume. 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. Mova as barras deslizantes para selecionar um nível de prioridade. **Taxas de prioridade de modificação** — A taxa de prioridade mais baixa beneficia o desempenho do sistema, mas a operação de modificação leva mais tempo. A taxa de prioridade mais alta beneficia a operação de modificação, mas o desempenho do sistema pode ser comprometido.

Configuração	Descrição
Armazenamento em cache	Exibe a configuração de armazenamento em cache, que você pode alterar para afetar o desempenho geral de E/S de um volume.
Cache SSD	Exibe a configuração de cache SSD, que você pode ativar em volumes compatíveis como uma forma de melhorar o desempenho somente de leitura. Os volumes são compatíveis se compartilharem as mesmas capacidades de Drive Security e Data Assurance. **O recurso de cache SSD utiliza um ou mais discos de estado sólido (SSDs) para implementar um cache de leitura**. O desempenho dos aplicativos é aprimorado devido aos tempos de leitura mais rápidos dos SSDs. Como o cache de leitura está no array de storage, o armazenamento em cache é compartilhado entre todos os aplicativos que utilizam o array de storage. Basta selecionar o volume que você deseja armazenar em cache, e então o armazenamento em cache será automático e dinâmico.

5. Clique em **Salvar**.

   System Manager altera as configurações do volume com base nas suas seleções.

Depois que você terminar

Selecione o menu: Home [View Operations in Progress] para visualizar o progresso das operações de alteração que estão sendo executadas no momento para o volume selecionado.

Alterar configurações de carga de trabalho no SANtricity System Manager

Você pode alterar o nome de uma carga de trabalho e visualizar o 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 o menu: storage [Volumes].
2. Selecione a guia **Applications & Workloads**.

   A visualização Applications & Workloads é exibida.

3. Selecione a carga de trabalho que deseja alterar e, em seguida, selecione **View/Edit Settings**.

   A caixa de diálogo Applications & Workloads Settings é exibida.

4. **Opcional:** Altere o nome da carga de trabalho fornecido pelo usuário.
5. Clique em **Salvar**.

Altere as configurações de armazenamento em cache de um volume no SANtricity System Manager

Você pode alterar as configurações de armazenamento em cache de leitura e armazenamento em cache de gravação para impactar o desempenho geral de E/S de

um volume.

Sobre esta tarefa

Tenha em mente estas diretrizes ao alterar as configurações de armazenamento em cache de um volume:

- Após abrir a caixa de diálogo Alterar configurações de cache, você poderá ver um ícone ao lado das propriedades de cache selecionadas. Esse ícone indica que o controlador suspendeu temporariamente as operações de armazenamento em cache.

  Essa ação pode ocorrer quando uma bateria nova está carregando, quando um controlador foi removido ou se o controlador detectou uma incompatibilidade nos tamanhos de cache. Após a resolução da condição, as propriedades de armazenamento em cache selecionadas na caixa de diálogo se tornam ativas. Se as propriedades de armazenamento em cache selecionadas não se tornarem ativas, entre em contato com o suporte técnico.

- Você pode alterar as configurações de armazenamento em cache para um único volume ou para vários volumes em um array de storage. Você pode alterar as configurações de armazenamento em cache para todos os volumes padrão ou para todos os volumes thin ao mesmo tempo.

Passos

1. Selecione o menu: storage [Volumes].
2. Selecione qualquer volume e, em seguida, selecione **More › Change cache settings**.

   A caixa de diálogo Alterar configurações de cache é exibida. Todos os volumes no array de storage aparecem nesta caixa de diálogo.

3. Selecione a guia **Básico** para alterar as configurações de armazenamento em cache de leitura e armazenamento em cache de gravação.

   Detalhes do campo

Configuração de armazenamento em cache	Descrição
Armazenamento em cache de leitura	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 serem liberados.
Armazenamento em cache de gravação	O cache de gravação é um buffer que armazena dados do host que ainda não foram gravados nos discos. Os dados permanecem no cache de gravação até serem gravados nos discos. O armazenamento em cache pode aumentar o desempenho de E/S. O cache é limpo automaticamente após o **armazenamento em cache** ser desativado para um volume.

4. Selecione a guia **Advanced** para alterar as configurações avançadas de volumes thick. As configurações avançadas de cache estão disponíveis apenas para volumes thick.

Detalhes do campo

Configuração de armazenamento em cache	Descrição
Pré-busca dinâmica de cache de leitura	O pré-carregamento dinâmico de leitura em cache permite que o controlador copie blocos de dados sequenciais adicionais para o cache enquanto lê blocos de dados de uma unidade para o cache. Esse armazenamento em cache aumenta a chance de que solicitações futuras de dados possam ser atendidas pelo cache. O pré-carregamento dinâmico de leitura em cache é importante para aplicativos multimídia que usam E/S sequencial. A taxa e a quantidade de dados pré-carregados no cache se ajustam automaticamente com base na taxa e no tamanho das solicitações de leitura do host. O acesso aleatório não faz com que dados sejam pré-carregados no cache. Esse recurso não se aplica quando o armazenamento em cache está desativado. Para um volume fino, a pré-busca de leitura em cache dinâmica está sempre desativada e não pode ser alterada.
Armazenamento em cache de gravação sem baterias	A configuração de armazenamento em cache de gravação sem baterias permite que o armazenamento em cache continue mesmo quando as baterias estão ausentes, com defeito, completamente descarregadas ou não totalmente carregadas. Escolher armazenamento em cache de gravação sem baterias geralmente não é recomendado, pois os dados podem ser perdidos se houver uma queda de energia. Normalmente, o armazenamento em cache é desativado temporariamente pelo controlador até que as baterias sejam carregadas ou uma bateria com defeito seja substituída. **Possível perda de dados** — Se você selecionar esta opção e não tiver uma fonte de alimentação universal para proteção, poderá perder dados. Além disso, você poderá perder dados se não tiver baterias para o controlador e ativar a opção **Gravar em cache sem baterias**. Essa configuração só está disponível se você tiver habilitado o armazenamento em cache de gravação. Essa configuração não está disponível para volumes finos.

Configuração de armazenamento em cache	Descrição
Armazenamento em cache de gravação com espelhamento	O armazenamento em cache com espelhamento ocorre quando os dados gravados na memória cache de um controlador também são gravados na memória 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 está disponível somente se o armazenamento em cache de gravação estiver habilitado e houver dois controladores. O armazenamento em cache com espelhamento é a configuração padrão na criação do volume. Essa configuração só está disponível se você tiver habilitado o armazenamento em cache de gravação. Essa configuração não está disponível para volumes finos.

5. Clique em **Salvar** para alterar as configurações de armazenamento em cache.

Altere as configurações de verificação de mídia para um volume no SANtricity System Manager

Uma verificação de mídia é uma operação em segundo plano que examina todos os dados e informações de redundância no volume. Use esta opção para ativar ou desativar as configurações de verificação de mídia para um ou mais volumes ou para alterar a duração da verificação.

Antes de começar

Entenda o seguinte:

- As varreduras de mídia são executadas continuamente a uma taxa constante com base na capacidade a ser varrida e na duração da varredura. As varreduras em segundo plano podem ser temporariamente suspensas por uma tarefa em segundo plano de prioridade mais alta (por exemplo, reconstrução), mas serão retomadas na mesma taxa constante.
- Um volume é verificado somente quando a opção de verificação de mídia está habilitada para o array de storage e para esse volume. Se a verificação de redundância também estiver habilitada para esse volume, as informações de redundância no volume serão verificadas quanto à consistência com os dados, desde que o volume possua redundância. A verificação de mídia com verificação de redundância é habilitada por padrão para cada volume quando ele é criado.
- Caso seja encontrado um erro irrecuperável na mídia durante a verificação, os dados serão reparados utilizando informações de redundância, se disponíveis.

  Por exemplo, informações de redundância estão disponíveis em volumes RAID 5 otimizados ou em volumes RAID 6 que estão otimizados ou têm apenas 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 setores ilegíveis. Tanto erros de mídia corrigíveis quanto incorrigíveis são registrados no log de eventos.

  Se a verificação de redundância encontrar uma inconsistência entre os dados e as informações de redundância, isso será relatado no registro de eventos.

O período padrão de verificação de mídia é definido em 120 dias.

Sobre esta tarefa

A verificação de mídia detecta e corrige erros em blocos de disco que são lidos com pouca frequência pelos aplicativos. Isso pode evitar perda de dados em caso de falha de uma unidade, pois os dados das unidades com falha são reconstruídos usando informações de redundância e dados de outras unidades no grupo de volume ou pool.

Você pode realizar as seguintes ações:

- Ative ou desative as verificações de mídia em segundo plano para todo o array de storage
- Altere a duração da varredura para todo o array de storage
- Ativar ou desativar a verificação de mídia para um ou mais volumes
- Ative ou desative a verificação de redundância para um ou mais volumes

Passos

1. Selecione o menu: storage [Volumes].
2. Selecione qualquer volume e, em seguida, selecione **More › Change media scan settings**.

   A caixa de diálogo Alterar configurações de verificação de mídia da unidade é exibida. Todos os volumes no array de storage aparecem nesta caixa de diálogo.

3. Para ativar a verificação de mídia, selecione a caixa de seleção **Verificar mídia ao longo de…**.

   Desativar a caixa de seleção de verificação de mídia suspende todas as configurações de verificação de mídia.

4. Especifique o número de dias durante os quais você deseja que a verificação de mídia seja executada.
5. Selecione a caixa de seleção **Verificação de mídia** para cada volume no qual deseja realizar uma verificação de mídia.

   System Manager habilita a opção Verificação de Redundância para cada volume no qual você optar por executar uma verificação 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**.

   System Manager aplica alterações às verificações de mídia em segundo plano com base na sua seleção.

Use os serviços de cópia

Saiba mais sobre cópia de volume no SANtricity System Manager

A função Copiar Volume permite criar uma cópia pontual de um volume, criando dois volumes separados, o volume de origem e o volume de destino, no mesmo array de storage.

Esta função realiza uma cópia byte a 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 de um volume mudam, você pode usar a função Copy Volume para copiar dados de pools ou grupos de volume que usam unidades de menor capacidade para pools ou grupos de volume que usam unidades de maior capacidade. Por exemplo, você pode usar a função Copy Volume para fazer o seguinte:

- Mova os dados para unidades de disco maiores.
- Troque para unidades com uma taxa de transferência de dados mais alta.
- Mude para unidades que utilizam novas tecnologias para obter maior desempenho.
- Alterar um volume fino para um volume espesso.

Os volumes de origem e destino da cópia devem ter os mesmos tamanhos de bloco endereçáveis/lógicos (tamanho do setor) relatados pelo host.

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 de 512** - as unidades são 4K, mas o tamanho de bloco relatado é 512.

Alterar um volume fino para um volume espesso

Se você deseja converter um volume fino em um volume espesso, use a operação Copy Volume para criar uma cópia do volume fino. O destino de uma operação Copy Volume é sempre um volume espesso.

> System Manager não oferece uma opção para criar thin volumes. Se você deseja criar thin volumes, use a command line interface (CLI).

Backup de dados

A função Copy Volume permite fazer backup de um volume copiando dados de um volume para outro no mesmo array de storage. Você pode usar o volume de destino como backup do volume de origem, para testes de sistema ou para fazer backup em outro dispositivo, como uma unidade de fita.

Restaurar dados do volume de Snapshot para o volume base

Se precisar restaurar dados para o volume base a partir do seu volume de Snapshot associado, você pode usar a função Copy Volume para copiar os dados do volume de Snapshot para o volume base. Você pode criar uma cópia de volume dos dados no volume de Snapshot 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 como volumes de origem e de destino com a função Copy Volume.

Tipo de volume	Volume de origem da cópia de volume off-line	Volume de origem da cópia de volume on-line	Volume de destino online e off-line
Volume espesso em um pool	Sim	Sim	Sim

Tipo de volume	Volume de origem da cópia de volume off-line	Volume de origem da cópia de volume on-line	Volume de destino online e off-line
Volume espesso em um grupo de volume	Sim	Sim	Sim
Volume fino	Sim[1]	Sim	Não
Volume de Snapshot	Sim[2]	Não	Não
Volume base do Snapshot	Sim	Sim	Não
Volume primário do espelho remoto	Sim[3]	Sim	Não

[1] O volume de destino deve ter uma capacidade igual ou superior à capacidade relatada do volume fino.

[2] Você não poderá usar a cópia de volume Snapshot 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.

Saiba mais sobre os tipos de operações de cópia de volume no software SANtricity

Você pode realizar uma operação de Cópia de Volume *offline* ou uma operação de Cópia de Volume *online*. Uma operação offline lê dados de um volume de origem e os copia para um volume de destino. Uma operação online usa um volume de snapshot como origem e copia seus dados para um volume de destino.

Para garantir a integridade de dados, toda a atividade de E/S para o volume de destino é suspensa durante qualquer tipo de operação de Copy Volume. Essa suspensão ocorre porque o estado dos dados no volume de destino fica inconsistente até que o procedimento seja concluído.

As operações de Copy Volume offline e online são descritas abaixo.

Operação de cópia de volume offline

A relação de Copy Volume offline é entre um volume de origem e um volume de destino. Uma cópia offline lê dados do volume de origem e os copia para um volume de destino, enquanto suspende todas as atualizações no volume de origem com a cópia em andamento. Todas as atualizações no 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 participam de uma cópia offline estão disponíveis para atividades de E/S somente leitura enquanto uma operação de Copy Volume tiver o status de In Progress ou Pending. • As solicitações de gravação são permitidas após a cópia offline ser concluída. • Para evitar mensagens de erro de proteção contra gravação, não acesse um volume de origem que esteja participando de uma operação de Copy Volume com o status de In Progress.
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 poderá ser rejeitada pelos controladores do array de storage, e uma mensagem de erro poderá aparecer. • O driver do sistema de arquivos com 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. • Para evitar que esse problema ocorra, não tente acessar um volume de origem que esteja participando de uma cópia offline enquanto a operação Copy Volume estiver com o status de In Progress.

Operação de cópia de volume online

A relação de Copy Volume online é entre um volume de snapshot e um volume de destino. Você pode iniciar uma operação de Copy Volume enquanto o volume de origem estiver online e disponível para gravação de dados. Essa função é realizada criando um snapshot do volume e usando o snapshot como o volume de origem real para a cópia.

Ao iniciar uma operação de Copy Volume para um volume de origem, System Manager cria uma imagem pontual do volume base e uma relação de cópia entre a imagem pontual do volume base e um volume de destino. Usar a imagem pontual como volume de origem permite que o array de storage continue gravando no volume de origem enquanto a cópia está em andamento.

Durante uma operação de cópia online, ocorre uma queda no desempenho devido ao copy-on-write. Após a conclusão da cópia online, 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 no array de storage. • Um volume de destino pode ser um volume padrão em um grupo de volume ou um volume padrão em um pool. Um volume de destino não pode ser um volume fino ou um volume base em um grupo de snapshot. • Você pode usar a função online Copy Volume para copiar dados de um volume thin para um volume standard em um pool que reside no mesmo array de storage. Mas você não pode usar a função Copy Volume para copiar dados de um volume standard para um volume thin.
Desempenho do volume base	• Se o volume de snapshot usado como origem da cópia estiver ativo, o desempenho do volume base será prejudicado devido às operações de copy-on-write. Quando a cópia for concluída, o snapshot será desativado e o desempenho do volume base será restaurado. Embora o snapshot esteja desativado, o volume de capacidade reservada e a relação de cópia permanecem intactos.
Tipos de volumes criados	• Um volume de snapshot e um volume de capacidade reservada são criados durante a operação de cópia online. • O volume de snapshot não é um volume real que contém dados; em vez disso, é uma referência aos dados que estavam contidos em um volume em um momento específico. • Para cada snapshot que é tirado, um volume de capacidade reservada é criado para armazenar os dados do snapshot. O volume de capacidade reservada é usado apenas para gerenciar a imagem do snapshot.
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 salvaguarda. • Como o volume de capacidade reservada armazena cópias dos dados originais nesses blocos de dados, alterações subsequentes nesses blocos de dados são gravadas somente no volume de origem. • A operação de cópia online utiliza menos espaço de 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 da criação do snapshot.

Copie um volume no SANtricity System Manager

Você pode copiar dados de um volume para outro no mesmo array de storage e criar uma duplicata física pontual (clone) de um volume de origem.

Antes de começar

- Toda a atividade de I/O para o volume de origem e o volume de destino deve ser interrompida.
- Todos os sistemas de arquivos no volume de origem e no volume de destino devem ser desmontados.
- Se você já utilizou o volume de destino em uma operação de Cópia de Volume anteriormente, você não

precisa mais desses dados ou já fez backup dos dados.

Sobre esta tarefa

O volume de origem é o volume que aceita operações de E/S do host e armazena os dados do aplicativo. Quando uma cópia de volume é iniciada, os dados do volume de origem são copiados integralmente 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 de Copy Volume. O volume de destino deve ter a mesma ou maior capacidade que o volume de origem; no entanto, ele pode ter um nível RAID diferente.

Mais informações sobre cópias online e off-line

Cópia online

Uma cópia online cria uma cópia pontual de qualquer volume dentro de um array de storage, enquanto ainda é possível gravar no volume com a cópia em andamento. Essa função é alcançada criando um snapshot do volume e usando o snapshot 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 thin no array de storage.

Cópia off-line

Uma cópia off-line lê os dados do volume de origem e os copia para um volume de destino, suspendendo todas as atualizações no volume de origem durante o processo de cópia. Todas as atualizações no volume de origem são suspensas para evitar inconsistências cronológicas no volume de destino. A relação de cópia de volume off-line ocorre entre um volume de origem e um volume de destino.

Uma operação de cópia de volume sobrescreve os dados no volume de destino e falha todos os volumes de Snapshot associados ao volume de destino, caso existam.

Passos

1. Selecione o menu: storage [Volumes].
2. Selecione o volume que deseja usar como origem para a operação de Cópia de Volume e, em seguida, selecione **Copy Services › Copy volume**.

   A caixa de diálogo Copy Volume-Select Target é exibida.

3. Selecione o volume de destino para o qual deseja copiar os dados.

   A tabela exibida 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 Copy Volume.

   A prioridade de cópia determina quanto dos recursos do sistema são usados para concluir a operação de cópia de volume em comparação com as solicitações de E/S de serviço.

Mais informações sobre taxas de prioridade de cópia

Existem cinco taxas de prioridade de cópia:

- Mais baixo
- Baixo
- Médio
- Alto
- Mais alto

Se a prioridade de cópia estiver definida para a taxa mais baixa, a atividade de E/S é priorizada e a operação Copy Volume leva mais tempo. Se a prioridade de cópia estiver definida para a taxa mais alta, a operação Copy Volume é priorizada, mas a atividade de E/S do array de storage pode ser afetada.

5. Selecione se deseja criar uma cópia online ou uma cópia off-line. Para criar uma cópia online, marque a caixa de seleção **Manter o volume de origem online durante a operação de cópia**.
6. Faça uma das seguintes ações:
   - Para realizar uma operação de cópia *online*, clique em **Avançar** para continuar para a caixa de diálogo **Reserve Capacity**.
   - Para realizar uma operação de cópia off-line, clique em **Concluir** para iniciar a cópia off-line.
7. Se você escolher criar uma cópia online, defina a capacidade reservada necessária para armazenar dados e outras informações para a cópia online e clique em **Concluir** para iniciar a cópia online.

   A tabela de volumes candidatos exibe apenas os candidatos que suportam a capacidade reservada especificada. A capacidade reservada é a capacidade física alocada que é usada para qualquer operação de serviço de cópia e objeto de storage. Não é diretamente legível pelo host.

   Aloque a capacidade reservada usando as seguintes diretrizes:

   - A configuração padrão para capacidade reservada é 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 permanecer ativo, maior deverá ser a capacidade reservada.

Resultados

System Manager copia todos os dados do volume de origem para o volume de destino. Após a conclusão da operação de Copy Volume, o volume de destino torna-se automaticamente somente leitura para os hosts.

Depois que você terminar

Selecione o menu: Home [View Operations in Progress] para visualizar o progresso da operação Copy Volume. Essa operação pode ser demorada e pode afetar o desempenho do sistema.

Execute uma operação Copy Volume no SANtricity System Manager

Você pode visualizar uma operação de Copy Volume em andamento e interromper, alterar a prioridade, recopiar ou limpar uma operação de Copy Volume.

Passos

1. Selecione o menu: Início [Visualizar operações em andamento].

   A caixa de diálogo Operações em andamento é exibida.

2. Localize a operação Copy Volume na qual deseja realizar uma ação e clique no link na coluna **Actions** para executar uma das seguintes ações.

   Leia todo o texto de advertência fornecido nas caixas de diálogo, especialmente ao interromper uma operação.

Ação	Descrição
Parar	Você pode interromper uma operação de Copy Volume enquanto a operação estiver com o status Em andamento, Pendente ou Falha. Quando a Copy Volume é interrompida, todos os hosts mapeados têm acesso de gravação ao volume de origem. Se dados forem gravados no volume de origem, os dados no volume de destino não corresponderão mais aos dados no volume de origem.
Alterar prioridade	Você pode alterar a prioridade de uma operação de Cópia de Volume enquanto a operação estiver com o status de Em Andamento para selecionar a taxa com que uma operação de Cópia de Volume é concluída.
Recopiar	Você pode copiar um volume novamente quando tiver interrompido uma operação de Copy Volume e quiser iniciá-la novamente ou quando uma operação de Copy Volume falhar ou for interrompida. A operação de Copy Volume recomeça do início. A ação de recópia sobrescreve os dados existentes no volume de destino e falha todos os volumes de Snapshot associados ao volume de destino, caso existam.
Limpar	Você pode remover a operação Copiar Volume enquanto a operação estiver com o status Em andamento, Pendente ou Falha. Certifique-se de que deseja realizar esta operação antes de selecionar **Limpar**. Não há caixa de diálogo de confirmação.

Perguntas frequentes sobre volumes e cargas de trabalho para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

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 array de storage.

Um volume é criado a partir da capacidade disponível em um pool ou um grupo de volume. 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 sobrealocação de capacidade quando tenho capacidade livre suficiente em um grupo de volume 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 do não uso de toda a capacidade livre disponível durante a criação do volume.

Ao criar um volume em um grupo de volume que possui uma ou mais áreas de capacidade livre, a capacidade do volume é limitada à maior área de capacidade livre nesse grupo de volume. 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 com capacidade livre, o gráfico do grupo de volume conterá um link indicando o número de áreas de capacidade livre existentes. Selecione o link para exibir uma janela pop-up que indica a capacidade de cada área.

Ao consolidar a capacidade livre, você pode criar volumes adicionais a partir da quantidade máxima de capacidade livre em um grupo de volume. Você pode consolidar a capacidade livre existente em um grupo de volume selecionado usando um dos seguintes métodos:

- Quando pelo menos uma área de capacidade livre é detectada para um grupo de volume, a recomendação "Consolidar capacidade livre" aparece na página inicial na área de Notificações. Clique no link **Consolidar capacidade livre** para abrir a caixa de diálogo.
- Você também pode selecionar **Pools & Volume Groups › Uncommon Tasks › Consolidate volume group free capacity** para abrir a caixa de diálogo.

Se você deseja usar uma área de capacidade livre específica em vez da maior área de capacidade livre, use a interface de linha de comando (CLI).

Como a carga de trabalho selecionada afeta a criação de volumes?

Durante a criação de um volume, você será solicitado a fornecer informações sobre o uso da carga de trabalho. O sistema utiliza essas informações para criar uma configuração de volume ideal para você, que pode ser editada conforme necessário. Opcionalmente, você pode ignorar esta etapa na sequência de criação do volume.

Uma carga de trabalho é um objeto de storage que suporta uma aplicação. Você pode definir uma ou mais cargas de trabalho, ou instâncias, por aplicação. Para algumas aplicações, o sistema configura a carga de trabalho para conter volumes com características subjacentes semelhantes. Essas características de volume são otimizadas com base no tipo de aplicação que a carga de trabalho suporta. Por exemplo, se você criar uma carga de trabalho que suporte uma aplicação Microsoft SQL Server e, posteriormente, criar volumes para essa carga de trabalho, as características subjacentes do volume serão otimizadas para suportar Microsoft SQL Server.

- **Específico da aplicação** — Ao criar 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 da aplicação e outro tráfego da sua instância da aplicação. Características do volume, como tipo de E/S, tamanho do segmento, propriedade do controlador e cache de leitura e gravação, são automaticamente recomendadas e otimizadas para cargas de trabalho criadas para os seguintes tipos de aplicação.
  - Microsoft® SQL Server™

- Microsoft® Exchange Server™
- Aplicações de videovigilância
- VMware ESXi™ (para volumes a serem usados com Virtual Machine File System)

  Você pode revisar a configuração de volume recomendada e editar, adicionar ou excluir os volumes e características recomendados pelo sistema usando a caixa de diálogo Add/Edit Volumes.

- **Outros** (ou aplicações sem suporte específico para criação de volumes) — Outras cargas de trabalho utilizam uma configuração de volume que você deve especificar manualmente quando quiser criar uma carga de trabalho que não está associada a uma aplicação específica ou se não houver otimização incorporada para a aplicação que você pretende usar no array de storage. Você deve especificar manualmente a configuração de volume usando a caixa de diálogo Adicionar/Editar Volumes.

Por que esses volumes não estão associados a uma workload?

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 array de storage diferente.

Por que não posso 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 array de storage diferente. Como resultado, os volumes nessa carga de trabalho não estão associados a uma carga de trabalho específica de aplicativo, portanto, a carga de trabalho não pode ser excluída.

Como as cargas de trabalho específicas da aplicação me ajudam a gerenciar meu array de storage?

As características de volume da sua carga de trabalho específica da aplicação ditam como essa carga interage com os componentes do seu array de storage e ajudam a determinar o desempenho do seu ambiente sob uma determinada configuração.

Uma aplicação é um software como SQL Server ou Exchange. Você define uma ou mais cargas de trabalho para dar suporte a cada aplicação.

Como fornecer essas informações ajuda a criar storage?

As informações da carga de trabalho são usadas para otimizar as características 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 array de storage.

Com base nas informações de carga de trabalho que você fornece, System Manager cria os volumes apropriados e os coloca nos pools ou grupos de volumes disponíveis que existem atualmente no sistema. O sistema cria os volumes e otimiza suas características com base nas melhores práticas atuais para a carga de trabalho que você selecionou.

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 características recomendados pelo sistema usando a caixa de diálogo Add/Edit Volumes.

Consulte a documentação específica da sua aplicação para obter informações sobre melhores práticas.

O que preciso fazer para reconhecer a capacidade expandida?

Se você aumentar a capacidade de um volume, o host pode não reconhecer imediatamente o aumento na capacidade do volume.

A maioria dos sistemas operacionais reconhece a capacidade expandida do volume e a expande automaticamente após a expansão de volume ser iniciada. No entanto, alguns podem não reconhecer. Se o seu sistema operacional não reconhecer automaticamente a capacidade expandida do volume, talvez seja necessário realizar uma nova verificação do disco ou reinicializar.

Após expandir a capacidade do volume, você deve aumentar manualmente o tamanho do sistema de arquivos para que corresponda. Como fazer isso depende do sistema de arquivos que você está usando.

Consulte a documentação do sistema operacional do seu host para obter mais detalhes.

Por que não vejo todos os meus pools e/ou grupos de volume?

Qualquer pool ou grupo de volume para o qual você não possa mover o volume não é exibido na lista.

Pools ou grupos de volume não são elegíveis por nenhum dos seguintes motivos:

- Os recursos de Data Assurance (DA) de um pool ou grupo de volume 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 tamanho de segmento?

Um segmento é a quantidade de dados em kilobytes (KiB) armazenada em uma unidade antes que o array de storage passe para a próxima unidade na faixa (grupo RAID). O tamanho do segmento se aplica somente a grupos de volume, não a pools.

O tamanho do segmento é definido pelo número de blocos de dados que ele contém. Ao determinar o tamanho do segmento, você deve saber que tipo de dados irá armazenar em um volume. Se um aplicativo normalmente usa leituras e gravações pequenas e aleatórias (IOPS), um tamanho de segmento menor geralmente funciona melhor. Alternativamente, se o aplicativo tem leituras e gravações grandes e sequenciais (taxa de transferência), um tamanho de segmento maior geralmente é melhor.

Independentemente de uma aplicação utilizar pequenas leituras e gravações aleatórias ou grandes leituras e gravações sequenciais, o array de storage apresenta melhor desempenho se o tamanho do segmento for maior que o tamanho típico do bloco de dados. Isso normalmente facilita e agiliza o acesso aos dados pelas unidades, o que é importante para um melhor desempenho do array de storage.

Ambientes onde o desempenho de IOPS é importante

Em um ambiente de operações de entrada/saída por segundo (IOPS), o array de storage tem um desempenho melhor se você usar um tamanho de segmento maior do que o tamanho típico do bloco de dados (“chunk”) que é lido/gravado em uma unidade. Isso garante que cada chunk seja gravado em uma unidade única.

Ambientes onde a taxa de transferência é importante

Em um ambiente de throughput, o tamanho do segmento deve ser uma fração exata do total de unidades para dados e do tamanho típico do bloco de dados (tamanho de E/S). Isso distribui os dados como uma única faixa entre as unidades no grupo de volume, levando a leituras e gravações mais rápidas.

O que é propriedade preferencial do controlador?

A propriedade do controlador preferencial define o controlador que é designado como proprietário, ou controlador primário, do volume.

A gestão dos controladores é muito importante e deve ser planejada cuidadosamente. Os controladores devem ser distribuídos da forma mais equilibrada possível para o total de I/Os.

Por exemplo, se um controlador lê principalmente blocos de dados grandes e sequenciais e o outro controlador tem 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 entre os dois controladores.

Quando eu deveria usar a seleção atribuir host posteriormente?

Se você deseja acelerar o processo de criação de volumes, pode ignorar a etapa de atribuição de host para que os volumes recém-criados sejam inicializados offline.

Os volumes recém-criados devem ser inicializados. O sistema pode inicializá-los usando um dos dois modos — um processo de inicialização em segundo plano Immediate Available Format (IAF) ou um processo offline.

Ao mapear um volume para um host, você força todos os volumes em inicialização nesse grupo a passarem para a inicialização em segundo plano. Esse processo de inicialização em segundo plano permite E/S simultânea do host, o que às vezes pode ser demorado.

Quando nenhum dos volumes em um grupo de volume está mapeado, a inicialização offline é realizada. O processo offline é muito mais rápido do que o processo em segundo plano.

O que preciso saber sobre os requisitos de tamanho de bloco do host?

Para os sistemas EF300 e EF600, um volume pode ser configurado 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 (notavelmente 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 configurando um volume para apresentar um tamanho de bloco de 4KiB; no entanto, verifique se o seu host permite blocos de 4KiB (ou “4Kn”).
- O tipo de unidades que você selecionar para seu pool ou grupo de volume também determina quais tamanhos de bloco de volume são suportados, conforme a seguir:
  - Se você criar um grupo de volume usando unidades que gravam em blocos de 512 bytes, então só poderá criar volumes com blocos de 512 bytes.
  - Se você criar um grupo de volume usando unidades que gravam em blocos de 4KiB, então poderá criar volumes com blocos de 512 bytes ou de 4KiB.
- Se o array tiver uma placa de interface de host iSCSI, todos os volumes serão 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 o tamanho de um bloco depois de definido. Se precisar alterar o tamanho de um bloco, você deve excluir o volume e recriá-lo.

Hosts e clusters de hosts

Aprenda sobre hosts e clusters de hosts no SANtricity software

Você pode configurar hosts e clusters de hosts, que definem as conexões entre o array de storage e os servidores de dados.

O que são hosts e clusters de hosts?

Um *host* é um servidor que envia operações de E/S para um volume em um array de storage. Um *host cluster* é um grupo de hosts, que você pode criar para atribuir os mesmos volumes a vários hosts.

Saiba mais:

- "Terminologia do host"
- "Acessar volumes"
- "Número máximo de LUNs"

Como faço para configurar hosts e clusters de hosts?

Para definir conexões de host, você pode acessar **Storage › Hosts** para configurar o host manualmente. Se desejar que dois ou mais hosts compartilhem o acesso ao mesmo conjunto de volumes, você pode então definir um cluster e atribuir os volumes a esse cluster.

Saiba mais:

- "Criação manual de host"
- "Como os volumes são atribuídos a hosts e clusters de hosts"
- "Fluxograma para criação de hosts e atribuição de volumes"
- "Criar host manualmente"
- "Criar cluster de hosts"
- "Atribuir volumes aos hosts"

Informações relacionadas

Saiba mais sobre tarefas relacionadas a hosts:

- "Defina o balanceamento de carga automático"
- "${post_edited_translations.segment}"
- "${post_edited_translations.segment}"

Conceitos

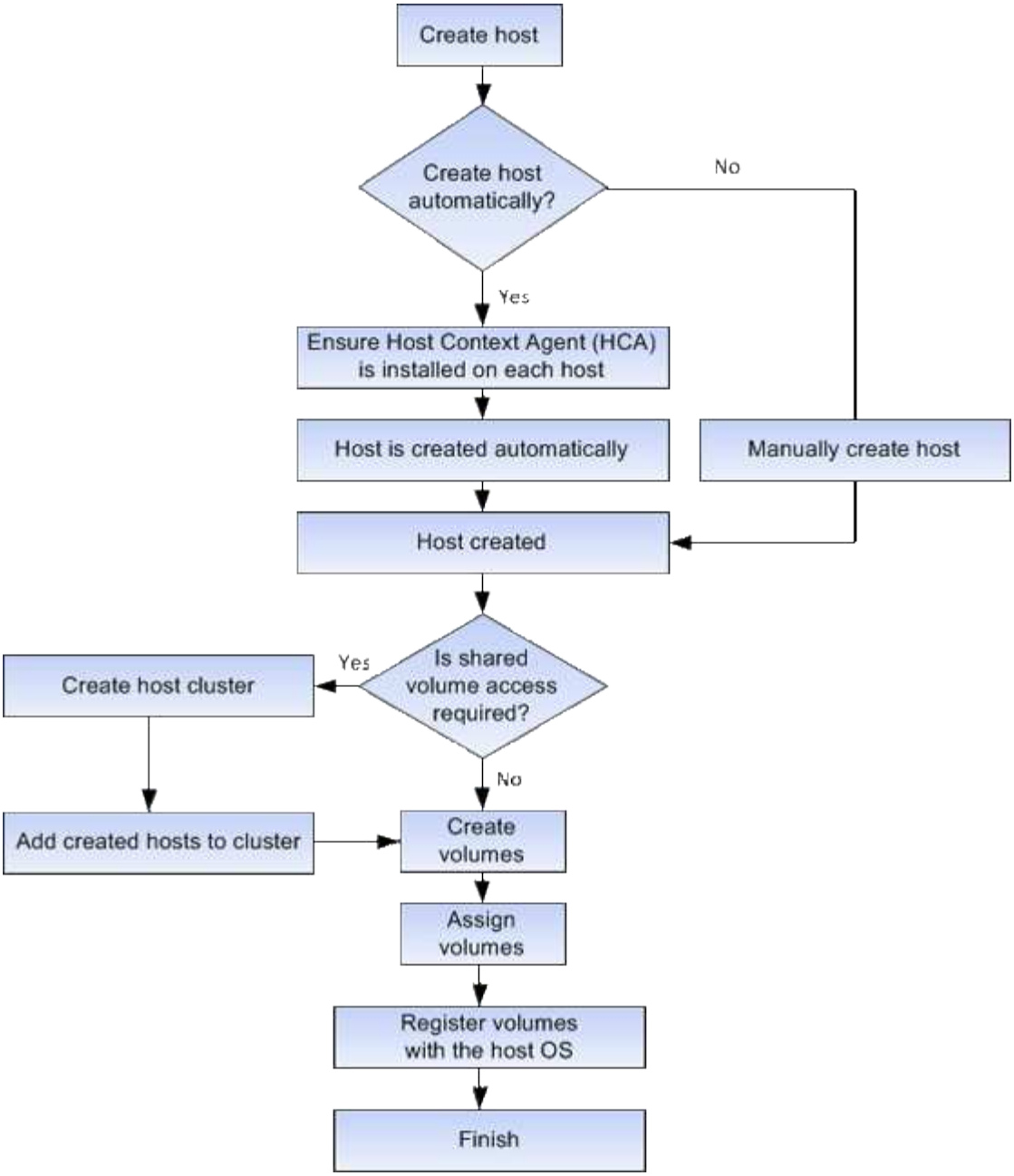
Aprenda sobre a terminologia de hosts no software SANtricity

Aprenda como os termos do host se aplicam ao seu array de storage.

Componente	Definição
Host	Um host é um servidor que envia I/O para um volume em um array de storage.
Nome do host	O nome do host deve ser igual ao nome do sistema do host.
Cluster de hosts	Um cluster de hosts é um grupo de hosts. Você cria um cluster de hosts para facilitar a atribuição dos mesmos volumes a vários hosts.
Protocolo de interface do host	Um protocolo de interface de host é a conexão (como Fibre Channel, iSCSI, etc.) entre os controladores e os hosts.
HBA ou Network Interface Card (NIC)	Um adaptador de barramento de host (HBA, na sigla em inglês) é uma placa que reside em um host e contém uma ou mais portas de host.
Porta do 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 I/O.
Identificador da porta do host	Um identificador de porta de host é um nome exclusivo mundial associado a cada porta de host em um adaptador de barramento de host (HBA). • Os identificadores de porta de host Internet Small Computer System Interface (iSCSI) devem ter entre 1 e 233 caracteres. Os identificadores de porta de host iSCSI são exibidos no formato IQN padrão (por exemplo, `iqn.xxx.com.xxx:8b3ad`). • Identificadores de porta de host não iSCSI, como Fibre Channel e Serial Attached SCSI (SAS), são exibidos separados por dois pontos a cada dois caracteres (por exemplo, `xx:yy:zz`). Identificadores de porta de host Fibre Channel devem ter 16 caracteres.
Tipo de sistema operacional do host	O tipo de sistema operacional do host é uma configuração que define como os controladores no array de storage reagem às operações de E/S, dependendo do sistema operacional (ou variante) do host. Isso também é chamado às vezes de *tipo de host*.
Porta do host do controlador	Uma porta de host do controlador é uma porta no controlador que fornece a conexão física com um host e é usada para operações de I/O.
LUN	Um número de unidade lógica (LUN, na sigla em inglês) é o número atribuído ao espaço de endereçamento que um host usa para acessar um volume. O volume é apresentado ao host como capacidade na forma de um LUN. Cada host possui seu próprio espaço de endereçamento LUN. Portanto, o mesmo LUN pode ser usado por diferentes hosts para acessar volumes diferentes.

Como funciona a criação de host e a atribuição de volumes no SANtricity System Manager

A figura a seguir ilustra como configurar o acesso ao host.



Saiba mais sobre a criação manual de hosts no SANtricity System Manager

A criação de um host é uma das etapas necessárias para que o array de storage saiba quais hosts estão conectados 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 hosts permite garantir que os identificadores de porta detectados pelos controladores do array de storage estejam associados corretamente aos hosts.

Durante a criação manual de hosts, você associa identificadores de porta do host selecionando-os em uma lista ou inserindo-os manualmente. Após criar um host, você pode atribuir volumes a ele ou adicioná-lo a um cluster de hosts se planejar compartilhar o acesso aos volumes.

Como os volumes são atribuídos a hosts e clusters de hosts no SANtricity software

Para que um host ou cluster de hosts envie E/S para um volume, você deve atribuir o volume ao host ou cluster de hosts.

Você pode selecionar um host ou cluster de hosts ao criar um volume ou pode atribuir um volume a um host ou cluster de hosts posteriormente. Um cluster de hosts é um grupo de hosts. Você cria um cluster de hosts para facilitar a atribuição dos mesmos volumes a vários hosts.

A atribuição de volumes aos hosts é flexível, permitindo atender às suas necessidades específicas de storage.

- **Host independente, não faz parte de um cluster de hosts** — Você pode atribuir um volume a um host individual. O volume só pode ser acessado apenas por esse host.
- **Cluster de hosts** — Você pode atribuir um volume a um cluster de hosts. O volume pode ser acessado por todos os hosts no cluster de hosts.
- **Host dentro de um cluster de hosts** — Você pode atribuir um volume a um host individual que faça parte de um cluster de hosts. Mesmo que o host faça parte de um cluster de hosts, o volume só poderá ser acessado por esse host individual e não por outros hosts no cluster de hosts.

Ao criar volumes, os números de unidades lógicas (LUNs) são atribuídos automaticamente. O LUN serve como "endereço" entre o host e o controlador durante as operações de I/O. Você pode alterar os LUNs após o volume ser criado.

Acesse volumes no SANtricity System Manager

Um volume de acesso é um volume configurado de fábrica no array de storage que é usado para comunicação com o array de storage e o host por meio da conexão de E/S do host. O volume de acesso requer um Logical Unit Number (LUN).

O volume de acesso é utilizado na seguinte instância:

- **Gerenciamento em banda** — O volume de acesso é usado para uma conexão em banda para gerenciar o array de storage. Isso só pode ser feito se você estiver gerenciando o array de storage com a interface de linha de comando (CLI).

> O gerenciamento em banda usando o volume de acesso não está disponível para os sistemas de storage E4000, EF600/EF600C ou EF300/EF300C.

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, você verá três volumes (Volume_1, Volume_2 e Access).

Se você não estiver criando hosts automaticamente ou gerenciando um array de storage em 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 ao LUN, bem como quaisquer conexões de gerenciamento em banda com o host.

Saiba mais sobre o número máximo de LUNs no SANtricity software

O array de storage possui um número máximo de logical unit numbers (LUNs) que podem ser usadas para cada host.

O número máximo depende do sistema operacional do host. O array de storage controla o número de LUNs em uso. Se você tentar atribuir um volume a um host que exceda o número máximo de LUNs, o host não poderá acessar o volume.

Saiba mais sobre o tipo padrão de sistema operacional host no software SANtricity

O tipo de host padrão é usado pelo array de storage quando os hosts são conectados inicialmente. Ele define como os controladores no array de storage trabalham com o sistema operacional do host quando os volumes são acessados.

Você pode alterar o tipo de host se houver necessidade de alterar como o array de storage opera em relação aos hosts que estão conectados a ele. Geralmente, você alterará o tipo de host padrão antes de conectar hosts ao array de storage ou quando conectar hosts adicionais.

Tenha estas orientações em mente:

- Se todos os hosts que você planeja conectar ao array de storage 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 conectar ao array de storage (ambiente de host heterogêneo), altere o tipo de host para corresponder à maioria dos sistemas operacionais dos hosts.

  Por exemplo, se você estiver conectando oito hosts diferentes ao array de storage e seis desses hosts estiverem executando um sistema operacional Windows, você deve selecionar Windows como o tipo de sistema operacional padrão do host.

- Se a maioria dos hosts conectados tiver uma combinação de sistemas operacionais diferentes, altere o tipo de host para Factory Default.

  Por exemplo, se você estiver conectando oito hosts diferentes ao array de storage, 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 deve selecionar Factory Default como o tipo de sistema operacional padrão do host.

Configurar acesso ao host

Crie um host manualmente no SANtricity System Manager

Para hosts que não podem ser descobertos automaticamente, você pode criar um host manualmente. Criar um host é uma das etapas necessárias para que o array de storage saiba quais hosts estão conectados a ele e para permitir o acesso de E/S aos volumes.

Sobre esta tarefa

Tenha estas diretrizes em mente ao criar um host:

- Você deve definir as portas de identificador do host que estão associadas ao host.
- Certifique-se de fornecer o mesmo nome que o nome de sistema atribuído ao host.
- Esta operação não terá sucesso se o nome que você escolher já estiver em uso.
- O comprimento do nome não pode exceder 30 caracteres.

Passos

1. Selecione o menu: storage [Hosts].
2. Clique no menu: criar [Host].

   A caixa de diálogo Create Host é exibida.

3. Selecione as configurações para o host conforme apropriado.

Detalhes do campo

Configuração	Descrição
Nome	Digite um nome para o novo host.
Tipo de sistema operacional do host	Selecione o sistema operacional que está sendo executado no novo host na lista suspensa.
Tipo de interface do host	(Opcional) Se você tiver mais de um tipo de interface de host suportada no seu array de storage, selecione o tipo de interface de host que deseja usar.
Portas do host	Faça uma das seguintes ações: • **Selecione a interface de I/O** Geralmente, as portas do host devem estar logadas e disponíveis na lista suspensa. Você pode selecionar os identificadores de porta do host na lista. • **Adição manual** Se o identificador de porta de um host não for exibido na lista, isso significa que a porta do host não fez login. Um utilitário HBA ou o utilitário iniciador iSCSI pode ser usado para encontrar os identificadores de porta do host e associá-los ao host. Você pode inserir manualmente os identificadores de porta do host ou copiá-los/colá-los do utilitário (um de cada vez) no campo **Portas do host**. Você deve selecionar um identificador de porta de host por vez para associá-lo ao host, mas pode continuar selecionando quantos identificadores estão associados ao host. Cada identificador é exibido no campo **Portas do host**. Se necessário, você também pode remover um identificador selecionando o **X** ao lado dele.

Configuração	Descrição
Iniciador CHAP	(Opcional) Se você selecionou ou inseriu manualmente uma porta de host com um iSCSI IQN e deseja exigir que um host que tente acessar o array de storage se autentique usando Challenge Handshake Authentication Protocol (CHAP), selecione a caixa de seleção **CHAP initiator**. Para cada porta de host iSCSI que você selecionou ou inseriu manualmente, faça o seguinte: • Insira o mesmo segredo CHAP que foi definido em cada iniciador iSCSI de host para autenticação CHAP. Se você estiver usando autenticação CHAP mútua (autenticação bidirecional que permite que um host se valide para o array de storage e que um array de storage se valide para o host), você também deve definir o segredo CHAP para o array de storage na configuração inicial ou alterando as configurações. • Deixe o campo em branco se você não precisar de autenticação do host. Atualmente, o único método de autenticação iSCSI usado pelo System Manager é CHAP.

4. Clique em **Create**.

Resultados

Após a criação bem-sucedida do host, o sistema cria um nome padrão para cada porta do host configurada para o host (rótulo do usuário).

O alias padrão é `<Hostname_Port Number>`. Por exemplo, o alias padrão para a primeira porta criada para `host IPT is IPT_1`.

Crie um cluster de hosts no SANtricity System Manager

Você cria um cluster de hosts quando dois ou mais hosts requerem acesso de E/S aos mesmos volumes.

Sobre esta tarefa

Tenha em mente estas diretrizes ao criar um cluster de hosts:

- Esta operação não é iniciada a menos que haja dois ou mais hosts disponíveis para criar o cluster.
- Hosts em clusters de hosts podem ter sistemas operacionais diferentes (heterogêneos).
- Hosts NVMe em clusters de hosts não podem ser misturados com hosts não NVMe.
- Para criar um volume com Data Assurance (DA) ativado, a conexão de host que você pretende usar deve ser compatível com DA.

  Se alguma das conexões de host nos controladores em seu array de storage não suportar DA, os hosts associados não poderão acessar dados em volumes com DA habilitado.

- Esta operação não terá sucesso se o nome que você escolher já estiver em uso.

- O comprimento do nome não pode exceder 30 caracteres.

Passos

1. Selecione o menu: storage [Hosts].
2. Selecione o menu: criar [Cluster de Hosts].

   A caixa de diálogo Criar Cluster de Hosts é exibida.

3. Selecione as configurações para o cluster de hosts conforme apropriado.

   Detalhes do campo

Configuração	Descrição
Nome	Digite o nome para o novo cluster de hosts.
Selecione os hosts para compartilhar o acesso ao volume	Selecione dois ou mais hosts na lista suspensa. Somente os hosts que ainda não fazem parte de um cluster de hosts aparecem na lista.

4. Clique em **Create**.

   Se os hosts selecionados estiverem conectados a tipos de interface que possuem diferentes capacidades de Data Assurance (DA), uma caixa de diálogo será exibida com a mensagem de que DA estará indisponível no cluster de hosts. Essa indisponibilidade impede que volumes com DA habilitado sejam adicionados ao cluster de hosts. Selecione **Sim** para continuar ou **Não** para cancelar.

   O DA aumenta a integridade de dados em todo o sistema de storage. O DA permite que o array de storage verifique erros que possam ocorrer quando os dados são movidos entre os hosts e as unidades. Usar o DA para o novo volume garante que quaisquer erros sejam detectados.

Resultados

O novo cluster de hosts aparece na tabela com os hosts atribuídos nas linhas abaixo.

Atribuir volumes aos hosts no SANtricity System Manager

Você deve atribuir um volume a um host ou a um cluster de hosts para que ele possa ser usado em operações de E/S. Essa atribuição concede a um host ou a um cluster de hosts acesso a um ou mais volumes em um array de storage.

Sobre esta tarefa

Tenha em mente estas diretrizes ao atribuir volumes aos hosts:

- Você pode atribuir um volume a apenas um host ou cluster de hosts por vez.
- Os volumes atribuídos são compartilhados entre os controladores no array de storage.
- O mesmo número de unidade lógica (LUN) não pode ser usado duas vezes por um host ou um cluster de hosts 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. Lembre-se de que, uma

vez que um volume associado ao grupo de volume seja mapeado, *todos* os volumes retornarão à inicialização mais lenta. Você pode verificar o progresso da inicialização em **Início › Operações em Andamento**.

A atribuição de um volume falha sob estas condições:

- Todos os volumes estão atribuídos.
- O volume já está atribuído a outro host ou cluster de hosts.

A possibilidade de atribuir um volume não está disponível nestas condições:

- Não existem hosts ou host clusters 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 Data Assurance (DA) aplicam-se da seguinte forma:

- Para um host compatível com DA, você pode selecionar volumes que estejam habilitados para DA ou que não estejam habilitados para DA.
- Para um host que não seja compatível com DA, se você selecionar um volume que esteja habilitado para DA, um aviso informa que o sistema deve desativar automaticamente o DA no volume antes de atribuir o volume ao host.

Passos

1. Selecione o menu: storage [Hosts].
2. Selecione o host ou cluster de hosts ao qual deseja atribuir volumes e clique em **Assign Volumes**.

   Uma caixa de diálogo é exibida 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. Selecione a caixa de seleção ao lado de cada volume que você deseja atribuir ou selecione a caixa de seleção no cabeçalho da tabela para selecionar todos os volumes.
4. Clique em **Assign** para concluir a operação.

Resultados

Após atribuir com sucesso um volume ou volumes a um host ou um cluster de hosts, o sistema executa as seguintes ações:

- O volume atribuído recebe o próximo número LUN disponível. O host usa o número LUN para acessar o volume.
- O nome do volume fornecido pelo usuário aparece nas listagens de volumes associadas ao host. Se aplicável, o volume de acesso configurado de fábrica também aparece nas listagens de volumes associadas ao host.

Gerenciar hosts e clusters

Alterar o tipo de host padrão no SANtricity System Manager

Use a configuração Alterar sistema operacional do host padrão para alterar o tipo de host

padrão no nível do array de storage. Geralmente, você alterará o tipo de host padrão antes de conectar hosts ao array de storage ou quando conectar hosts adicionais.

Sobre esta tarefa

Tenha estas orientações em mente:

- Se todos os hosts que você planeja conectar ao array de storage 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 conectar ao array de storage (ambiente de host heterogêneo), altere o tipo de host para corresponder à maioria dos sistemas operacionais dos hosts.

  Por exemplo, se você estiver conectando oito hosts diferentes ao array de storage e seis desses hosts estiverem executando um sistema operacional Windows, você deve selecionar Windows como o tipo de sistema operacional padrão do host.

- Se a maioria dos hosts conectados tiver uma combinação de sistemas operacionais diferentes, altere o tipo de host para Factory Default.

  Por exemplo, se você estiver conectando oito hosts diferentes ao array de storage, 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 deve selecionar Factory Default como o tipo de sistema operacional padrão do host.

Passos

1. Selecione o menu: configurações [Sistema].
2. Desça até **Configurações adicionais** e, em seguida, 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 **Change**.

Desatribuir volumes no SANtricity System Manager

Remova a atribuição de volumes dos hosts ou clusters de hosts se você não precisar mais de acesso de E/S a esse volume do host ou cluster de hosts.

Sobre esta tarefa

Tenha em mente estas orientações ao desatribuir um volume:

- Se você estiver removendo o último volume atribuído de um cluster de hosts e esse cluster também tiver hosts com volumes específicos atribuídos, certifique-se de remover ou mover essas atribuições antes de remover a última atribuição do cluster de hosts.
- Se um cluster de hosts, um host ou uma porta de host estiver atribuído a um volume que está registrado no sistema operacional, você deve limpar esse registro antes de poder remover esses nós.

Passos

1. Selecione o menu: storage [Hosts].
2. Selecione o host ou cluster de hosts que deseja editar e clique em **Unassign Volumes**.

   Uma caixa de diálogo aparece que mostra todos os volumes que estão atualmente atribuídos.

3. Selecione a caixa de seleção ao lado de cada volume que você deseja desatribuir ou selecione 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 será reconhecido pelo sistema operacional do host.

Excluir um host ou cluster de hosts no SANtricity System Manager

Você pode excluir um host ou host cluster.

Sobre esta tarefa

Mantenha estas diretrizes em mente ao excluir um host ou um cluster de hosts:

- Quaisquer atribuições de volume específicas são excluídas e os volumes associados estão disponíveis para uma nova atribuição.
- Se o host fizer parte de um cluster de hosts com suas próprias atribuições específicas, o cluster de hosts não será afetado. No entanto, se o host fizer parte de um cluster de hosts que não possui outras atribuições, o cluster de hosts e quaisquer outros hosts ou identificadores de porta de host associados herdam quaisquer atribuições padrão.
- Quaisquer identificadores de porta de host que estavam associados ao host tornam-se indefinidos.

Passos

1. Selecione o menu: storage [Hosts].
2. Selecione o host ou cluster de hosts que você deseja excluir e clique em **Excluir**.

   A caixa de diálogo de confirmação é exibida.

3. Confirme que deseja realizar a operação e clique em **Delete**.

Resultados

Se você excluiu um host, o sistema executa as seguintes ações:

- Exclui o host e, se aplicável, remove-o do cluster de hosts.
- Remove o acesso a quaisquer volumes atribuídos.
- Retorna os volumes associados para um estado não atribuído.
- Retorna quaisquer identificadores de porta do host associados ao host para um estado não associado.

Se você excluiu um cluster de hosts, o sistema executa as seguintes ações:

- Exclui o cluster de hosts e seus hosts associados (se houver).
- Remove o acesso a quaisquer volumes atribuídos.
- Retorna os volumes associados para um estado não atribuído.
- Retorna quaisquer identificadores de porta de host associados aos hosts para um estado não associado.

Defina o relatório de conectividade de host no SANtricity System Manager

Você pode habilitar o relatório de conectividade de host para que o array de storage monitore continuamente a conexão entre os controladores e os hosts configurados e, em seguida, alerte você caso a conexão seja interrompida. Esse recurso está habilitado por padrão.

Sobre esta tarefa

Se você desativar o relatório de conectividade de host, o sistema deixará de monitorar problemas de conectividade ou de driver multipath com um host conectado ao array de storage.

> Desativar o relatório de conectividade de host também desativa o balanceamento de carga automático, que monitora e equilibra a utilização de recursos do controlador.

Passos

1. Selecione o menu: configurações [Sistema].
2. Desça até **Configurações adicionais** e clique em **Ativar/desativar relatório de conectividade de host**.

   O texto abaixo desta opção indica se ela está atualmente habilitada ou desabilitada.

   Uma caixa de diálogo de confirmação é aberta.

3. Clique em **Yes** para continuar.

   Ao selecionar esta opção, você alterna o recurso entre ativado/desativado.

Gerenciar configurações

Altere as configurações de um host no SANtricity System Manager

Você pode alterar o nome, o tipo de sistema operacional do host e os clusters de hosts associados a um host.

Passos

1. Selecione o menu: storage [Hosts].
2. Selecione o host que você deseja editar e clique em **View/Edit Settings**.

   Uma caixa de diálogo aparece que mostra as configurações atuais do host.

3. Se ainda não estiver selecionado, clique na guia **Propriedades**.
4. Altere as configurações conforme necessário.

Detalhes do campo

Configuração	Descrição
Nome	Você pode alterar o nome do host fornecido pelo usuário. É obrigatório especificar um nome para o host.
Cluster de hosts associado	Você pode escolher uma das seguintes opções: • **Nenhum** — O host permanece um host independente. Se o host estava associado a um cluster de hosts, o sistema remove o host do cluster. • **<Host Cluster>** — O sistema associa o host ao cluster selecionado.
Tipo de sistema operacional do 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 hosts no SANtricity System Manager

Você pode alterar o nome do cluster de hosts, ou adicionar ou remover hosts em um cluster de hosts.

Passos

1. Selecione o menu: storage [Hosts].
2. Selecione o cluster de hosts que deseja editar e clique em **View/Edit Settings**.

   Uma caixa de diálogo aparece que mostra as configurações atuais do cluster de hosts.

3. Altere as configurações do cluster de hosts conforme apropriado.

Detalhes do campo

Configuração	Descrição
Nome	Você pode especificar o nome do cluster de hosts fornecido pelo usuário. É obrigatório especificar um nome para o cluster.
Anfitriões associados	Para adicionar um host, clique na caixa **Associated Hosts** e selecione um nome de host na lista suspensa. Você não pode inserir um nome de host manualmente. Para excluir um host, clique no **X** ao lado do nome do host.

4. Clique em **Salvar**.

Altere os identificadores de porta do host para um host no SANtricity System Manager

Altere os identificadores de porta do host quando desejar alterar o rótulo do 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.

Sobre esta tarefa

Ao alterar os identificadores de porta do host, tenha em mente as seguintes diretrizes:

- **Adicionar** — Ao adicionar uma porta de host, você está associando o identificador da porta de host ao host que você criou para se conectar ao seu array de storage. Você pode inserir manualmente as informações da porta usando um utilitário de adaptador de barramento de host (HBA).
- **Editar** — Você pode editar as portas do host para mover (associar) uma porta do host a um host diferente. Você pode ter movido o adaptador de barramento do host ou iniciador iSCSI para um host diferente, então deve mover (associar) a porta do host ao novo host.
- **Excluir** — você pode excluir portas de host para remover (desassociar) portas de host de um host.

Passos

1. Selecione o menu: storage [Hosts].
2. Selecione o host ao qual as portas serão associadas e clique em **View/Edit Settings**.

   Se você deseja adicionar portas a um host em um cluster de hosts, expanda o cluster de hosts e selecione o host desejado. Não é possível adicionar portas no nível do cluster de hosts.

   Uma caixa de diálogo aparece que mostra as configurações atuais do host.

3. Clique na guia **Host Ports**.

   A caixa de diálogo exibe os identificadores de porta do host atual.

4. Altere as configurações do identificador da porta do host conforme apropriado.

Configuração	Descrição
Porta do host	Você pode escolher uma das seguintes opções: • **Adicionar** — Use Adicionar para associar um novo identificador de porta do host ao host. O comprimento do nome do identificador de porta do host é determinado pela tecnologia da interface do host. Os nomes de identificador de porta do host Fibre Channel e Infiniband devem ter 16 caracteres. Os nomes de identificador de porta do host iSCSI têm um máximo de 223 caracteres. A porta deve ser única. Um número de porta que já tenha sido configurado não é permitido. • **Excluir** — Use Excluir para remover (desassociar) um identificador de porta de host. A opção Excluir não remove fisicamente a porta do host. Esta 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. Se você excluir um identificador de porta de host, ele deixará de estar associado a esse host. Além disso, o host perderá o acesso a qualquer um dos volumes atribuídos a ele por meio desse identificador de porta de host.
Rótulo	Para alterar o nome da etiqueta da porta, clique no ícone **Editar** (lápis). O nome da etiqueta da porta deve ser único. Um nome de etiqueta que já tenha sido configurado não é permitido.
Segredo CHAP	Aparece apenas para hosts iSCSI. Você pode definir ou alterar o segredo CHAP para os iniciadores (hosts iSCSI). System Manager usa o método Challenge Handshake Authentication Protocol (CHAP), que valida a identidade dos targets e iniciadores durante o link inicial. A autenticação é baseada em uma chave de segurança compartilhada chamada segredo CHAP.

5. Clique em **Salvar**.

Perguntas frequentes sobre sistemas host e clusters de hosts para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

O que são hosts e clusters de hosts?

Um host é um servidor que envia E/S para um volume em um array de storage. Um cluster de hosts é um grupo de hosts. Você cria um cluster de hosts para facilitar a atribuição dos mesmos volumes a vários hosts.

Você define um host separadamente. Ele pode ser uma entidade independente ou ser adicionado a um cluster de hosts. Você pode atribuir volumes a um host individual, ou um host pode fazer parte de um cluster de hosts que compartilha o acesso a um ou mais volumes com outros hosts no cluster de hosts.

O cluster de hosts é uma entidade lógica que você cria no SANtricity System Manager. Você precisa adicionar hosts ao cluster de hosts antes de poder atribuir volumes.

Por que eu precisaria criar um cluster de host?

Você precisa criar um cluster de hosts se quiser que dois ou mais hosts compartilhem o acesso ao mesmo conjunto de volumes. Normalmente, os hosts individuais têm software de clustering instalado para coordenar o acesso aos volumes.

Como posso saber qual tipo de sistema operacional do host é o correto?

O campo Tipo de Sistema Operacional do Host contém o sistema operacional do host. Você pode selecionar o tipo de host recomendado na lista suspensa.

Os tipos de host que aparecem na lista suspensa dependem do modelo do array de storage e da versão do firmware. As versões mais recentes exibem primeiro as opções mais comuns, que são as mais propensas a serem adequadas. A presença nesta lista não implica que a opção seja totalmente compatível.

Para obter mais informações sobre suporte de host, consulte o "NetApp Ferramenta de Matriz de Interoperabilidade".

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)	Compatível com sistemas operacionais Linux que utilizam uma solução de failover multipath Device Mapper com kernel 3.10 ou posterior.
VMware ESXi	Compatível com sistemas operacionais VMware ESXi que executam a arquitetura Native Multipathing Plug-in (NMP) usando o módulo incorporado Storage Array Type Policy da VMware, SATP_ALUA.
Windows (clustered ou non-clustered)	Compatível com configurações do Windows em cluster ou não em cluster que não estão executando o driver de multipath ATTO.
ATTO Cluster (todos os sistemas operacionais)	Compatível com todas as configurações de cluster usando o driver de multipath da ATTO Technology, Inc.
Linux (Veritas DMP)	Compatível com sistemas operacionais Linux usando uma solução de multipath Veritas DMP.
Linux (ATTO)	Compatível com sistemas operacionais Linux usando um driver de multipath da ATTO Technology, Inc.
Mac OS (ATTO)	Compatível com versões do Mac OS que utilizam um driver de multipath da ATTO Technology, Inc.

Tipo de sistema operacional do host	Sistema operacional (SO) e driver multipath
Windows (ATTO)	Compatível com sistemas operacionais Windows usando um driver de multipathing da ATTO Technology, Inc.
IBM SVC	Suporta uma configuração IBM SAN Volume Controller.
Padrão de fábrica	Reservado para a inicialização do array de storage. Se o tipo de sistema operacional do seu host estiver definido como Factory Default, altere-o para corresponder ao sistema operacional do host e ao driver multipath em execução no host conectado.
Linux DM-MP (Kernel 3.9 ou anterior)	Compatível com sistemas operacionais Linux que utilizam uma solução de failover multipath Device Mapper com kernel 3.9 ou anterior.
Clustered Window (obsoleto)	Se o tipo de sistema operacional do seu host estiver definido com esse valor, use a configuração do Windows (clustered ou non-clustered).

O que são HBAs e portas de adaptador?

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 I/O.

As portas do adaptador no HBA são chamadas de portas de host. A maioria dos HBAs possui uma ou duas portas de host. O HBA possui um World Wide Identifier (WWID) exclusivo, e cada porta de host do HBA possui um WWID exclusivo. Os identificadores de porta de host são usados para associar o HBA apropriado ao host físico quando você cria manualmente o host por meio do SANtricity System Manager.

Como faço para associar as portas do host a um host?

Se você estiver criando um host manualmente, primeiro deve usar o utilitário de adaptador de barramento de host (HBA) apropriado disponível no host para determinar os identificadores de porta do host associados a cada HBA instalado no host.

Quando você tiver essas informações, selecione os identificadores de porta do host que fizeram login no array de storage 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 de host incorretos, poderá causar acesso não intencional a esses dados a partir de outro host.

Como faço para criar segredos CHAP?

Se você configurar a autenticação Challenge Handshake Authentication Protocol (CHAP) em qualquer host iSCSI conectado ao array de storage, você deverá inserir novamente o segredo CHAP do iniciador para cada host iSCSI.

Para isso, você pode usar System Manager como parte da operação Criar Host ou através da opção Exibir/Editar Configurações.

Se você estiver usando autenticação mútua CHAP, também deve definir um segredo CHAP de destino para o array de storage na página Configurações e inserir 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 login no array de storage acesse os 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 está fisicamente instalada em um host e fez login no array de storage.

> Se você deseja que os hosts tenham acesso específico a determinados volumes no array de storage, você *não* deve usar o cluster padrão. Em vez disso, você deve associar os identificadores de porta do host aos seus respectivos hosts. Essa tarefa pode ser feita manualmente durante a operação Criar Host. Em seguida, você atribui os volumes a um host individual ou a um cluster de hosts.

Você deve usar o cluster padrão *somente* em situações especiais onde seu ambiente de storage externo seja propício para permitir que todos os hosts e todos os identificadores de porta de host conectados ao array de storage tenham acesso a todos os volumes (modo de acesso total) sem precisar informar especificamente os hosts ao array de storage ou à interface de usuário.

Inicialmente, você só pode atribuir volumes 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 Default Cluster) é exibida na interface de usuário, onde você pode então gerenciar essa entidade.

O que é o relatório de conectividade de host?

Quando o relatório de conectividade de host está ativado, o array de storage monitora continuamente a conexão entre os controladores e os hosts configurados e, em seguida, alerta você se a conexão for interrompida.

A conexão pode ser interrompida se houver um cabo solto, danificado ou ausente, ou outro problema com o host. Nessas situações, o sistema pode exibir uma mensagem do Recovery Guru:

- **Perda de redundância do host** — Abre se qualquer um dos controladores não conseguir se comunicar com o host.
- **Tipo de host incorreto** — Abre se o tipo do host estiver especificado incorretamente no array de storage, o que pode resultar em problemas de failover.

Você pode querer desativar o relatório de conectividade de host em situações em que a reinicialização de um controlador possa demorar mais do que o tempo limite da conexão. Desativar esse recurso suprime as mensagens do Recovery Gurus.

> Desativar o relatório de conectividade de host também desativa o balanceamento de carga automático, que monitora e equilibra o uso de recursos do controlador. No entanto, se você reativar o relatório de conectividade de host, o recurso de balanceamento de carga automático não será reativado automaticamente.

Instantâneos

Saiba mais sobre snapshots no SANtricity System Manager

O recurso Snapshot permite criar imagens de ponto no tempo dos volumes do array de storage para uso em backup ou testes.

O que são imagens de Snapshot?

Uma *imagem de snapshot* é uma cópia lógica dos dados do volume, capturada em um determinado ponto no tempo. Semelhante a um ponto de restauração, as imagens de snapshot permitem reverter para um conjunto de dados conhecido. Embora o host possa acessar a imagem de snapshot, ele não pode ler ou gravar diretamente nela.

Saiba mais:

- "Como funciona o armazenamento de Snapshot"
- "Terminologia de Snapshot"
- "Volumes base, capacidade reservada e grupos de Snapshot"
- "Agendamentos de Snapshot e grupos de consistência"
- "Volumes de Snapshot"

Como faço para criar Snapshots?

Você pode criar manualmente uma imagem de snapshot a partir de um volume base ou de um grupo de consistência de snapshot. Esse procedimento está disponível em **Storage › Snapshots**.

Saiba mais:

- "Requisitos e diretrizes para Snapshots"
- "Fluxo de trabalho para criação de imagens e volumes Snapshot"
- "Criar uma imagem de Snapshot"
- "Agendar imagens de Snapshot"
- "Crie um grupo de consistência de Snapshot"
- "Criar um volume de Snapshot"

Como faço para reverter dados de um Snapshot?

Um *rollback* é o processo de retornar os dados de um volume base para um ponto anterior no tempo. Você pode reverter os dados do Snapshot em **Storage › Snapshots**.

Saiba mais:

- "Reverter Snapshot"
- "Inicie um reverter de imagem de Snapshot para um volume base"
- "Inicie um reverter de imagem de snapshot 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 snapshots"

Conceitos

Como funciona o armazenamento de Snapshot no SANtricity software

O recurso Snapshot utiliza a tecnologia copy-on-write para armazenar imagens de Snapshot e usar a capacidade reservada alocada.

Como as imagens Snapshot são usadas

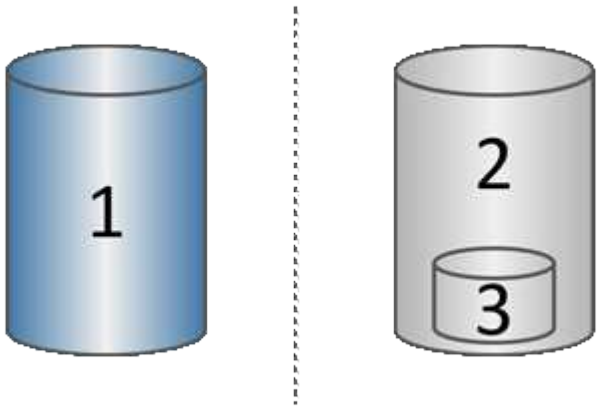
Uma imagem Snapshot é uma cópia lógica, somente leitura do conteúdo do volume, capturada em um ponto no tempo. Você pode usar Snapshots para proteger contra perda de dados.

As imagens de Snapshot também são úteis para ambientes de teste. Ao criar uma cópia virtual dos dados, você pode testar os dados usando o Snapshot sem alterar o volume real. Além disso, os hosts não têm permissão de gravação nas imagens de Snapshot, portanto, seus Snapshots são sempre um recurso de backup seguro.

Criação de Snapshot

À medida que os Snapshots são criados, o recurso Snapshots armazena os dados da imagem da seguinte forma:

- Quando uma imagem de snapshot é criada, ela corresponde exatamente ao volume base. O recurso de Snapshots utiliza tecnologia copy-on-write. Após a criação do snapshot, 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 da gravação dos novos dados no volume base.
- Os snapshots subsequentes incluem apenas os blocos de dados alterados. Antes que os dados sejam sobrescritos no volume base, o recurso Snapshots utiliza sua tecnologia copy-on-write para salvar as imagens necessárias dos setores afetados na capacidade reservada para snapshots.



[1] Volume base (capacidade física do disco); [2] Snapshots (capacidade lógica do disco); [3] Capacidade reservada (capacidade física do disco)

- A capacidade reservada armazena os blocos de dados originais de partes do volume base que foram alteradas após o snapshot ser feito e inclui um índice para rastrear as alterações. Geralmente, o tamanho da capacidade reservada é definido como 40 por cento do volume base. (Se precisar de mais capacidade reservada, você pode aumentar a capacidade reservada.)
- As imagens de Snapshot são armazenadas em uma ordem específica, com base em seu carimbo de data/hora. Somente a imagem de Snapshot mais antiga de um volume base está disponível para exclusão manual.

Restauração de Snapshot

Para restaurar dados para um volume base, você pode usar um volume Snapshot ou uma imagem Snapshot:

- **Snapshot volume** — Se precisar recuperar arquivos excluídos, crie um snapshot volume a partir de uma imagem de snapshot válida e, em seguida, atribua-o ao host.
- **Snapshot image** — Se você precisar restaurar um volume base para um ponto no tempo, use uma imagem de Snapshot anterior para reverter os dados para o volume base.

Aprenda sobre a terminologia de Snapshot no software SANtricity

Saiba como os termos de Snapshot se aplicam ao seu array de storage.

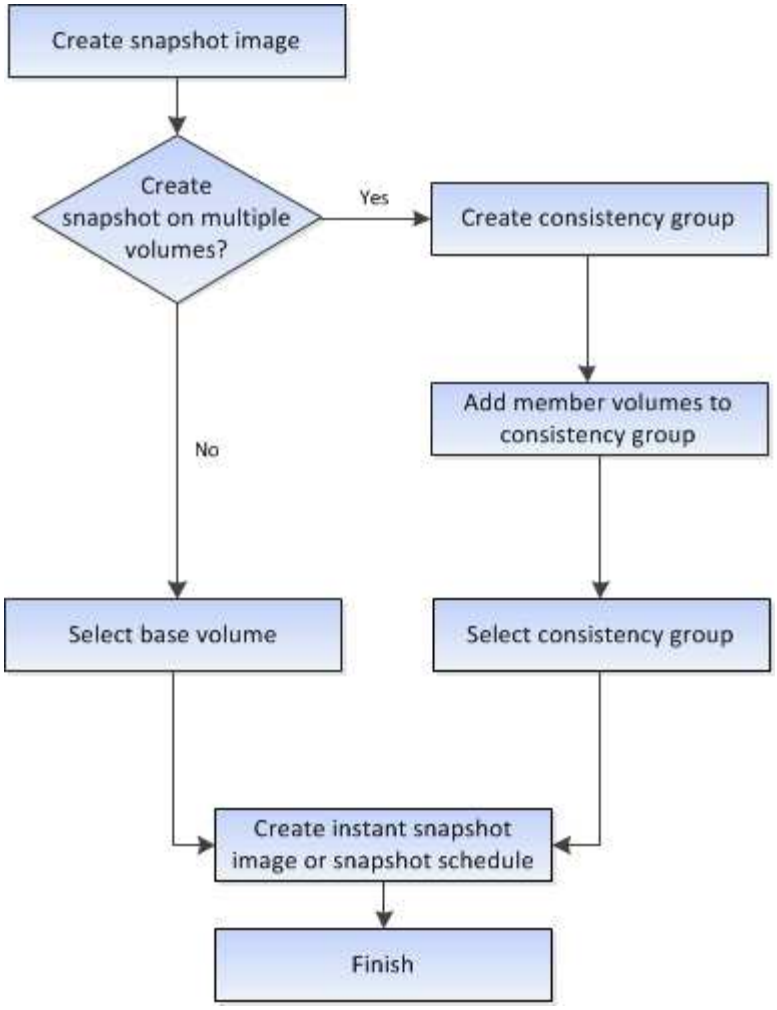
Termo	Descrição
Recurso de Snapshots	O recurso Snapshot é usado para criar e gerenciar imagens de volumes.
Snapshot imagem instantânea	Uma imagem de snapshot é uma cópia lógica dos dados do volume, capturada em um determinado ponto no tempo. Assim como um ponto de restauração, as imagens de snapshot permitem reverter para um conjunto de dados conhecido e bom. Embora o host possa acessar a imagem de snapshot, ele não pode ler ou gravar diretamente nela.
Volume base	Um volume base é a origem a partir da qual uma imagem de Snapshot é criada. Pode ser um volume espesso ou fino e geralmente é atribuído a um host. O volume base pode residir em um grupo de volume ou em um pool de discos.
Volume de Snapshot	Um volume de snapshot permite que o host acesse dados na imagem do snapshot. O volume de snapshot contém sua própria capacidade reservada, que salva quaisquer modificações no volume base sem afetar a imagem original do snapshot.
Grupo de Snapshot	Um grupo de Snapshot é uma coleção de imagens de Snapshot 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 cronograma de Snapshot é uma tabela para criar imagens de Snapshot automatizadas. Por meio do cronograma, você pode controlar a frequência das criações de imagens.

Termo	Descrição
Grupo de consistência Snapshot	Um grupo de consistência de snapshot é uma coleção de volumes que são tratados como uma única entidade quando uma imagem de snapshot é criada. Cada um desses volumes possui sua própria imagem de snapshot, mas todas as imagens são criadas no mesmo ponto no tempo.
Volume membro do grupo de consistência de Snapshot	Cada volume que pertence a um grupo de consistência de Snapshot é chamado de volume membro. Quando você adiciona um volume a um grupo de consistência de Snapshot, System Manager cria automaticamente um novo grupo de Snapshot correspondente a esse volume membro.
Reverter	Um rollback é o processo de retornar os dados de um volume base para um ponto anterior no tempo.
Capacidade reservada	A capacidade reservada é a capacidade física alocada que é usada para qualquer operação de serviço de cópia e objeto de armazenamento. Ela não é diretamente legível pelo host.

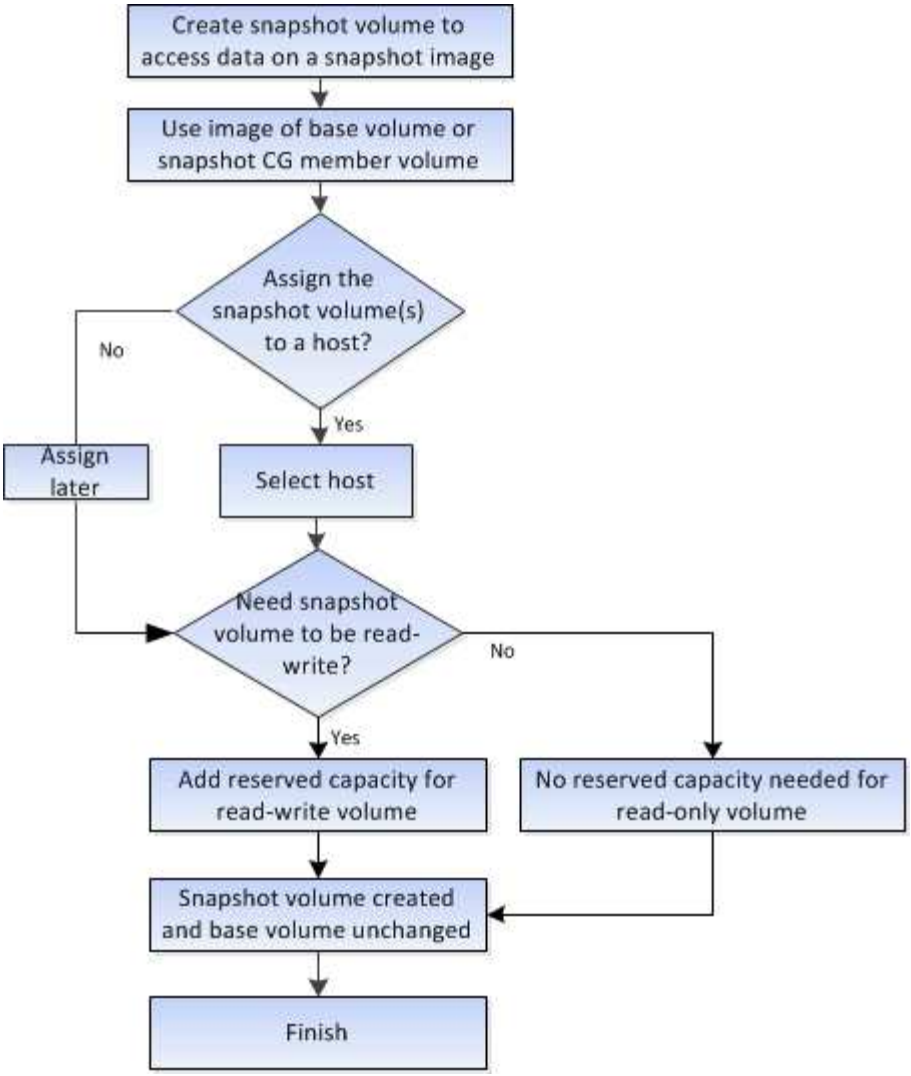
Como funciona a criação de imagens de snapshot e volumes de snapshot no SANtricity System Manager

No SANtricity System Manager, você pode criar imagens Snapshot e volumes Snapshot seguindo estes passos.

Fluxo de trabalho para criação de imagens Snapshot



Fluxo de trabalho para criação de volumes de Snapshot



Requisitos e diretrizes para Snapshots no SANtricity System Manager

Ao criar e usar Snapshots, revise os seguintes requisitos e diretrizes.

Snapshot imagens instantâneas e grupos de instantâneos

- Cada imagem de Snapshot está associada a exatamente um grupo de Snapshot.
- Um grupo de Snapshot é criado na primeira vez que você cria uma imagem de Snapshot agendada ou instantânea para um objeto associado. Isso cria capacidade reservada.

  Você pode visualizar os grupos de Snapshot na página Pools & Volume Groups.

- Imagens de Snapshot agendadas não ocorrem quando o array de storage está offline ou desligado.
- Se você excluir um grupo de Snapshot que possui um agendamento de Snapshot, o agendamento de Snapshot também será excluído.
- Se você tiver um volume de Snapshot que não precisa mais, pode reutilizá-lo, juntamente com qualquer capacidade reservada associada, em vez de excluí-lo. Isso cria um volume de Snapshot diferente do mesmo volume base. Você pode reassociar o volume de Snapshot ou o volume de Snapshot do grupo de consistência à mesma imagem de Snapshot ou a uma imagem de Snapshot diferente, desde que a imagem de Snapshot esteja no mesmo volume base.

Grupo de consistência 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 um agendamento.
- Se você excluir um grupo de consistência de Snapshot que tenha um agendamento de Snapshot, o agendamento de Snapshot também será excluído.
- Não é possível gerenciar individualmente um grupo de Snapshot que está associado a um grupo de consistência de Snapshot. Em vez disso, você deve executar as operações de gerenciamento (criar imagem de Snapshot, excluir imagem de Snapshot ou grupo de Snapshot e reverter imagem de Snapshot) no nível do grupo de consistência de Snapshot.

Volume base

- Um volume de Snapshot deve ter as mesmas configurações de Data Assurance (DA) e segurança que o volume base associado.
- Não é possível criar um volume de Snapshot de um volume base com falha.
- Se o volume base residir em um grupo de volume, os volumes membros de qualquer grupo de consistência de Snapshot associado podem residir em um pool ou em um grupo de volume.
- Se um volume base reside em um pool, todos os volumes membros de qualquer grupo de consistência de Snapshot associado devem residir no mesmo pool que o volume base.

Capacidade reservada

- A capacidade reservada está associada a apenas um volume base.
- O uso de um agendamento pode resultar em um grande número de imagens de Snapshot. Certifique-se de ter capacidade reservada suficiente para os Snapshots agendados.
- O volume de capacidade reservada para um grupo de consistência de Snapshot deve ter as mesmas configurações de Data Assurance (DA) e segurança que o volume base associado ao volume membro do grupo de consistência de Snapshot.

Imagens Snapshot pendentes

A criação de Snapshot pode permanecer no estado Pendente nas seguintes condições:

- O volume base que contém esta imagem de Snapshot é membro de um grupo de espelhamento assíncrono.
- O volume base está atualmente em uma operação de sincronização. A criação da imagem Snapshot é concluída assim que a operação de sincronização é concluída.

Número máximo de imagens Snapshot

- Se um volume for membro de um grupo de consistência de Snapshot, System Manager cria um grupo de Snapshot para esse volume membro. Esse grupo de Snapshot é contabilizado no número máximo permitido de grupos de Snapshot por volume base.
- Se você tentar criar uma Snapshot em um grupo de Snapshot ou grupo de consistência de Snapshot, mas o grupo associado tiver atingido o número máximo de Snapshots, você tem duas opções:
  - Ative a exclusão automática para o grupo de Snapshot ou grupo de consistência de Snapshot.
  - Exclua manualmente uma ou mais imagens de Snapshot do grupo de Snapshot ou grupo de consistência de Snapshot e tente a operação novamente.

Exclusão automática

Se o grupo de Snapshot ou grupo de consistência de Snapshot estiver habilitado para exclusão automática, System Manager exclui a imagem de Snapshot mais antiga quando o sistema cria uma nova para o grupo.

Operação de reverter

- Não é possível executar as seguintes ações enquanto uma operação de reverter estiver em andamento:
  - Exclua a imagem Snapshot que está sendo usada para o rollback.
  - Crie uma nova imagem de Snapshot para um volume base que está participando de uma operação de reverter.
  - Altere a política Repository-Full do grupo de Snapshot associado.
- Não é possível iniciar uma operação de reverter enquanto qualquer uma destas operações estiver em andamento:
  - Expansão de capacidade (adicionar capacidade a um pool ou grupo de volume)
  - Expansão de volume (aumentar a capacidade de um volume)
  - Alteração do nível RAID para um grupo de volume
  - Alteração do tamanho do segmento para um volume
- Não é possível iniciar uma operação de reverter se o volume base estiver participando de uma cópia de volume.
- Não é possível iniciar uma operação de reverter se o volume base for um volume secundário em um espelho remoto.
- Uma operação de reverter falha se qualquer parte da capacidade utilizada no volume de repositório de Snapshot associado tiver setores ilegíveis.

Saiba mais sobre volumes base, capacidade reservada e grupos de Snapshot no SANtricity System Manager

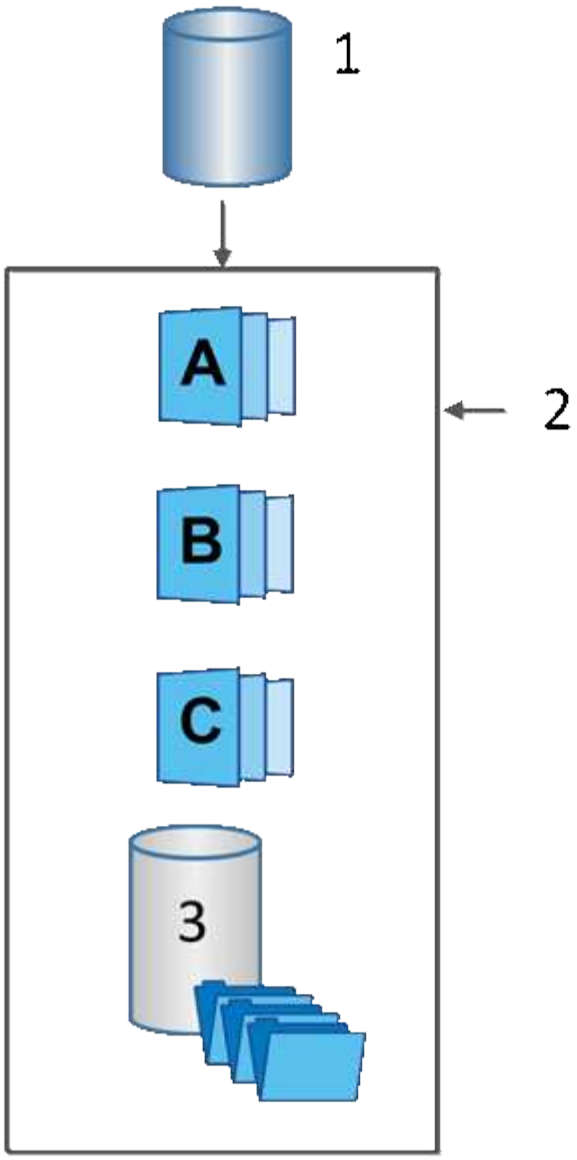
O recurso de Snapshots utiliza volumes base, capacidade reservada e grupos de Snapshot.

Volumes de base

Um *volume base* é o volume usado como fonte para uma imagem de snapshot. Um volume base pode ser um volume espesso ou um volume fino e pode residir em um pool ou grupo de volume.

Para tirar snapshots do volume base, você pode criar uma imagem instantânea a qualquer momento ou pode automatizar o processo definindo uma programação regular para snapshots.

A figura a seguir mostra a relação entre os objetos de snapshot e o volume base.



[1] Volume base; [2] Objetos de Snapshot no grupo (imagens e capacidade reservada); [3] Capacidade reservada para o grupo de Snapshot.

Capacidade reservada e grupos de snapshot

System Manager organiza as imagens de snapshot em *snapshot groups*. Quando System Manager estabelece o snapshot group, ele automaticamente cria a *reserved capacity* associada para armazenar as imagens de snapshot do grupo e para acompanhar as alterações subsequentes em snapshots adicionais.

Se o volume base estiver em um grupo de volume, a capacidade reservada pode estar localizada em um pool ou grupo de volume. Se o volume base estiver em um pool, a capacidade reservada deve estar localizada no mesmo pool que o volume base.

Snapshot groups não exigem nenhuma ação do usuário, mas você pode ajustar a capacidade reservada em um snapshot group a qualquer momento. Além disso, você pode ser solicitado a criar capacidade reservada quando as seguintes condições forem atendidas:

- Sempre que você cria um snapshot de um volume base que ainda não possui um grupo de snapshot,

System Manager cria automaticamente um grupo de snapshot. Essa ação também cria capacidade reservada para o volume base que é usada para armazenar as imagens de snapshot subsequentes.

- Sempre que você cria um agendamento de snapshot para um volume base, System Manager cria automaticamente um grupo de snapshot.

Exclusão automática

Ao trabalhar com snapshots, utilize a opção padrão para que a exclusão automática esteja ativada. A exclusão automática remove automaticamente a imagem de snapshot mais antiga quando o grupo de snapshots atinge o limite do grupo de snapshots de 32 imagens. Se você desativar a exclusão automática, então os limites do grupo de snapshots serão eventualmente excedidos e você precisará realizar ações manuais para configurar as configurações do grupo de snapshots e gerenciar a capacidade reservada.

Saiba mais sobre agendamento do Snapshot e grupo de consistência no SANtricity System Manager

Utilize agendamentos para a coleta de imagens de Snapshot e grupos de consistência de Snapshot para gerenciar múltiplos volumes base.

Para gerenciar facilmente as operações de Snapshot para volumes base, você pode usar os seguintes recursos:

- **Snapshot schedule** — Automatize snapshots para um único volume base.
- **Grupo de consistência do Snapshot** — Gerencie vários volumes base como uma única entidade.

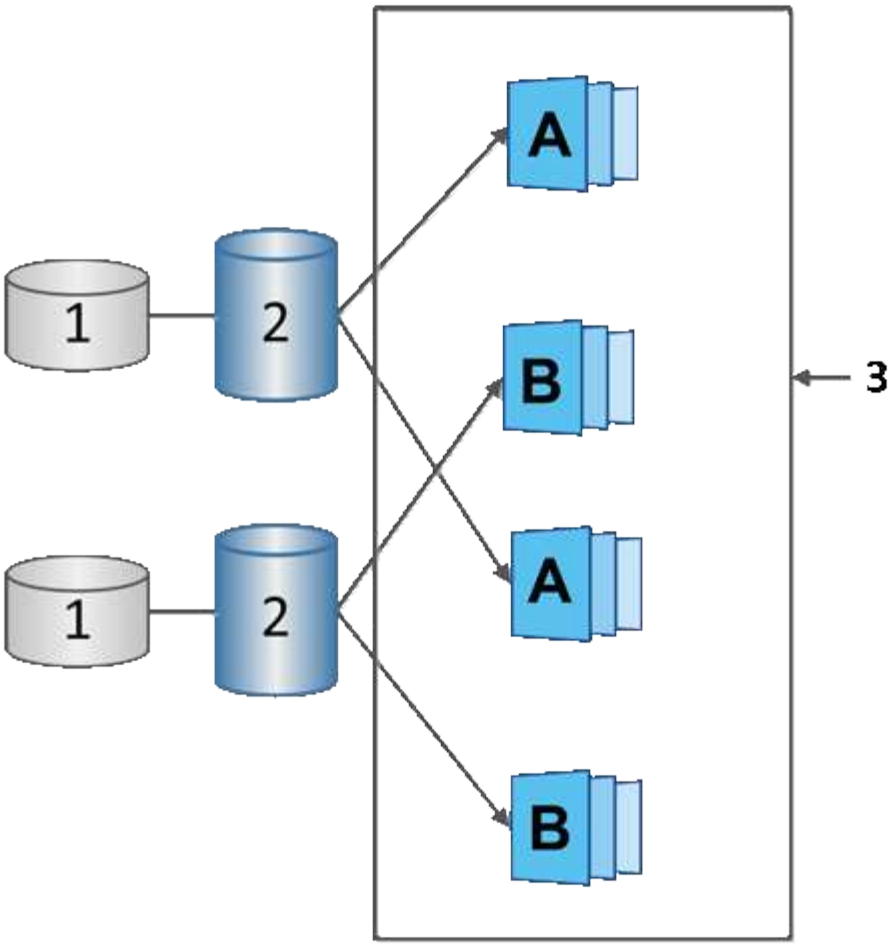
Agendamento do Snapshot

Se você deseja tirar snapshots automaticamente para um volume base, pode criar um agendamento. Por exemplo, você pode definir um agendamento que tira imagens de snapshot todo sábado à meia-noite, no primeiro dia de cada mês ou em quaisquer datas e horários que você decidir. Após o máximo de 32 snapshots ser atingido para um único agendamento, você pode suspender os snapshots agendados, criar mais capacidade reservada ou excluir snapshots. Os snapshots podem ser excluídos manualmente ou automatizando o processo de exclusão. Após uma imagem de snapshot ser excluída, capacidade reservada adicional fica disponível para reutilização.

Grupo de consistência Snapshot

Você cria um grupo de consistência de snapshot quando deseja garantir que as imagens de snapshot sejam criadas em vários volumes ao mesmo tempo. As ações de imagem de snapshot são executadas no grupo de consistência de snapshot como um todo. Por exemplo, você pode agendar snapshots sincronizados de todos os volumes com o mesmo timestamp. Grupos de consistência de snapshot são ideais para aplicativos que abrangem vários volumes, como aplicativos de banco de dados que armazenam logs 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 membros. Quando você adiciona um volume a um grupo de consistência, o System Manager cria automaticamente uma nova capacidade reservada correspondente a esse volume membro. Você pode definir um agendamento para criar automaticamente uma imagem de snapshot de cada volume membro.



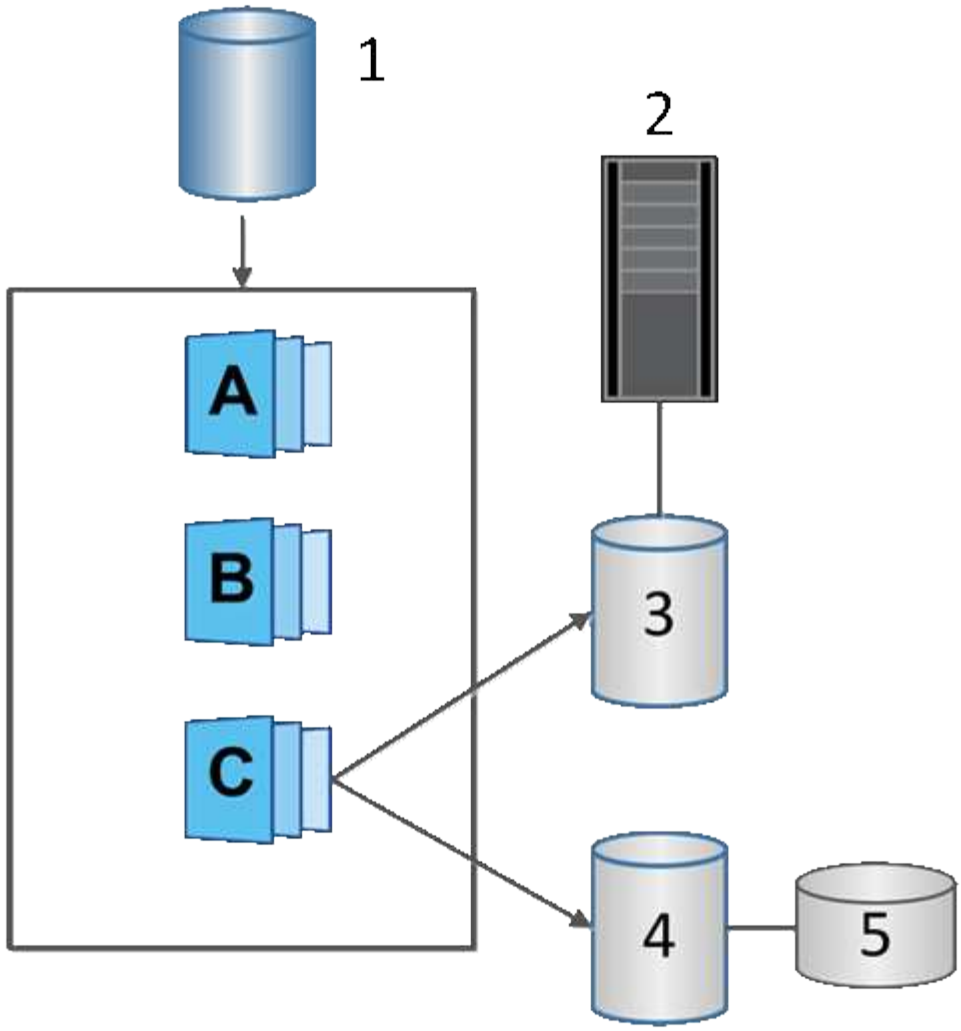
[1] Capacidade reservada; [2] Volume de membro; [3] Imagens de Snapshot do grupo de consistência

Saiba mais sobre volumes de Snapshot no software SANtricity

Você pode criar um volume de Snapshot e atribuí-lo a um host se desejar ler ou gravar dados de Snapshot. O volume de Snapshot compartilha as mesmas características do volume base (nível RAID, características de E/S e assim por diante).

Ao criar um volume de Snapshot, você pode designá-lo como *somente leitura* ou *acessível para leitura e gravação*.

Ao criar volumes de Snapshot somente leitura, não é necessário adicionar capacidade reservada. Ao criar volumes de Snapshot de leitura e gravação, é preciso adicionar capacidade reservada para fornecer acesso de gravação.



[1] Volume base; [2] Host; [3] Volume de Snapshot somente leitura; [4] Volume de Snapshot leitura e gravação; [5] Capacidade reservada

Saiba mais sobre reverter de Snapshot no software SANtricity

Uma operação de reverter retorna um volume base a um estado anterior, determinado pelo Snapshot selecionado.

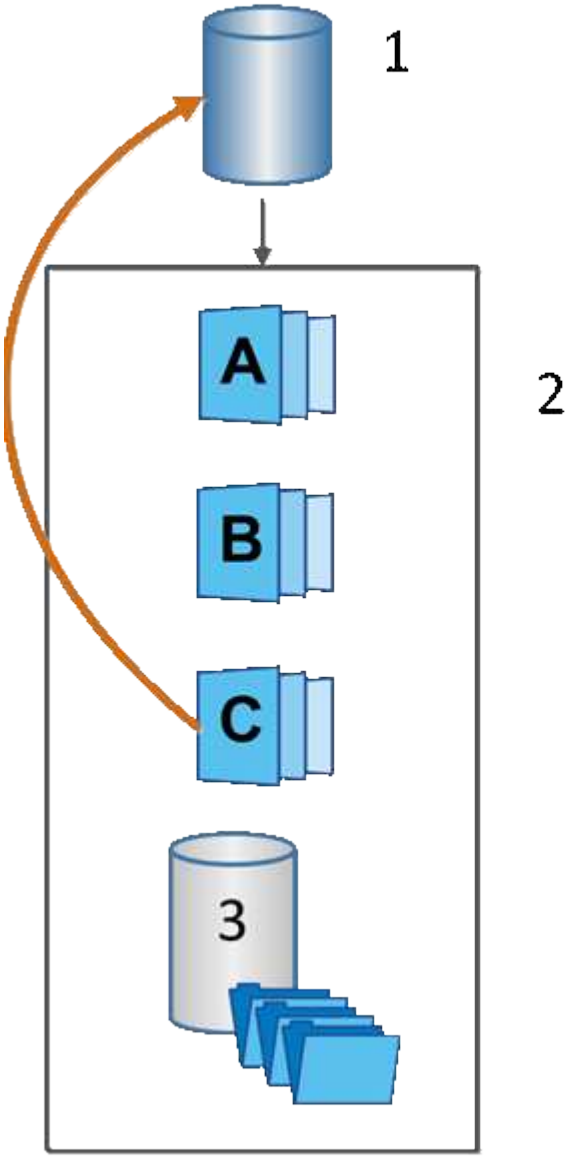
Para reverter, você pode selecionar uma imagem de Snapshot de qualquer uma das seguintes fontes:

- **Snapshot image rollback**, para uma restauração completa de um volume base.
- **Reverter grupo de consistência do Snapshot**, que pode ser usada para reverter um ou mais volumes.

Durante o reverter, o recurso de Snapshots preserva todas as imagens de snapshot no grupo. Ele também permite que o host acesse o volume base durante esse processo, se necessário para operações de E/S.

Quando uma reverter é iniciada, um processo em segundo plano percorre os endereços de bloco lógico (LBAs) do volume base e, em seguida, encontra os dados copy-on-write na imagem de Snapshot de rollback a serem restaurados. 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 o rollback está sendo processado. A transferência de

dados continua como uma operação em segundo plano até que o rollback seja concluído.



[1] Volume base; [2] Objetos Snapshot em um grupo; [3] Capacidade reservada do grupo de Snapshot

Criar Snapshots e objetos de Snapshot

Crie uma imagem de Snapshot no SANtricity System Manager

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 *instant snapshot* ou *instant image*.

Antes de começar

- O volume base deve ser ideal.
- A unidade deve estar otimizada.

- O grupo de Snapshot não pode ser designado como “reserved.”
- O volume de capacidade reservada deve ter as mesmas configurações de Data Assurance (DA) que o volume base associado ao grupo de snapshot.

Passos

1. Execute uma das seguintes ações para criar uma imagem de Snapshot:
   - Selecione **Storage › Volumes**. Selecione o objeto (base volume ou snapshot consistency group) e, em seguida, selecione **Copy Services › Create instant snapshot**.
   - Selecione **Storage › Snapshots**. Selecione a guia **Snapshot Images** e, em seguida, selecione **Create › Instant snapshot**.

     A caixa de diálogo Create Snapshot Image é exibida. Selecione o objeto (volume base ou grupo de consistência de snapshot) e clique em **Next**. Se uma imagem de snapshot anterior já tiver sido criada para o volume ou grupo de consistência de snapshot, o sistema cria o snapshot instantaneamente. Caso contrário, se esta for a primeira vez que uma imagem de snapshot é criada para o volume ou grupo de consistência de snapshot, a caixa de diálogo Confirm Create Snapshot Image é exibida.

2. Clique em **Criar** para aceitar a notificação de que é necessária capacidade reservada e para prosseguir para a etapa Reserve Capacity.

   A caixa de diálogo Reserve Capacity é exibida.

3. Use o seletor para ajustar a porcentagem de capacidade e, em seguida, clique em **Avançar** para aceitar o volume destacado na tabela.

   A caixa de diálogo Edit Settings é exibida.

4. Selecione as configurações para a imagem de Snapshot conforme apropriado e confirme que deseja realizar a operação.

Detalhes do campo

Configuração	Descrição
Configurações de imagem Snapshot	Limite de imagens do Snapshot
Mantenha a caixa de seleção marcada se desejar que as imagens de Snapshot sejam excluídas automaticamente após o limite especificado; use a caixa de rotação para alterar o limite. Se você desmarcar esta caixa de seleção, a criação de imagens de Snapshot será interrompida após 32 imagens.	**Configurações de capacidade reservada**
Avise-me quando…	Use a caixa de seleção para ajustar o ponto percentual em que o sistema envia uma notificação de alerta quando a capacidade reservada para um grupo de Snapshot estiver quase cheia. Quando a capacidade reservada para o grupo 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 para capacidade totalmente reservada	Escolha uma das seguintes políticas: • **Excluir imagem de snapshot mais antiga** — O sistema exclui automaticamente a imagem de snapshot mais antiga no grupo de snapshots, o que libera a capacidade reservada da imagem de snapshot para reutilização dentro do grupo. • **Rejeitar gravações no volume base** — Quando a capacidade reservada atinge a 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

- System Manager exibe a nova imagem de Snapshot na tabela Snapshot Images. A tabela lista a nova imagem por carimbo de data/hora e volume base associado ou grupo de consistência de Snapshot.
- A criação de Snapshot pode permanecer no estado Pendente devido às seguintes condições:
  - O volume base que contém esta imagem de Snapshot é membro de um grupo de espelhamento assíncrono.

- O volume base está atualmente em uma operação de sincronização. A criação da imagem Snapshot é concluída assim que a operação de sincronização é concluída.

Agendar imagens de Snapshot no SANtricity System Manager

Você cria um agendamento do Snapshot para permitir a recuperação em caso de problema com o volume base e para realizar backups agendados. Snapshots de volumes base ou grupos de consistência de Snapshot podem ser criados em um agendamento diário, semanal ou mensal, a qualquer hora do dia.

Antes de começar

O volume base deve ser Optimal.

Sobre esta tarefa

Esta tarefa descreve como criar um agendamento do Snapshot para um grupo de consistência de Snapshot ou volume base existente.

> Você também pode criar um agendamento do Snapshot ao mesmo tempo em que cria uma imagem de Snapshot de um volume base ou grupo de consistência.

Passos

1. Execute uma das seguintes ações para criar um agendamento do Snapshot:
   - Selecione o menu: storage [Volumes].

     Selecione o objeto (volume ou grupo de consistência de snapshot) para este agendamento do Snapshot e, em seguida, selecione **Copy Services › Criar agendamento do Snapshot**.
   - Selecione o menu: storage[Snapshots].

     Selecione a guia **Agendamentos** e clique em **Criar**.
2. Selecione o objeto (volume ou grupo de consistência de Snapshot) para este agendamento do Snapshot e clique em **Next**.

   A caixa de diálogo Criar agendamento do Snapshot é exibida.
3. Execute uma das seguintes ações:
   - **Use um agendamento previamente definido de outro objeto de Snapshot**.

     Certifique-se de que as opções avançadas estejam exibidas. Clique em **Mostrar mais opções**. Clique em **Importar agendamento**, selecione o objeto com o agendamento que deseja importar e clique em **Importar**.
   - **Modifique as opções básicas ou avançadas**.

     No canto superior direito da caixa de diálogo, clique em **Mostrar mais opções** para exibir todas as opções e então consulte a tabela a seguir.

Detalhes do campo

Campo	Descrição
Configurações básicas	Selecione dias
Selecione dias específicos da semana para imagens de Snapshot.	Hora de início
Na lista suspensa, selecione um novo horário de início para os Snapshots diários (as opções são fornecidas em incrementos de meia hora). O horário de início padrão é meia hora à frente do horário atual.	Fuso horário
Na lista suspensa, selecione o fuso horário do seu array.	**Configurações avançadas**
Dia / mês	Escolha uma das seguintes opções: • **Diário / Semanal** — Selecione dias individuais para sincronização de Snapshots. Você também pode selecionar a caixa de seleção **Selecionar todos os dias** no canto superior direito se desejar um agendamento diário. • **Mensal / Anual** — Selecione meses individuais para snapshots de sincronização. No campo **Em dia(s)**, insira os dias do mês para as sincronizações ocorrerem. As entradas válidas são **1** até **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,Last. Você também pode selecionar a caixa de seleção **Select all months** no canto superior direito se quiser um agendamento mensal.
Hora de início	Na lista suspensa, selecione um novo horário de início para os Snapshots diários (as opções são fornecidas em incrementos de meia hora). O horário de início padrão é meia hora à frente do horário atual.
Fuso horário	Na lista suspensa, selecione o fuso horário do seu array.

Campo	Descrição
Snapshots por dia / Intervalo entre snapshots	Selecione o número de imagens de Snapshot a serem criadas por dia. Se selecionar mais de uma, selecione também o intervalo de tempo entre as imagens de Snapshot. Para várias imagens de Snapshot, certifique-se de ter capacidade reservada suficiente.
Criar imagem de Snapshot agora?	Selecione esta caixa de seleção para criar uma imagem instantânea além das imagens automáticas que você está agendando.
Data de início/término ou sem data de término	Insira a data de início para que as sincronizações comecem. Insira também uma data de término ou selecione **Sem data de término**.

4. Execute uma das seguintes ações:
   - Se o objeto for um grupo de consistência do Snapshot, clique em **Criar** para aceitar as configurações e criar o agendamento.
   - Se o objeto for um volume, clique em **Avançar** para alocar capacidade reservada para as imagens de Snapshot.

     A tabela de volumes candidatos exibe apenas os candidatos que suportam a capacidade reservada especificada. A capacidade reservada é a capacidade física alocada que é usada para qualquer operação de serviço de cópia e objeto de storage. Não é diretamente legível pelo host.

5. Use a caixa spinner para alocar a capacidade reservada para as imagens de Snapshot. Execute uma das seguintes ações:
   - **Aceite as configurações padrão.**

     Utilize esta opção recomendada para alocar a capacidade reservada para as imagens de Snapshot com as configurações padrão.

   - **Aloque suas próprias configurações de capacidade reservada para atender às suas necessidades de storage de dados.**

     Se você alterar a configuração padrão de capacidade reservada, clique em **Atualizar candidatos** para atualizar a lista de candidatos para a capacidade reservada que você especificou.

     Aloque 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 coleta de imagens de Snapshot.

6. Clique em **Next**.

   A caixa de diálogo Edit Settings é exibida.

7. Edite as configurações do agendamento do Snapshot conforme necessário e, em seguida, clique em **Concluir**.

Detalhes do campo

Configuração	Descrição
Limite de imagens Snapshot	Ative a exclusão automática de snapshot images quando…
Mantenha a caixa de seleção marcada se desejar que as imagens de Snapshot sejam excluídas automaticamente após o limite especificado; use a caixa de rotação para alterar o limite. Se você desmarcar esta caixa de seleção, a criação de imagens de Snapshot será interrompida após 32 imagens.	**Configurações de capacidade reservada**
Avise-me quando…	Use o seletor giratório para ajustar o ponto percentual em que o sistema envia uma notificação de alerta quando a capacidade reservada para um agendamento estiver quase cheia. Quando a capacidade reservada para o agendamento exceder o limite especificado, use o aviso prévio para aumentar a capacidade reservada ou para excluir objetos desnecessários antes que o espaço restante se esgote.
Política para capacidade totalmente reservada	Escolha uma das seguintes políticas: • **Excluir imagem de Snapshot mais antiga** — O sistema exclui automaticamente a imagem de Snapshot mais antiga, o que libera a capacidade reservada da imagem de Snapshot para reutilização dentro do grupo de Snapshot. • **Rejeitar gravações no volume base** — Quando a capacidade reservada atinge a porcentagem máxima definida, o sistema rejeita qualquer solicitação de gravação de E/S para o volume base que acionou o acesso à capacidade reservada.

Crie um grupo de consistência de snapshot no SANtricity System Manager

Para garantir que você tenha cópias consistentes, você pode criar um conjunto de vários volumes chamado *grupo de consistência de snapshot*.

Este grupo permite criar imagens instantâneas de todos os volumes ao mesmo tempo para consistência. Cada volume que pertence a um grupo de consistência de snapshot é denominado *volume 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 membro.

Sobre esta tarefa

A sequência de criação do grupo de consistência de Snapshot permite selecionar volumes membros para o grupo e alocar capacidade aos volumes membros.

O processo para criar um grupo de consistência de snapshot é um procedimento de várias etapas.

Etapa 1: adicione membros ao grupo de consistência de Snapshot

Selecione os membros para especificar uma coleção de volumes que compõem o grupo de consistência de Snapshot. Quaisquer ações que você executar no grupo de consistência de Snapshot serão aplicadas uniformemente aos volumes membros selecionados.

Antes de começar

Os volumes dos membros devem estar Otimizados.

Passos

1. Selecione o menu: storage[Snapshots].
2. Clique na guia **Snapshot Consistency Groups**.
3. Selecione o menu: criar [Snapshot grupo de consistência].

   A caixa de diálogo Criar Grupo de Consistência de Snapshot é exibida.

4. Selecione os volumes a serem adicionados como volumes membros ao grupo de consistência de snapshot.
5. Clique em **Next** e vá para Etapa 2: reserve capacidade para grupo de consistência de Snapshot.

Etapa 2: reserve capacidade para grupo de consistência de Snapshot

Associe a capacidade reservada ao grupo de consistência de snapshot. System Manager sugere os volumes e a capacidade com base nas propriedades do grupo de consistência de snapshot. Você pode aceitar a configuração de capacidade reservada recomendada ou personalizar o storage alocado.

Sobre esta tarefa

Na caixa de diálogo Capacidade Reservada, a tabela de volumes candidatos exibe apenas os candidatos que suportam a capacidade reservada especificada. A capacidade reservada é a capacidade física alocada que é usada para qualquer operação de serviço de cópia e storage. Não é diretamente legível pelo host.

Passos

1. Use a caixa de rotação para alocar a capacidade reservada para o grupo de consistência de Snapshot. Execute uma das seguintes ações:
   - **Aceite as configurações padrão**.

     Utilize esta opção recomendada para alocar a capacidade reservada para cada volume membro com as configurações padrão.

   - **Aloque suas próprias configurações de capacidade reservada para atender às suas necessidades de storage de dados.**

     Aloque 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 coleta de imagens de Snapshot.

2. **Opcional:** Se você alterar a configuração padrão de capacidade reservada, clique em **Atualizar candidatos** para atualizar a lista de candidatos para a capacidade reservada que você especificou.
3. Clique em **Próximo** e vá para Etapa 3: editar as configurações do grupo de consistência de Snapshot.

Etapa 3: editar as configurações do grupo de consistência de Snapshot

Aceite ou selecione as configurações de exclusão automática e os 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 Snapshot permite selecionar volumes membros para o grupo e alocar capacidade aos volumes membros.

Passos

1. Aceite ou altere as configurações padrão para o grupo de consistência do snapshot conforme apropriado.

Detalhes do campo

Configuração	Descrição
Configurações do grupo de consistência do Snapshot	Nome
Especifique o nome para o grupo de consistência de Snapshot.	Ative a exclusão automática de snapshot images quando…
Mantenha a caixa de seleção marcada se desejar que as imagens de Snapshot sejam excluídas automaticamente após o limite especificado; use a caixa de rotação para alterar o limite. Se você desmarcar esta caixa de seleção, a criação de imagens de Snapshot será interrompida após 32 imagens.	**Configurações de capacidade reservada**
Avise-me quando…	Use a caixa de seleção para ajustar o ponto percentual em que o sistema envia uma notificação de alerta quando a capacidade reservada para um grupo de consistência de snapshot estiver quase cheia. 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 para capacidade totalmente reservada	Escolha uma das seguintes políticas: • **Excluir imagem de snapshot mais antiga** — O sistema exclui automaticamente a imagem de snapshot mais antiga no grupo de consistência de snapshot, o que libera a capacidade reservada da imagem de snapshot para reutilização dentro do grupo. • **Rejeitar gravações no volume base** — Quando a capacidade reservada atinge a 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 se certificar de que a configuração do seu grupo de consistência de Snapshot está correta,

clique em **Concluir**.

Crie um volume de Snapshot no SANtricity System Manager

Você cria um volume de snapshot para fornecer acesso do host a uma imagem de snapshot de um volume ou grupo de consistência. Você pode designar o volume de snapshot como somente leitura ou leitura/gravação.

Sobre esta tarefa

A sequência de criação de volume de snapshot permite criar um volume de snapshot a partir de uma imagem de snapshot e oferece opções para alocar capacidade reservada caso o volume seja leitura/gravação. Um volume de snapshot pode ser designado como um dos seguintes:

- Um volume de snapshot somente leitura fornece a um aplicativo host acesso de leitura a uma cópia dos dados contidos na imagem do snapshot, mas sem a capacidade de modificar a imagem do snapshot. Um volume de snapshot somente leitura não possui capacidade reservada associada.
- Um volume de snapshot de leitura/gravação fornece ao aplicativo host acesso de gravação a uma cópia dos dados contidos na imagem do snapshot. Ele possui sua própria capacidade reservada, usada para salvar quaisquer modificações subsequentes feitas pelo aplicativo host no volume base sem afetar a imagem do snapshot referenciada.

O processo para criar um volume de snapshot é um procedimento de várias etapas.

Etapa 1: analise os membros para um volume de Snapshot

Selecione uma imagem de Snapshot de um volume base ou de um grupo de consistência de Snapshot. Se você selecionar uma imagem de Snapshot de um grupo de consistência de Snapshot, os volumes membros do grupo de consistência de Snapshot aparecerão para revisão.

Passos

1. Selecione o menu: storage[Snapshots].
2. Selecione a guia **Snapshot Volumes**.
3. Selecione **Create**.

   A caixa de diálogo Criar Volume de Snapshot é exibida.

4. Selecione a imagem de Snapshot (volume ou grupo de consistência de Snapshot) que deseja converter em um volume de Snapshot e clique em **Next**. Use uma entrada de texto no campo **Filter** para refinar a lista.

   Se a seleção for para uma imagem de Snapshot de grupo de consistência, a caixa de diálogo Revisar membros será exibida.

   Na caixa de diálogo Revisar membros, revise a lista de volumes selecionados para conversão em volumes de snapshot e clique em **Next**.

5. Vá para Etapa 2: atribua o volume de snapshot ao host.

Etapa 2: atribua o volume de snapshot ao host

Selecione um host ou cluster de hosts específico para atribuí-lo ao volume de snapshot. Essa atribuição concede a um host ou cluster de hosts acesso ao volume de snapshot. Você pode optar por atribuir um host posteriormente, se necessário.

Antes de começar

- Hosts ou clusters de hosts válidos existem na página Hosts.
- Os identificadores de porta do host devem ter sido definidos para o host.
- Antes de criar um volume com DA habilitado, verifique se a conexão de host planejada oferece suporte ao recurso Data Assurance (DA). Se alguma das conexões de host nos controladores do seu array de storage não oferecer suporte a DA, os hosts associados não poderão acessar dados em volumes com DA habilitado.

Sobre esta tarefa

Ao atribuir volumes, tenha em mente estas diretrizes:

- O sistema operacional do host pode ter limites específicos quanto à quantidade de volumes que o host pode acessar.
- Você pode definir uma atribuição de host para cada volume de snapshot no array de storage.
- Os volumes atribuídos são compartilhados entre os controladores no array de storage.
- O mesmo número de unidade lógica (LUN) não pode ser usado duas vezes por um host ou um cluster de hosts para acessar um volume de snapshot. Você deve usar um LUN exclusivo.

A atribuição de um volume a um host falha se você tentar atribuir um volume a um cluster de hosts que conflita com uma atribuição já estabelecida para um host no cluster de hosts.

Passos

1. Na caixa de diálogo **Atribuir ao host**, selecione o host ou cluster de hosts que você deseja atribuir ao novo volume. Se você quiser criar o volume sem atribuir um host, selecione **Atribuir posteriormente** 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 de Snapshot e requer capacidade reservada.
   - **Somente leitura** — Esta opção fornece ao host acesso somente leitura ao volume de snapshot e não requer capacidade reservada.
3. Clique em **Avançar** e faça um dos seguintes:
   - Se o seu volume de snapshot for leitura/gravação, a caixa de diálogo Revisar Capacidade será exibida. Vá para Etapa 3: reserve capacidade para um volume de snapshot.
   - Se o seu volume de snapshot for somente leitura, a caixa de diálogo Editar Prioridade será exibida. Vá para Etapa 4: editar as configurações de um volume de snapshot.

Etapa 3: reserve capacidade para um volume de snapshot

Associe a capacidade reservada a um volume de snapshot de leitura/gravação. System Manager sugere os volumes e a capacidade com base nas propriedades do volume base ou do grupo de consistência de snapshot. Você pode aceitar a configuração de capacidade reservada recomendada ou personalizar o storage alocado.

Sobre esta tarefa

Você pode aumentar ou diminuir a capacidade reservada para o volume de snapshot conforme necessário. Se você perceber que a capacidade reservada para o snapshot é maior do que você precisa, pode reduzir seu tamanho para liberar espaço que é necessário para outros volumes lógicos.

Passos

1. Use a caixa de rotação para alocar a capacidade reservada para o volume de Snapshot.

   A tabela Volume Candidate exibe apenas os candidatos que suportam a capacidade reservada especificada.

   Execute uma das seguintes ações:

   - **Aceite as configurações padrão**.

     Use esta opção recomendada para alocar a capacidade reservada para o volume de snapshot com as configurações padrão.

   - **Aloque suas próprias configurações de capacidade reservada para atender às suas necessidades de storage de dados**.

     Se você alterar a configuração padrão de capacidade reservada, clique em **Atualizar candidatos** para atualizar a lista de candidatos para a capacidade reservada que você especificou.

     Aloque a capacidade reservada usando as seguintes diretrizes.

     - A configuração padrão para capacidade reservada é 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 coleta de imagens de Snapshot.
2. **Opcional:** Se você estiver criando o volume de snapshot para um grupo de consistência de snapshot, a opção "Alterar candidato" aparece na tabela Candidatos de Capacidade Reservada. Clique em **Alterar candidato** para selecionar um candidato alternativo de capacidade reservada.
3. Clique em **Próximo** e vá para Etapa 4: editar as configurações de um volume de snapshot.

Etapa 4: editar as configurações de um volume de snapshot

Altere as configurações de um volume de snapshot, como seu nome, armazenamento em cache, limites de alerta de capacidade reservada e assim por diante.

Sobre esta tarefa

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

Passos

1. Aceite ou altere as configurações do volume de Snapshot conforme necessário.

Detalhes do campo

Configuração	Descrição
Configurações de volume do Snapshot	Nome
Especifique o nome para o volume de Snapshot.	Ativar SSD Cache
Selecione esta opção para ativar armazenamento em cache somente leitura em SSDs.	**Configurações de capacidade reservada**
Avise-me quando…	**Aparece apenas para um volume de Snapshot de leitura/gravação**. Use a caixa de seleção para ajustar o ponto percentual em que o sistema envia uma notificação de alerta quando a capacidade reservada para um grupo de Snapshot estiver quase cheia. Quando a capacidade reservada para o grupo 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.

2. Revise a configuração do volume de Snapshot. Clique em **Voltar** para fazer quaisquer alterações.
3. Quando estiver satisfeito com a configuração do seu volume de Snapshot, clique em **Concluir**.

Gerenciar agendamentos de Snapshot

Altere as configurações de um agendamento do Snapshot no SANtricity System Manager

Para um agendamento do Snapshot, você pode alterar os horários de coleta automática ou a frequência da coleta.

Sobre esta tarefa

Você pode importar configurações de um agendamento do Snapshot existente ou pode modificar as configurações conforme necessário.

Como um agendamento do Snapshot está associado a um grupo de Snapshot ou grupo de consistência de Snapshot, a capacidade reservada pode ser afetada por alterações nas configurações de agendamento.

Passos

1. Selecione o menu: storage[Snapshots].
2. Clique na aba **Schedules**.
3. Selecione o agendamento do Snapshot que você deseja alterar e clique em **Editar**.

A caixa de diálogo Editar agendamento do Snapshot é exibida.

4. Faça uma das seguintes ações:
   - **Use um agendamento previamente definido de outro objeto de Snapshot** — Clique em **Importar agendamento**, selecione o objeto com o agendamento que deseja importar e clique em **Importar**.
   - **Edite as configurações de agendamento** — Consulte os detalhes do campo abaixo.

     Detalhes do campo

Configuração	Descrição
Dia / mês	Escolha uma das seguintes opções: • **Diário / Semanal** — Selecione dias individuais para sincronização de Snapshots. Você também pode selecionar a caixa de seleção **Selecionar todos os dias** no canto superior direito se desejar um agendamento diário. • **Mensal / Anual** — Selecione meses individuais para snapshots de sincronização. No campo **Em dia(s)**, insira os dias do mês para as sincronizações ocorrerem. As entradas válidas são **1** até **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,Last. Você também pode selecionar a caixa de seleção **Select all months** no canto superior direito se quiser um agendamento mensal.
Hora de início	Na lista suspensa, selecione um novo horário de início para os Snapshots diários. As opções são apresentadas em incrementos de meia hora. O horário de início padrão é meia hora à frente do horário atual.
Fuso horário	Na lista suspensa, selecione o fuso horário do seu array de storage.
Snapshots por dia Tempo entre Snapshots	Selecione o número de imagens de Snapshot a serem criadas por dia. Se você selecionar mais de um, selecione também o tempo entre os pontos de restauração. Para múltiplos pontos de restauração, certifique-se de ter capacidade reservada adequada.
Data de início Data de término Sem data de término	Insira a data de início para que as sincronizações comecem. Insira também uma data de término ou selecione **Sem data de término**.

5. Clique em **Salvar**.

Ativar e suspender um agendamento de snapshots no SANtricity System Manager

Você pode suspender temporariamente a coleta agendada de imagens instantâneas quando precisar economizar espaço de storage. Esse método é mais eficiente do que excluir e, posteriormente, recriar o agendamento de instantâneos.

Sobre esta tarefa

O estado do agendamento de snapshot permanece suspenso até que você use a opção **Ativar** para retomar a atividade de snapshot agendada.

Passos

1. Selecione o menu: storage[Snapshots].
2. Caso ainda não esteja visível, clique na guia **Schedules**.

   Os horários estão listados na página.

3. Selecione um agendamento de snapshot ativo que você deseja suspender e clique em **Ativar / Suspender**.

   O status da coluna Estado muda para **Suspenso**, e o agendamento de snapshot interrompe a coleta de todas as imagens de snapshot.

4. Para retomar a coleta de imagens instantâneas, selecione a programação de snapshot suspensa que deseja retomar e clique em **Ativar/Suspender**.

   O status da coluna State muda para **Active**.

Excluir um agendamento de Snapshot no SANtricity System Manager

Se você não quiser mais coletar imagens de Snapshot, poderá excluir um agendamento de Snapshot existente.

Sobre esta tarefa

Ao excluir um agendamento de snapshot, as imagens de snapshot associadas não são excluídas juntamente com ele. Se você acha que a coleta de imagens de snapshot poderá ser retomada em algum momento, você deve suspender o agendamento de snapshot em vez de excluí-lo.

Passos

1. Selecione o menu: storage[Snapshots].
2. Clique na aba **Schedules**.
3. Selecione a programação de Snapshot que deseja excluir e confirme a operação.

Resultados

O sistema remove todos os atributos de agendamento do volume base ou do grupo de consistência de Snapshot.

Gerenciar imagens de Snapshot

Visualize as configurações de Snapshot no SANtricity System Manager

Você pode visualizar as propriedades, o status, a capacidade reservada e os objetos associados atribuídos a cada imagem de Snapshot.

Sobre esta tarefa

Os objetos associados a uma imagem de Snapshot incluem o volume base ou grupo de consistência de Snapshot para o qual esta imagem de Snapshot é um ponto de restauração, o grupo de Snapshot associado e quaisquer volumes de Snapshot criados a partir da imagem de Snapshot. Use as configurações de Snapshot para determinar se deseja copiar ou converter a imagem de Snapshot.

Passos

1. Selecione o menu: storage[Snapshots].
2. Clique na guia **Snapshot Images**.
3. Selecione a imagem de Snapshot que você deseja visualizar e, em seguida, clique em **View Settings**.

   A caixa de diálogo Configurações de Snapshot é exibida.

4. Veja as configurações para a imagem Snapshot.

Iniciar o rollback da imagem de Snapshot para um volume base no SANtricity System Manager

Você pode executar uma operação de reverter para alterar o conteúdo de um volume base para corresponder ao conteúdo salvo em uma imagem de Snapshot.

A operação de reverter não altera o conteúdo das imagens de Snapshot associadas ao volume base.

Antes de começar

- Existe capacidade reservada suficiente para iniciar uma operação de reverter.
- A imagem de Snapshot selecionada está como Ideal e o volume selecionado está como Ideal.
- O volume selecionado não possui uma operação de reverter já em andamento.

Sobre esta tarefa

A sequência de início de reverter permite iniciar o reverter em uma imagem de Snapshot de um volume base, oferecendo opções para adicionar capacidade de storage. Você não pode iniciar mais de uma operação de reverter para um volume base ao mesmo tempo.

> O host pode acessar imediatamente o novo volume base revertido, mas o volume base existente não permite acesso de leitura e gravação ao host após o início do reverter. Você pode criar um Snapshot do volume base imediatamente antes de iniciar o reverter para preservar o volume base anterior à reversão para fins de recuperação.

Passos

1. Selecione o menu: storage[Snapshots].
2. Selecione a guia **Snapshot Images**.
3. Selecione a imagem do Snapshot e, em seguida, selecione menu: reverter[Iniciar].

   A caixa de diálogo Confirmar início de reverter é exibida.

4. **Opcional:** selecione a opção **Aumentar a capacidade** se necessário.

   A caixa de diálogo Increase Reserved Capacity é exibida.

   a. Use a caixa de rotação para ajustar a porcentagem de capacidade.

      Se não houver capacidade livre no pool ou grupo de volume que contém o objeto de storage selecionado e o array de storage tiver Unassigned Capacity, você pode adicionar capacidade. Você pode criar um novo pool ou grupo de volume e então tentar novamente esta operação usando a nova capacidade livre nesse pool ou grupo de volume.

   b. Clique em **Increase**.

5. Confirme que deseja realizar esta operação e, em seguida, clique em **Reverter**.

Resultados

System Manager executa as seguintes ações:

- Restaura o volume com o conteúdo salvo na imagem de Snapshot selecionada.
- Torna os volumes revertidos imediatamente disponíveis para acesso do host. Não é necessário aguardar a conclusão da operação de reverter.

Depois que você terminar

Selecione o menu: Home [View Operations in Progress] para visualizar o progresso da operação de reverter.

Se a operação de reverter não for bem-sucedida, a operação será pausada. Você pode retomar a operação pausada e, se ainda assim não for bem-sucedida, siga o procedimento do Recovery Guru para corrigir o problema ou entre em contato com o suporte técnico.

Iniciar reverter imagem de Snapshot para volumes membros do grupo de consistência de Snapshot no SANtricity System Manager

Você pode executar uma operação de reverter para alterar o conteúdo dos volumes membros do grupo de consistência de Snapshot para corresponder ao conteúdo que está salvo em uma imagem de Snapshot.

A operação de reverter não altera o conteúdo das imagens de Snapshot associadas ao grupo de consistência.

Antes de começar

- Existe capacidade reservada suficiente para iniciar uma operação de reverter.
- A imagem de Snapshot selecionada está como Ideal e o volume selecionado está como Ideal.
- O volume selecionado não possui uma operação de reverter já em andamento.

Sobre esta tarefa

A sequência de início de reverter permite iniciar o reverter em uma imagem de Snapshot de um grupo de consistência de Snapshot, oferecendo opções para adicionar capacidade de storage. Você não pode iniciar mais de uma operação de reverter para um grupo de consistência de Snapshot ao mesmo tempo.

O host tem acesso imediato aos novos volumes revertidos, mas os volumes membros existentes não permitem mais acesso de leitura e gravação do host após o início do reverter. Você pode criar uma imagem de Snapshot dos volumes membros imediatamente antes de iniciar o reverter para preservar os volumes base pré-reverter para fins de recuperação.

O processo para iniciar o rollback de uma imagem de Snapshot de um grupo de consistência de Snapshot é um procedimento de várias etapas.

Passo 1: selecionar membros

Você deve selecionar os volumes membros que serão revertidos.

Passos

1. Selecione o menu: storage[Snapshots].
2. Selecione a guia **Snapshot Images**.
3. Selecione a imagem de Snapshot do grupo de consistência de Snapshot e, em seguida, selecione **Rollback › Start**.

   A caixa de diálogo Iniciar reverter é exibida.

4. Selecione o volume ou volumes do membro.
5. Clique em **Avançar** e faça um dos seguintes:
   - Se algum dos volumes de membro selecionados estiver associado a mais de um objeto de capacidade reservada que armazena imagens de Snapshot, a caixa de diálogo Revisar Capacidade será exibida. Vá para Etapa 2: analisar a capacidade.
   - Se nenhum dos volumes de membro selecionados estiver associado a mais de um objeto de capacidade reservada que armazena imagens de Snapshot, a caixa de diálogo Editar Prioridade será exibida. Vá para Etapa 3: editar prioridade.

Etapa 2: analisar a capacidade

Se você selecionou volumes membros associados a mais de um objeto de capacidade reservada, como um grupo de Snapshot e um volume de capacidade reservada, você pode revisar 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 **Increase capacity** na coluna **Edit**.

   A caixa de diálogo Increase Reserved Capacity é exibida.

2. Use o seletor giratório para ajustar a porcentagem de capacidade e, em seguida, clique em **Increase**.

   Se não houver capacidade livre no pool ou grupo de volume que contém o objeto de storage selecionado e o array de storage tiver Unassigned Capacity, você pode adicionar capacidade. Você pode criar um novo pool ou grupo de volume e tentar novamente esta operação usando a nova capacidade livre nesse pool ou grupo de volume.

3. Clique em **Próximo** e vá para Etapa 3: editar prioridade.

   A caixa de diálogo Edit Priority é exibida.

Etapa 3: editar prioridade

Você pode editar a prioridade da operação de reverter, se necessário.

Sobre esta tarefa

A prioridade de reverter determina quantos recursos do sistema são dedicados à operação de reverter, em detrimento do desempenho do sistema.

Passos

1. Use o controle deslizante para ajustar a prioridade de reverter conforme necessário.
2. Confirme que deseja realizar esta operação e, em seguida, clique em **Concluir**.

Resultados

System Manager executa as seguintes ações:

- Restaura os volumes membros do grupo de consistência de Snapshot com o conteúdo salvo na imagem de Snapshot selecionada.
- Torna os volumes revertidos imediatamente disponíveis para acesso do host. Não é necessário aguardar a conclusão da operação de reverter.

Depois que você terminar

Selecione o menu: Home [View Operations in Progress] para visualizar o progresso da operação de reverter.

Se a operação de reverter não for bem-sucedida, a operação será pausada. Você pode retomar a operação pausada e, se ainda assim não for bem-sucedida, siga o procedimento do Recovery Guru para corrigir o problema ou entre em contato com o suporte técnico.

Retomar o reverter de uma imagem de Snapshot no SANtricity System Manager

Se ocorrer um erro durante uma operação de reverter imagem Snapshot, a operação será pausada automaticamente. Você pode retomar uma operação de reverter que esteja pausada.

Passos

1. Selecione o menu: storage[Snapshots].
2. Clique na guia **Snapshot Images**.
3. Destaque o rollback pausado e, em seguida, selecione **Rollback › Resume**.

   A operação é retomada.

Resultados

System Manager executa as seguintes ações:

- Se a operação de reverter for retomada com sucesso, você poderá visualizar o progresso da operação de reverter na janela Operações em Andamento.
- Se a operação de reverter não for bem-sucedida, a operação será pausada novamente. Você pode seguir o procedimento do Recovery Guru para corrigir o problema ou entrar em contato com o suporte técnico.

Cancelar o rollback da imagem de Snapshot no SANtricity System Manager

Você pode cancelar um reverter ativo que esteja em andamento (copiando dados ativamente), um reverter pendente (em uma fila de espera aguardando recursos para iniciar) ou um reverter que tenha sido pausado devido a um erro.

Sobre esta tarefa

Ao cancelar uma operação de reverter que está em andamento, o volume base retorna a um estado inutilizável e aparece como falho. Portanto, considere cancelar uma operação de reverter somente quando existirem opções de recuperação para restaurar o conteúdo do volume base.

> Se o grupo de snapshot no qual a imagem de snapshot reside tiver uma ou mais imagens de snapshot que foram excluídas automaticamente, a imagem de snapshot usada para a operação de reverter poderá não estar disponível para reverter futuros.

Passos

1. Selecione o menu: storage[Snapshots].
2. Clique na guia **Snapshot Images**.
3. Selecione o rollback ativo ou pausado e, em seguida, selecione **Rollback › Cancelar**.

   A caixa de diálogo Confirm Cancel Rollback é exibida.
4. Clique em **Yes** para confirmar.

Resultados

System Manager interrompe a operação de reverter. O volume base é utilizável, mas pode conter dados que são inconsistentes ou não estão intactos.

Depois que você terminar

Após cancelar uma operação de reverter, você deve realizar uma das seguintes ações:

- Reinicialize o conteúdo do volume base.
- Execute uma nova operação de reverter para restaurar o volume base usando a mesma imagem de snapshot que foi usada na operação Cancelar Reverter ou uma imagem de snapshot diferente para executar a nova operação de reverter.

Excluir uma imagem de Snapshot no SANtricity System Manager

Você exclui imagens de Snapshot para limpar a imagem de Snapshot mais antiga de um grupo de Snapshot ou grupo de consistência.

Sobre esta tarefa

Você pode excluir uma única imagem de snapshot ou pode excluir imagens de snapshot de grupos de consistência de snapshot que tenham o mesmo carimbo de data/hora de criação. Você também pode excluir imagens de snapshot de um grupo de snapshot.

Não é possível excluir uma imagem de snapshot se ela não for a imagem de snapshot mais antiga do volume base associado ou do grupo de consistência de snapshot.

Passos

1. Selecione o menu: storage[Snapshots].
2. Clique na guia **Snapshot Images**.
3. Selecione a imagem de Snapshot que deseja excluir e confirme que deseja realizar a operação.

   Se você selecionou uma imagem de Snapshot de um grupo de consistência de Snapshot, selecione cada volume membro que deseja excluir e confirme que deseja executar a operação.

4. Clique em **Delete**.

Resultados

System Manager executa as seguintes ações:

- Exclui a imagem do Snapshot do array de storage.
- Libera a capacidade reservada para reutilização dentro do grupo de Snapshot ou grupo de consistência de Snapshot.
- Desativa todos os volumes de snapshot associados que existem para a imagem de snapshot excluída.
- A partir de uma exclusão de grupo de consistência de snapshot, move qualquer volume membro associado à imagem de snapshot excluída para o estado Parado.

Gerenciar grupos de consistência de Snapshot

Adicione um volume membro a um grupo de consistência de Snapshot no SANtricity System Manager

Você pode adicionar um novo volume membro a um grupo de consistência de snapshot. Ao adicionar um novo volume membro, você também deve reservar capacidade para o volume membro.

Antes de começar

- O volume de membro deve ser Optimal.
- O grupo de consistência de Snapshot deve ter menos volumes do que o número máximo permitido (conforme definido na sua configuração).
- Cada volume de capacidade reservada deve ter as mesmas configurações de Data Assurance (DA) e segurança que o volume membro associado.

Sobre esta tarefa

Você pode adicionar volumes padrão ou volumes finos ao grupo de consistência de Snapshot. O volume base pode residir em um pool ou grupo de volume.

Passos

1. Selecione o menu: storage[Snapshots].
2. Selecione a guia **Snapshot Consistency Groups**.

   A tabela é exibida e mostra todos os grupos de consistência de Snapshot associados ao array de storage.

3. Selecione o grupo de consistência de Snapshot 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 deseja adicionar e, em seguida, clique em **Avançar**.

   A etapa Capacidade de Reserva é exibida. A tabela Candidatos a Volume mostra apenas os candidatos que suportam a capacidade de reserva especificada.

5. Use a caixa de rotação para alocar a capacidade reservada para o volume do membro. Execute uma das seguintes ações:
   - **Aceite as configurações padrão.**

Utilize esta opção recomendada para alocar a capacidade reservada para o volume de membro com as configurações padrão.

- **Aloque suas próprias configurações de capacidade reservada para atender às suas necessidades de storage de dados.**

  Se você alterar a configuração padrão de capacidade reservada, clique em **Atualizar candidatos** para atualizar a lista de candidatos para a capacidade reservada que você especificou.

  Aloque a capacidade reservada usando as seguintes diretrizes.

  - A configuração padrão para capacidade reservada é 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 coleta de imagens de Snapshot.

6. Clique em **Concluir** para adicionar os volumes de membro.

Remover um volume membro de um grupo de consistência de Snapshot no SANtricity System Manager

Você pode remover um volume membro de um grupo de consistência de Snapshot existente.

Sobre esta tarefa

Ao remover um volume membro de um grupo de consistência de Snapshot, System Manager exclui automaticamente os objetos de Snapshot associados a esse volume membro.

Passos

1. Selecione o menu: storage[Snapshots].
2. Clique na guia **Snapshot Consistency Groups**.
3. Expanda o grupo de consistência de Snapshot que deseja modificar selecionando o sinal de mais (+) ao lado dele.
4. Selecione o volume do membro que você deseja remover e clique em **Remover**.
5. Confirme que deseja realizar a operação e, em seguida, clique em **Remover**.

Resultados

System Manager executa as seguintes ações:

- Exclui todas as imagens de Snapshot e volumes de Snapshot associados ao volume membro.
- Exclui o grupo de Snapshot associado ao volume membro.
- O volume de membro não é alterado ou excluído de nenhuma outra forma.

Altere as configurações de um grupo de consistência no SANtricity System Manager

Altere as configurações de um grupo de consistência de Snapshot quando desejar alterar seu nome, as configurações de exclusão automática ou o número máximo de imagens de Snapshot permitidas.

Passos

1. Selecione o menu: storage[Snapshots].
2. Clique na guia **Snapshot Consistency Groups**.
3. Selecione o grupo de consistência do Snapshot que você deseja editar e clique em **Exibir/Editar configurações**.

   A caixa de diálogo Configuração do Grupo de Consistência do Snapshot é exibida.

4. Altere as configurações do grupo de consistência do Snapshot conforme necessário.

Detalhes do campo

Configuração	Descrição
Configurações do grupo de consistência do Snapshot	Nome
Você pode alterar o nome do grupo de consistência do Snapshot.	Exclusão automática
Mantenha a caixa de seleção marcada se desejar que as imagens de Snapshot sejam excluídas automaticamente após o limite especificado; use a caixa de rotação para alterar o limite. Se você desmarcar esta caixa de seleção, a criação de imagens de Snapshot será interrompida após 32 imagens.	Limite de imagens do Snapshot
Você pode alterar o número máximo de imagens de Snapshot permitidas para um grupo de Snapshot.	Agendamento do Snapshot
Este campo indica se um agendamento está associado ao grupo de consistência do Snapshot.	**Objetos associados**
Volumes de membro	Você pode visualizar a quantidade de volumes de membros associados ao grupo de consistência do Snapshot.

5. Clique em **Salvar**.

Excluir um grupo de consistência de Snapshot no SANtricity System Manager

Você pode excluir grupos de consistência de Snapshot que não são mais necessários.

Antes de começar

Confirme que as imagens de todos os volumes dos membros não são mais necessárias para backup ou fins de teste.

Sobre esta tarefa

Esta operação exclui todas as imagens de snapshot ou agendamentos associados ao grupo de consistência de snapshot.

Passos

1. Selecione o menu: storage[Snapshots].
2. Selecione a guia **Snapshot Consistency Groups**.
3. Selecione o grupo de consistência de Snapshot que você deseja excluir e, em seguida, selecione **Tarefas incomuns › Excluir**.

   A caixa de diálogo Confirmar Exclusão do Snapshot Consistency Group é exibida.

4. Confirme que deseja realizar esta operação e, em seguida, clique em **Delete**.

Resultados

System Manager executa as seguintes ações:

- Exclui todas as imagens de snapshot e volumes de snapshot existentes do grupo de consistência de snapshot.
- Exclui todas as imagens de Snapshot associadas que existem para cada volume membro no grupo de consistência de Snapshot.
- Exclui todos os volumes de snapshot associados que existem para cada volume membro no grupo de consistência de snapshot.
- Exclui toda a capacidade reservada associada a cada volume membro no grupo de consistência de snapshot (se selecionado).

Gerenciar volumes de Snapshot

Converter volume de Snapshot para modo de leitura/gravação no SANtricity System Manager

Você pode converter um volume de snapshot somente leitura ou um volume de snapshot de grupo de consistência para o modo de leitura e gravação, se necessário.

Um volume de Snapshot que é convertido para acesso de leitura e gravação 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 o menu: storage[Snapshots].
2. Selecione a guia **Snapshot Volumes**.

   A tabela Snapshot Volumes é exibida e mostra todos os volumes de snapshot associados ao array de storage.

3. Selecione o volume de Snapshot somente leitura que deseja converter e clique em **Converter para Read/Write**.

A caixa de diálogo Converter para Leitura/Gravação é exibida com a etapa **Reservar 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 Snapshot de leitura e gravação, execute uma das seguintes ações:
   - **Aceite as configurações padrão** — Use esta opção recomendada para alocar a capacidade reservada para o volume de Snapshot com as configurações padrão.
   - **Aloque suas próprias configurações de capacidade reservada para atender às suas necessidades de storage de dados** — Aloque a capacidade reservada seguindo as diretrizes abaixo.
     - A configuração padrão para capacidade reservada é 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 **Avançar** para revisar ou editar as configurações.

   A caixa de diálogo Edit Settings é exibida.

6. Aceite ou especifique as configurações para o volume de Snapshot conforme apropriado e, em seguida, selecione **Concluir** para converter o volume de Snapshot.

Detalhes do campo

Configuração	Descrição
Configurações de capacidade reservada	Avise-me quando…

Altere as configurações de volume para um volume de Snapshot no SANtricity System Manager

Você pode alterar as configurações de um volume de Snapshot ou de um volume de Snapshot de grupo de consistência para renomeá-lo, ativar ou desativar o armazenamento em cache em SSD, ou alterar a atribuição de host, cluster de hosts ou número de unidade lógica (LUN).

Passos

1. Selecione o menu: storage[Snapshots].
2. Clique na guia **Snapshot Volumes**.
3. Selecione o volume de Snapshot que você deseja alterar e clique em **View/Edit Settings**.

   A caixa de diálogo Configurações de Volume de Snapshot é exibida.

4. Visualize ou edite as configurações do volume de Snapshot conforme necessário.

Detalhes do campo

Configuração	Descrição
Volume de Snapshot	Nome
Você pode alterar o nome do volume de Snapshot.	Designado para
Você pode alterar a atribuição do host ou do cluster de hosts para o volume de Snapshot.	LUN
Você pode alterar a atribuição de LUN para o volume de Snapshot.	Cache SSD
Você pode ativar/desativar o armazenamento em cache somente leitura em discos de estado sólido (SSDs).	**Objetos associados**
Snapshot imagem instantânea	Você pode visualizar as imagens de Snapshot associadas ao volume de Snapshot. Uma imagem de Snapshot é uma cópia lógica dos dados do volume, capturada em um determinado ponto no tempo. Assim como um ponto de restauração, as imagens de Snapshot permitem reverter para um conjunto de dados conhecido e bom. Embora o host possa acessar a imagem de Snapshot, ele não pode lê-la ou gravá-la diretamente.
Volume base	Você pode visualizar o volume base associado ao volume de Snapshot. Um volume base é a origem a partir da qual uma imagem de Snapshot é criada. Ele pode ser um volume thick ou com thin provisioning e geralmente é atribuído a um host. O volume base pode residir em um grupo de volume ou em um pool de disco.
Grupo de Snapshot	Você pode visualizar o grupo de Snapshot associado ao volume de Snapshot. Um grupo de Snapshot é uma coleção de imagens de Snapshot de um único volume base.

Copiar um volume de Snapshot no SANtricity System Manager

Você pode executar um processo de cópia de volume em um volume de Snapshot ou em um volume de Snapshot de grupo de consistência.

Sobre esta tarefa

Você pode copiar um volume de Snapshot para o volume de destino da mesma forma que em uma operação normal de cópia de volume. No entanto, volumes de Snapshot não podem permanecer online durante o processo de cópia de volume.

Passos

1. Selecione o menu: storage[Snapshots].
2. Selecione a guia **Snapshot Volumes**.

   A tabela Snapshot Volumes é exibida e mostra todos os volumes de snapshot associados ao array de storage.

3. Selecione o volume de Snapshot que você deseja copiar e, em seguida, selecione **Copy Volume**.

   A caixa de diálogo Copiar Volume é exibida, solicitando que você selecione um destino.

4. Selecione o volume de destino a ser usado como destino da cópia e clique em **Concluir**.

Recrie um volume de snapshot no SANtricity System Manager

Você pode recriar um volume de snapshot ou um volume de snapshot de grupo de consistência que você desativou anteriormente. Recriar um volume de snapshot leva menos tempo do que criar um novo.

Antes de começar

- O volume de snapshot deve estar no estado Ótimo ou Desativado.
- Todos os volumes de snapshot de membros devem estar em estado Desativado antes que você possa recriar o volume de snapshot do grupo de consistência de snapshots.

Sobre esta tarefa

Não é possível recriar um volume de snapshot de um membro individual; você só pode recriar o volume de snapshot do grupo de consistência de snapshot geral.

> Se o volume de snapshot ou o volume de snapshot do grupo de consistência de snapshot fizer parte de uma relação de cópia online, você não poderá executar a opção de re-criar no volume.

Passos

1. Selecione o menu: storage[Snapshots].
2. Selecione a guia **Snapshot Volumes**.

   A tabela Snapshot Volumes é exibida e mostra todos os volumes de snapshot associados ao array de storage.

3. Selecione o volume de Snapshot que deseja re-criar e, em seguida, selecione **Tarefas incomuns › Recriar**.

   A caixa de diálogo Recriar Snapshot Volume é exibida.

4. Selecione uma das seguintes opções:
   - **Uma imagem Snapshot existente criada a partir do volume <name>**

     Selecione esta opção para indicar uma imagem de Snapshot existente a partir da qual o volume de

Snapshot será recriado.

- **Uma nova (instantânea) imagem Snapshot do volume <name>**

  Selecione esta opção para criar uma nova imagem de Snapshot a partir da qual o volume de Snapshot será recriado.

5. Clique em **Recriar**.

Resultados

System Manager executa as seguintes ações:

- Exclui todos os `write` dados em qualquer volume de repositório de Snapshot associado.
- Os parâmetros de volume de Snapshot ou de volume de grupo de consistência de Snapshot permanecem os mesmos que os parâmetros de volume desativados anteriormente.
- Mantém os nomes originais para o volume de snapshot ou o volume de snapshot do grupo de consistência de snapshot.

Desative um volume de Snapshot no SANtricity System Manager

Você pode desativar um volume de Snapshot ou um volume de Snapshot em um grupo de consistência de Snapshot quando não precisar mais dele ou quiser interromper temporariamente o uso.

Sobre esta tarefa

Use a opção Disable se uma destas condições se aplicar:

- Você concluiu o uso do volume de snapshot ou do volume de snapshot do grupo de consistência de snapshot por enquanto.
- Você pretende recriar o volume de snapshot ou o volume de snapshot do grupo de consistência de snapshot (designado como leitura e gravação) posteriormente e deseja manter a capacidade reservada associada para não precisar criá-la novamente.
- Você deseja aumentar o desempenho do array de storage interrompendo a atividade de gravação em um volume de Snapshot de leitura/gravação.

Se o volume de snapshot ou o volume de snapshot do grupo de consistência de snapshots estiver designado como leitura/gravação, esta opção também permite interromper qualquer atividade de gravação adicional no volume de capacidade reservada associado. Se você decidir recriar o volume de snapshot ou o volume de snapshot do grupo de consistência de snapshots, deverá escolher uma imagem de snapshot do mesmo volume base.

Se o volume de Snapshot ou o volume de Snapshot do grupo de consistência de Snapshot fizer parte de uma relação de cópia online, você não poderá executar a opção Desabilitar no volume.

Passos

1. Selecione o menu: storage[Snapshots].
2. Selecione a guia **Snapshot Volumes**.

   System Manager exibe todos os volumes de snapshot associados ao array de storage.

3. Selecione o volume de Snapshot que deseja desativar e, em seguida, selecione **Tarefas incomuns › Desativar**.
4. Confirme que deseja realizar a operação e, em seguida, clique em **Desativar**.

Resultados

- O volume de Snapshot permanece associado ao seu volume base.
- O volume de Snapshot mantém seu World Wide Name (WWN).
- Se for leitura e gravação, o volume de snapshot mantém sua capacidade reservada associada.
- O volume de snapshot mantém todas as atribuições de host e acesso. No entanto, solicitações de leitura e gravação falham.
- O volume de snapshot perde sua associação com sua imagem de snapshot.

Excluir um volume de Snapshot no SANtricity System Manager

Você pode excluir um volume de snapshot ou um volume de snapshot de grupo de consistência que não seja mais necessário para backup ou teste de aplicativos de software.

Você também pode especificar se deseja excluir o volume de capacidade reservada de snapshot associado a um `read-write`snapshot volume ou manter 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 de Snapshot associado ou volume de Snapshot de grupo de consistência associado. Não é possível excluir um volume de Snapshot que esteja em uma cópia de volume com o status **In Progress**.

Passos

1. Selecione o menu: storage[Snapshots].
2. Selecione a guia **Snapshot Volumes**.

   System Manager exibe todos os volumes de snapshot associados ao array de storage.

3. Selecione o volume de snapshot que você deseja excluir e, em seguida, selecione **Uncommon Tasks › Delete**.
4. Confirme que deseja realizar a operação e clique em **Delete**.

Resultados

System Manager executa as seguintes ações:

- Exclui todos os volumes de snapshot de membros (para um volume de snapshot de grupo de consistência de snapshot).
- Remove todas as atribuições de host associadas.

Perguntas frequentes sobre Snapshots para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

Por que não vejo todos os meus volumes, hosts ou clusters de hosts?

Volumes de Snapshot com um volume base habilitado para Data Assurance (DA) não podem ser atribuídos a um host que não seja compatível com DA. Você deve desabilitar DA no volume base antes que um volume de Snapshot possa ser atribuído a um host que não seja compatível com DA.

Considere as seguintes diretrizes para o host ao qual você está atribuindo o volume de Snapshot:

- Um host não é compatível com DA se estiver conectado ao array de storage por meio de uma interface de I/O que não seja compatível com DA.
- Um cluster de hosts não é compatível com DA se tiver pelo menos um host membro que não seja compatível com DA.

> Não é possível desativar o DA em um volume associado a snapshots (grupos de consistência, grupos de snapshot, imagens de snapshot e volumes de snapshot), cópias de volume e espelhamentos. Toda a capacidade reservada e os objetos de snapshot associados devem ser excluídos antes que o DA possa ser desativado no volume base.

O que é uma imagem Snapshot?

Uma imagem de Snapshot é uma cópia lógica do conteúdo de um volume, capturada em um ponto no tempo. Imagens de Snapshot utilizam espaço mínimo de storage.

Os dados da imagem Snapshot são armazenados da seguinte forma:

- Quando uma imagem de snapshot é criada, ela corresponde exatamente ao volume base. Após a captura do snapshot, quando ocorre a primeira solicitação de gravação 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 snapshots subsequentes incluem apenas os blocos de dados que foram alterados desde que a primeira imagem do snapshot foi criada. Cada operação copy-on-write subsequente salva os dados originais que estão prestes a ser sobrescritos no volume base na capacidade reservada para o snapshot antes que os novos dados sejam gravados no volume base.

Por que usar Snapshot?

Você pode usar snapshots para se proteger e permitir a recuperação contra perda ou corrupção acidental ou maliciosa de dados.

Selecione um volume base ou um grupo de volumes base, denominado grupo de consistência de Snapshot, e então capture imagens de Snapshot de uma ou mais das seguintes maneiras:

- Você pode criar uma imagem de Snapshot de um único volume base ou um grupo de consistência de Snapshot composto por vários volumes base.
- Você pode tirar snapshots manualmente ou criar um agendamento para um volume base ou grupo de consistência de snapshot para capturar automaticamente imagens de snapshot periódicas.
- Você pode criar um volume de Snapshot acessível pelo host a partir de uma imagem de Snapshot.
- Você pode realizar uma operação de reverter para restaurar uma imagem de Snapshot.

O sistema retém várias imagens de Snapshot como pontos de restauração que você pode usar para reverter para conjuntos de dados válidos em pontos específicos no tempo. A capacidade de reverter oferece proteção contra exclusão acidental de dados e corrupção de dados.

Que tipos de volumes podem ser usados para Snapshots?

Volumes padrão e volumes finos são os únicos tipos de volumes que podem ser usados para armazenar imagens de Snapshot. Volumes não padrão não podem ser usados. O volume base pode residir em um pool ou grupo de volume.

Por que eu criaria um grupo de consistência de Snapshot?

Você cria um grupo de consistência de snapshot quando deseja garantir que as imagens de snapshot sejam criadas 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 um grupo de consistência de snapshot para coletar snapshots coordenados de todos os volumes e usá-los para restaurar todo o banco de dados.

Os volumes incluídos em um grupo de consistência de Snapshot são chamados de *volumes membros*.

Você pode executar as seguintes operações de snapshot em um grupo de consistência de snapshot:

- Crie uma imagem de Snapshot de um grupo de consistência de Snapshot para obter imagens simultâneas dos volumes membros.
- Crie um agendamento para o grupo de consistência de Snapshot para capturar automaticamente imagens simultâneas periódicas dos volumes membros.
- Crie um volume de Snapshot acessível ao host de uma imagem de grupo de consistência de Snapshot.
- Execute uma operação de reverter para um grupo de consistência de Snapshot.

O que é um volume de Snapshot e quando ele precisa de capacidade reservada?

Um volume de snapshot permite que o host acesse os dados na imagem do snapshot. O volume de snapshot contém sua própria capacidade reservada, que salva quaisquer modificações no volume base sem afetar a imagem original do snapshot. As imagens de snapshot não são acessíveis para leitura ou gravação pelos hosts. Se você deseja ler ou gravar dados no 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 de Snapshot determina se ele utiliza capacidade reservada.

- **Somente leitura** — Um volume de snapshot criado como somente leitura fornece a um aplicativo host acesso de leitura a uma cópia dos dados contidos na imagem do snapshot. Um volume de snapshot somente leitura não utiliza capacidade reservada.
- **Leitura e gravação** — Um volume de Snapshot criado como leitura e gravação permite que você faça alterações no volume de Snapshot sem afetar a imagem de Snapshot referenciada. Um volume de Snapshot de leitura e gravação usa a capacidade reservada para armazenar essas alterações. Você pode converter um volume de Snapshot somente leitura para leitura e gravação a qualquer momento.

O que é um grupo de Snapshot?

Um grupo de Snapshot é uma coleção de imagens de Snapshot de ponto no tempo de um único volume base associado.

System Manager organiza as imagens de Snapshot em *grupos de Snapshot*. 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 tira um Snapshot de um volume base que ainda não possui um grupo de Snapshot, System Manager cria automaticamente um grupo de Snapshot. Isso cria capacidade reservada para o volume base que é usada para armazenar as imagens de Snapshot subsequentes.
- Sempre que você cria um agendamento de snapshot para um volume base, System Manager cria automaticamente um grupo de snapshot.

Por que eu desativaria um volume de Snapshot?

Você desativa um volume de Snapshot quando deseja atribuir um volume de Snapshot diferente à imagem do Snapshot. Você pode reservar o volume de Snapshot desativado para uso posterior.

Se você não precisar mais do volume de Snapshot ou do volume de Snapshot do grupo de consistência e não pretende recriá-lo posteriormente, deverá excluir o volume em vez de desativá-lo.

O que é o estado Disabled?

Um volume de Snapshot com status Desativado não está atualmente atribuído a uma imagem de Snapshot. Para ativar o volume de Snapshot, você deve usar a operação de re-create para atribuir uma nova imagem de Snapshot ao volume de Snapshot desativado.

As características do volume de Snapshot são definidas pela imagem de Snapshot atribuída a ele. A atividade de leitura e gravação é suspensa em um volume de Snapshot com status Disabled.

Por que eu suspenderia um agendamento de Snapshot?

Quando um agendamento é suspenso, a criação das imagens de Snapshot agendadas não ocorre. Você pode pausar um agendamento de Snapshot para economizar espaço de storage e, em seguida, retomar os Snapshots agendados posteriormente.

Se você não precisar do agendamento de Snapshot, deverá excluí-lo em vez de suspendê-lo.

Espelhamento

Visão geral

Saiba mais sobre espelhamento assíncrono no software SANtricity

O recurso de espelhamento assíncrono fornece um mecanismo em nível de controlador, baseado em firmware, para replicação de dados entre um array de storage local e um array de storage remoto.

O que é espelhamento assíncrono?

O espelhamento assíncrono captura o estado do volume primário em um determinado momento e copia apenas os dados que foram alterados desde a última captura de imagem. O site primário pode ser atualizado imediatamente e o site secundário pode ser atualizado conforme a largura de banda permitir. As informações são armazenadas em cache e enviadas posteriormente, à medida que os recursos de rede se tornam disponíveis.

O espelhamento assíncrono é criado por volume, mas gerenciado em nível de grupo, permitindo associar um volume espelhado remoto distinto a qualquer volume primário em um determinado array de storage. Esse tipo de espelhamento é ideal para atender à demanda por operações ininterruptas e, em geral, é muito mais

eficiente em termos de rede para processos periódicos.

Saiba mais:

- "Como funciona o espelhamento assíncrono"
- "Terminologia de espelhamento assíncrono"
- "Status do espelho assíncrono"
- "Propriedade do volume"
- "Mudança de função de um grupo de consistência de espelhamento"

Como faço para configurar espelhamento assíncrono?

Você deve usar a interface do Unified Manager para realizar a configuração inicial de espelhamento entre os arrays. Depois de configurado, você pode gerenciar pares espelhados e grupos de consistência no System Manager.

Saiba mais:

- "Requisitos para usar 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 espelhamento"
- "O que você precisa saber antes de criar um par espelhado"
- "Como o espelhamento assíncrono difere do espelhamento síncrono"

Saiba mais sobre espelhamento síncrono no software SANtricity

O recurso de espelhamento síncrono fornece replicação de dados online e em tempo real entre arrays de storage a uma distância remota.

Este recurso não está disponível nos sistemas de storage EF600/EF600C ou EF300/EF300C.

O que é espelhamento síncrono?

O espelhamento síncrono replica volumes de dados em tempo real para garantir disponibilidade contínua. Os controladores do array de storage gerenciam a operação de espelhamento, que é transparente para as máquinas host e aplicativos de software.

Esse tipo de espelhamento é ideal para continuidade dos negócios, como recuperação de desastres.

Saiba mais:

- "Como o espelhamento síncrono funciona"
- "Terminologia de espelhamento síncrono"

- "Status de espelhamento síncrono"
- "Propriedade do volume"
- "Mudança de papéis entre volumes em um par espelhado"

Como faço para configurar espelhamento síncrono?

Você deve usar a interface do Unified Manager para realizar a configuração inicial de espelhamento entre os arrays. Uma vez configurado, você pode gerenciar os pares espelhados no System Manager.

Saiba mais:

- "Requisitos para usar 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 no SANtricity System Manager

O espelhamento assíncrono copia volumes de dados sob demanda ou de acordo com um cronograma, o que minimiza ou evita a interrupção que pode resultar de corrupção de dados ou perda.

O espelhamento assíncrono captura o estado do volume primário em um determinado momento e copia apenas os dados que foram alterados desde a última captura de imagem. O site primário pode ser atualizado imediatamente e o site secundário pode ser atualizado conforme a largura de banda permitir. As informações são armazenadas em cache e enviadas posteriormente, à medida que os recursos de rede se tornam disponíveis.

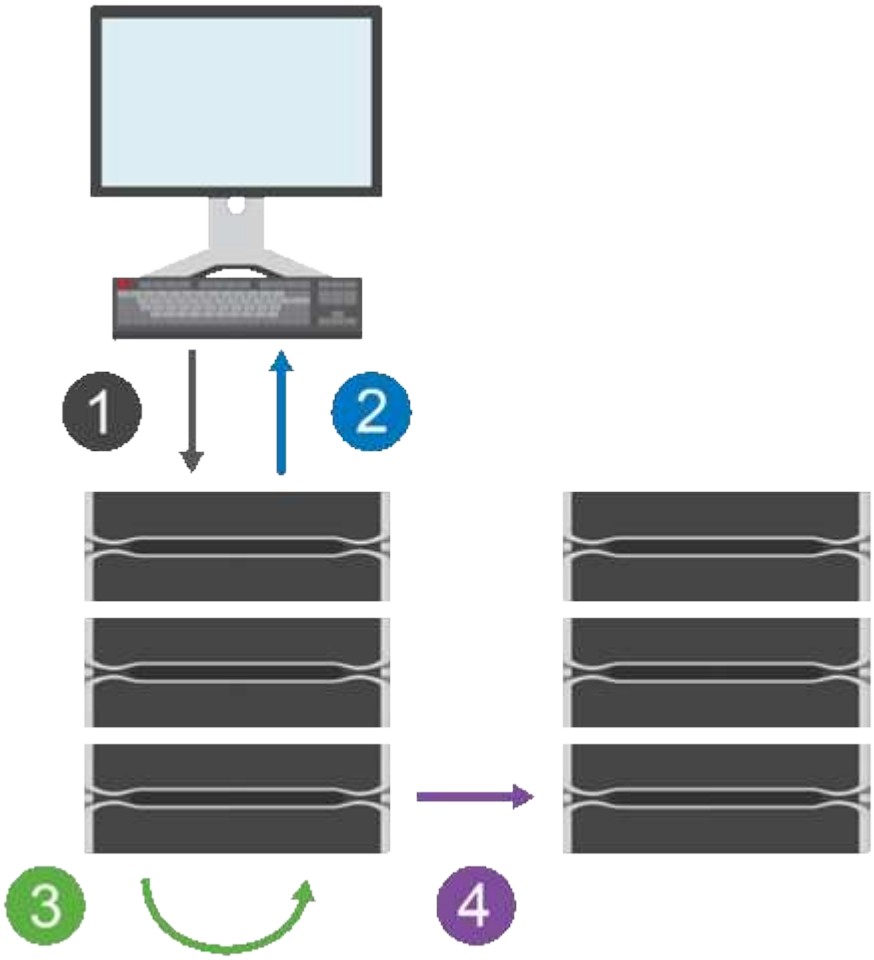
Esse tipo de espelhamento é ideal para atender à demanda por operações ininterruptas e, em geral, é muito mais eficiente em termos de rede para processos periódicos, como backup e arquivamento. Os motivos para usar espelhamento assíncrono incluem o seguinte:

- Consolidação de backup remoto.
- Proteja contra desastres locais ou de grande escala.
- Desenvolvimento e teste de aplicações em uma imagem pontual de dados ativos.

Sessão de espelhamento assíncrono

O espelhamento assíncrono captura o estado do volume primário em um determinado momento 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 permitir. As informações são armazenadas em cache e enviadas posteriormente, à medida que os recursos de rede se tornam disponíveis.

Existem quatro etapas principais em uma sessão de espelhamento assíncrono ativa.



1. A operação de gravação ocorre primeiro no array de storage do volume primário.
2. O status da operação é retornado ao host.
3. Todas as alterações no volume primário são registradas e monitoradas.
4. Todas as alterações são enviadas para o array de storage do volume secundário como um processo em segundo plano.

Esses passos são repetidos de acordo com os intervalos de sincronização definidos ou os passos podem ser repetidos manualmente se nenhum intervalo for definido.

O espelhamento assíncrono transfere dados para o local remoto apenas em intervalos definidos, de modo que a E/S local não é afetada significativamente 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 operar em distâncias maiores entre os sistemas de armazenamento local e remoto.

Os arrays de storage devem ter uma versão mínima de firmware de 7.84. (Cada um pode executar versões diferentes do sistema operacional.)

Grupos de consistência de espelhamento e pares espelhados

Você cria um grupo de consistência de espelhamento para estabelecer a relação de espelhamento entre o array de storage local e o array de storage remoto. A relação de espelhamento assíncrono consiste em um

par espelhado: um volume primário em um array de storage e um volume secundário em outro array de storage.

O array de storage que contém o volume primário geralmente está localizado no site primário e atende aos hosts ativos. O array de storage que contém o volume secundário geralmente está localizado em um site secundário e armazena uma réplica dos dados. O volume secundário normalmente contém uma cópia de backup dos dados e é usado para recuperação de desastres.

Configurações 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 espelhamento, 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 prioridade de sincronização e a política de ressincronização para concluir a operação de ressincronização após uma interrupção de comunicação.

Os volumes primário e secundário em um par espelhado podem ficar dessincronizados quando o array de storage do volume primário não consegue gravar dados no volume secundário. Essa condição pode ser causada pelos seguintes problemas:

- Problemas de rede entre os arrays de storage local e remoto.
- Um volume secundário com falha.
- Sincronização sendo suspensa manualmente no par espelhado.
- Conflito de função do grupo de espelhamento.

Você pode sincronizar os dados no array de storage no local remoto manualmente ou automaticamente.

Capacidade reservada e espelhamento assíncrono

A capacidade reservada é usada para monitorar as diferenças entre o volume primário e o volume secundário quando a sincronização não está ocorrendo. Ela 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 habilitar e configurar o espelhamento entre dois arrays, você deve usar a interface Unified Manager. Depois que o espelhamento estiver habilitado, você pode gerenciar os pares espelhados e as configurações de sincronização no System Manager.

Saiba mais sobre a terminologia de espelhamento assíncrono no software SANtricity

Aprenda como os termos de espelhamento assíncrono se aplicam ao seu array de storage.

Termo	Descrição
Array de storage local	O array de storage local é o array de storage sobre o qual você está agindo. Quando você vê **Primário** na coluna Função Local, isso indica que o array de storage contém o volume que detém a função primária na relação de espelhamento. Quando você vê **Secundário** na coluna Função Local, isso indica que o array de storage contém o volume que detém a função secundária na relação de espelhamento.
Grupo de consistência	Um grupo de consistência de espelhamento é um contêiner para um ou mais pares espelhados. Para operações de espelhamento assíncrono, você deve criar um grupo de consistência de espelhamento.
Par espelhado	Um par espelhado é composto por dois volumes, um volume primário e um volume secundário. No espelhamento assíncrono, um par espelhado sempre pertence a um grupo de consistência de espelhamento. As operações de gravação são realizadas primeiro no volume primário e depois replicadas para o volume secundário. Cada par espelhado em um grupo de consistência de espelhamento compartilha as mesmas configurações de sincronização.
Volume primário	O volume primário de um par espelhado é o volume de origem a ser espelhado.
Array de storage remoto	O array de storage remoto é geralmente designado como o site secundário, que normalmente contém uma réplica dos dados em uma configuração de espelhamento.
Capacidade reservada	A capacidade reservada é a capacidade física alocada que é usada para qualquer operação de serviço de cópia e objeto de armazenamento. Ela não é diretamente legível pelo host.
Mudança de função	A mudança de função consiste em atribuir a função principal ao volume secundário e vice-versa.
Volume secundário	O volume secundário de um par espelhado geralmente está localizado em um site secundário e contém uma réplica dos dados.
Sincronização	A sincronização ocorre na sincronização inicial entre o array de storage local e o array de storage remoto. A sincronização também ocorre quando os volumes primário e secundário ficam dessincronizados após uma interrupção na comunicação. Quando o link de comunicação volta a funcionar, quaisquer dados não replicados são sincronizados com o array de storage do volume secundário.

Espelhe um volume de forma assíncrona no software SANtricity

Você configura o espelhamento assíncrono usando o seguinte fluxo de trabalho.

1. Realize a configuração inicial no Unified Manager:

a. Selecione o array de storage local como a origem para a transferência de dados.

b. Crie ou selecione um grupo de consistência de espelhamento existente, que é um contêiner para o volume primário no array de storage local e o volume secundário no array de storage remoto. Os volumes primário e secundário são chamados de "par espelhado". Se você estiver criando o grupo de consistência de espelhamento pela primeira vez, especifique se deseja realizar sincronizações manuais ou agendadas.

c. Selecione um volume primário do array de storage local e, em seguida, determine sua capacidade reservada. A capacidade reservada é a capacidade física alocada para ser usada na operação de cópia.

d. Selecione um array de storage remoto como destino da transferência, um volume secundário e, em seguida, determine sua capacidade reservada.

e. Inicie a transferência inicial de dados do volume primário para o volume secundário. Dependendo do tamanho do volume, essa transferência inicial pode levar 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 será "Ótimo".

3. **Opcional:** você pode reagendar ou executar manualmente as transferências de dados subsequentes no System Manager. Somente novos e blocos 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. Há impacto mínimo na taxa de transferência de escrita e na latência.

Requisitos para usar espelhamento assíncrono no software SANtricity

Se você planeja usar espelhamento assíncrono, tenha em mente os seguintes requisitos.

Unified Manager

Para habilitar e configurar o espelhamento entre dois arrays, você deve usar a interface Unified Manager. Unified Manager é instalado em um sistema host juntamente com o Web Services Proxy.

- O serviço Web Services Proxy deve estar em execução.
- Unified Manager deve estar sendo executado em seu host local por meio de uma conexão HTTPS.
- Unified Manager deve exibir certificados SSL válidos para o array de storage. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando Unified Manager e navegando até **Certificate › Certificate Management**.

Array de storage

- Você precisa ter dois arrays de storage.
- Cada array de storage deve ter dois controladores.
- Os dois arrays de storage devem ser detectados no Unified Manager.
- Cada controlador, tanto no array primário quanto no array secundário, deve ter uma porta de gerenciamento Ethernet configurada e deve estar conectado à sua rede.

- Os arrays de storage possuem uma versão mínima de firmware de 7.84. (Cada um deles pode executar diferentes versões de sistema operacional.)
- Você deve saber a senha dos arrays de storage local e remoto.
- Você precisa ter capacidade livre suficiente no array de storage remoto para criar um volume secundário igual ou maior que o volume primário que você deseja espelhar.
- Seus arrays de storage locais e remotos estão conectados por meio de uma estrutura Fibre Channel ou 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 espelhamento, o administrador pode selecionar FC ou iSCSI para esse grupo se ambos estiverem conectados ao array de storage remoto. Não há failover de um tipo de canal para o outro.

O espelhamento assíncrono usa as portas de E/S do lado do host do array de storage para transmitir dados espelhados do lado primário para o lado secundário.

- **Espelhamento através de uma interface Fibre Channel (FC)**

  Cada controlador do array de storage dedica sua porta host FC de número mais alto às operações de espelhamento.

  Se o controlador tiver tanto portas FC básicas quanto portas FC de placa de interface de host (HIC), a porta de número mais alto estará em uma HIC. Qualquer host conectado à porta dedicada será desconectado e nenhuma solicitação de login de host será 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 de serviço de diretório e serviço de nomes. Em particular, FC-AL e ponto a ponto não são suportados como opções de conectividade entre os controladores que participam de relações de espelhamento.

- **Espelhamento através de uma interface iSCSI**

  Ao contrário do FC, iSCSI não requer uma porta dedicada. Quando o espelhamento assíncrono é usado em ambientes iSCSI, não é necessário dedicar nenhuma das portas iSCSI front-end do array de storage para uso com espelhamento assíncrono; essas portas são compartilhadas tanto para o tráfego de espelhamento assíncrono quanto para as conexões de E/S do host para o 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 sucesso uma conexão iSCSI é usada para toda a comunicação subsequente com esse array de storage. Se a comunicação falhar, uma nova sessão é tentada usando todas as portas disponíveis.

  As portas iSCSI são configuradas no nível do array, porta por porta. A comunicação entre controladores para mensagens de configuração e transferência de dados utiliza as configurações globais, incluindo as configurações para:

  - VLAN: os sistemas local e remoto devem ter a mesma configuração de VLAN para comunicar
  - Porta de escuta iSCSI
  - Quadros jumbo

- Prioridade Ethernet

> A comunicação entre controladores iSCSI deve usar uma porta de conexão do host e não a porta Ethernet de gerenciamento.

O espelhamento assíncrono usa as portas de E/S do host do array de storage para transmitir dados espelhados do lado primário para o lado secundário. Como o espelhamento assíncrono é destinado a redes de maior latência e menor custo, conexões iSCSI (e, portanto, baseadas em TCP/IP) são uma boa opção para ele. Quando o espelhamento assíncrono é usado em ambientes iSCSI, não é necessário dedicar nenhuma das portas iSCSI front-end do array de storage para uso com espelhamento assíncrono; essas portas são compartilhadas tanto para o tráfego de espelhamento assíncrono quanto para as conexões de E/S do host para o array.

> O E4000 não suporta espelhamento assíncrono ao usar o protocolo iSCSI.

Candidatos a volume espelhado

- Nível RAID, parâmetros de armazenamento em cache e 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 de bandeja, tamanho de 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 espelhamento.
- Os volumes candidatos devem compartilhar as mesmas capacidades de segurança de dados.
  - Se o volume primário for compatível com FIPS, o volume secundário deve ser compatível com FIPS.
  - Se o volume primário for compatível com FDE, o volume secundário deve ser compatível com FDE.
  - Se o volume primário não estiver usando Drive Security, o volume secundário não deve estar usando 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 suportada.
- Os volumes primário e secundário não devem ter Resource Partitioning ativado.

Capacidade reservada

- É necessário um volume de capacidade reservada para um volume primário e para um volume secundário em um par espelhado para registrar informações de gravação para recuperação de reinicializações do controlador e outras interrupções temporárias.
- Como tanto o volume primário quanto o volume secundário em um par espelhado exigem capacidade reservada adicional, você deve garantir que haja capacidade livre disponível em ambos os storage arrays na relação de espelhamento.
- O volume de capacidade reservado deve compartilhar o mesmo tipo de unidade que seus volumes de espelhamento associados.
  - Se o volume de capacidade reservada for criado em unidades NVMe, seus volumes espelhados também devem ser criados em 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 recursos de segurança, o volume primário e o volume secundário devem ter configurações de segurança compatíveis. Essa restrição não é aplicada; portanto, você deve verificá-la por conta própria.
- Se você estiver usando unidades com recursos de segurança, o volume primário e o volume secundário devem usar o mesmo tipo de unidade. Essa restrição não é obrigatória; portanto, você deve verificar por conta própria.
- Se você estiver usando Data Assurance (DA), o volume primário e o volume secundário devem ter as mesmas configurações de DA.

Visualizar o status do espelhamento assíncrono no SANtricity System Manager

O status do espelho define o estado dos grupos de consistência do espelho e dos pares de volumes espelhados.

Status para grupos de consistência de mirror

Status	Descrição
Sincronizando (sincronização inicial)	O progresso da sincronização inicial de dados que foi concluída entre os pares de volumes espelhados. Durante uma sincronização inicial, os volumes podem transitar para os seguintes estados: Degraded/Failed/Optimal/Unknown.
Sincronizando (sincronização por intervalo)	O progresso da sincronização periódica de dados que foi concluída entre os pares de volumes espelhados.
Sistema suspenso	Sincronização de dados suspensa pelo sistema de storage em todos os pares espelhados no nível do grupo de consistência de espelhamento. Pelo menos um par espelhado no grupo de consistência de espelhamento está em estado Parado ou Falha.
Usuário suspenso	Sincronização de dados suspensa pelo usuário em todos os pares espelhados no nível do grupo de consistência de espelhamento. Esse estado ajuda a reduzir qualquer impacto no desempenho do aplicativo host que possa ocorrer enquanto quaisquer dados alterados no array de storage local são copiados para o array de storage remoto.
Pausado	O processo de sincronização de dados foi temporariamente interrompido devido a um erro ao acessar o array de storage remoto.

Status	Descrição
Órfão	Um volume de par espelhado órfão existe quando um volume membro em um grupo de espelhamento de consistência foi removido em um lado do grupo de espelhamento de consistência (seja o lado primário ou o lado secundário), mas não no outro lado. Volumes de pares espelhados órfãos são detectados quando a comunicação entre arrays é restaurada e os dois lados da configuração de espelhamento reconciliam os parâmetros de espelhamento. Você pode remover um par espelhado para corrigir um estado de par espelhado órfão.
Alteração de função pendente/em andamento	Uma mudança de função entre os grupos de consistência de espelhamento está pendente ou em andamento. A inversão de papéis (para um papel primário ou secundário) afeta todos os pares espelhados assíncronos dentro do grupo de consistência de espelhamento selecionado. Você pode cancelar uma alteração de função pendente, mas não uma alteração de função em andamento.
Conflito de função	Ocorreu um conflito de funções entre grupos de consistência de espelhamento devido a um problema de comunicação entre o array de storage local e o array de storage remoto durante uma operação de mudança de função. Quando o problema de comunicação for resolvido, ocorrerá um Role Conflict. Use o Recovery Guru para recuperar desse erro. Uma promoção forçada não é permitida ao resolver um conflito de funções.

Status dos pares espelhados

O status de um par espelhado indica se os dados no volume primário e no volume secundário estão sincronizados.

Status	Descrição
Sincronizando	O progresso da sincronização inicial ou periódica de dados que foi concluída entre os pares espelhados. Existem dois tipos de sincronização: sincronização inicial e sincronização periódica. O progresso da sincronização inicial também é exibido na caixa de diálogo Long Running Operations.
Ideal	Os volumes no par espelhado estão sincronizados, o que indica que a conexão entre os arrays de storage está operacional e que cada volume está na condição de funcionamento desejada.

Status	Descrição
Incompleto	O par espelhado assíncrono está incompleto no array de storage remoto porque a sequência de criação do par espelhado foi iniciada em um array de storage que não é compatível com System Manager e o par espelhado não foi concluído no volume secundário. O processo de criação de um par espelhado é concluído quando um volume é adicionado ao grupo de consistência de espelhamento no array de storage remoto. Esse volume se torna o volume secundário no par espelhado assíncrono. O par espelhado é concluído automaticamente se o array de storage remoto for gerenciado pelo System Manager.
Falha	A operação de espelhamento assíncrono não pode funcionar normalmente devido a uma falha nos volumes primários, volumes secundários ou na capacidade reservada do espelho.
Órfão	Um volume de par espelhado órfão existe quando um volume membro em um grupo de espelhamento de consistência foi removido em um lado do grupo de espelhamento de consistência (seja o lado primário ou o lado secundário), mas não no outro lado. Volumes de pares espelhados órfãos são detectados quando a comunicação é restaurada entre os dois arrays de storage e os dois lados da configuração de espelhamento reconciliam os parâmetros de espelhamento. Você pode remover um par espelhado para corrigir um estado de par espelhado órfão.
Parado	O par espelhado está em estado Parado porque o grupo de consistência de espelhamento está em estado de suspensão do sistema.

Saiba mais sobre propriedade de volume no espelhamento assíncrono no software SANtricity

Você pode alterar o proprietário preferencial do controlador em um par espelhado.

Se o volume primário do par espelhado pertencer ao controlador A, então o volume secundário também será de propriedade do controlador A do array de storage remoto. Alterar o proprietário do volume primário alterará automaticamente o proprietário do volume secundário para garantir que ambos os volumes pertençam ao mesmo controlador. As alterações de propriedade atuais no lado primário se propagam automaticamente para as alterações de propriedade atuais correspondentes no lado secundário.

Por exemplo, um volume primário pertence ao controlador A, e então você altera o proprietário do controlador para o controlador B. Nesse caso, a próxima gravação remota altera o proprietário do controlador do volume secundário do controlador A para B. Como as alterações de propriedade do controlador no lado secundário são controladas pelo lado primário, elas não exigem nenhuma intervenção especial do administrador de storage.

Reinicializações do controlador

Uma reinicialização do controlador causa uma alteração na propriedade do volume no lado primário do

controlador proprietário preferencial para o controlador alternativo no array de storage.

Às vezes, uma gravação remota é interrompida por uma reinicialização do controlador ou um ciclo de energia do array de storage antes que possa ser gravada no volume secundário. Nesse caso, o controlador não precisa realizar uma sincronização completa do par espelhado.

Quando uma gravação remota é interrompida durante uma reinicialização do controlador, o novo proprietário do controlador no lado primário lê as informações armazenadas em um arquivo de log no volume de capacidade reservada do proprietário do controlador preferencial. O novo proprietário do controlador então copia os blocos de dados afetados do volume primário para o volume secundário, eliminando a necessidade de uma sincronização completa dos volumes espelhados.

Alterar funções do grupo de consistência de espelhamento no software SANtricity

Você pode alterar a função entre pares espelhados em um grupo de consistência de espelhamento. Você pode fazer isso rebaixando o grupo de consistência de espelhamento primário para a função secundária ou promovendo o grupo de consistência de espelhamento secundário para a função primária.

Analise as seguintes informações sobre a operação de alteração de função:

- A alteração de função afeta todos os pares espelhados dentro do grupo de consistência de espelhamento selecionado.
- Quando um grupo de consistência de espelhamento é rebaixado para a função secundária, todos os pares espelhados dentro desse grupo de consistência de espelhamento também são rebaixados para a função secundária e vice-versa.
- Quando o grupo de consistência de espelhamento primário é rebaixado para a função secundária, os hosts que foram atribuídos aos volumes membros desse grupo não têm mais acesso de gravação a eles.
- Quando um grupo de consistência de espelhamento é promovido à função primária, qualquer host que esteja acessando os volumes membros desse grupo agora poderá gravar neles.
- Se o array de storage local não conseguir se comunicar com o array de storage remoto, você pode forçar a mudança de função no array de storage local.

Forçar mudança de função

Você pode forçar uma mudança de função entre grupos de consistência de espelhamento quando um problema de comunicação entre o array de storage local e o array de storage remoto estiver impedindo a promoção dos volumes membros dentro do grupo de consistência de espelhamento secundário ou o rebaixamento dos volumes membros dentro do grupo de consistência de espelhamento primário.

Você pode forçar o grupo de consistência de espelhamento no lado secundário a fazer a transição para a função primária. Em seguida, o host de recuperação poderá acessar os volumes de membros recém-promovidos dentro desse grupo de consistência de espelhamento, e as operações de negócios podem continuar.

Quando uma promoção forçada é permitida e quando não é permitida?

A promoção forçada de um grupo de consistência de espelhamento só é permitida se todos os volumes membros do grupo de consistência de espelhamento tiverem sido sincronizados e possuírem pontos de recuperação consistentes.

A promoção forçada de um grupo de consistência de espelhamento não é permitida nas seguintes condições:

- Qualquer um dos volumes membros de um grupo de consistência de espelhamento está em processo de sincronização inicial.
- Qualquer um dos volumes membros de um grupo de consistência de espelhamento não possui uma imagem pontual do ponto de recuperação (por exemplo, devido a um erro de capacidade reservada total).
- O grupo de consistência de espelhamento não contém volumes membros.
- O grupo de consistência de espelhamento está nos estados Falha, Alteração de função pendente ou Alteração de função em andamento, ou se algum dos volumes membros associados ou volumes de capacidade reservada estiver com falha.

Conflito de função do grupo de espelhamento

Quando um problema de comunicação entre os arrays de storage local e remoto é resolvido, ocorre uma condição de Conflito de Função de Grupo de Espelhamento. Use o Recovery Guru para recuperar desse erro. Uma promoção forçada não é permitida ao resolver um conflito de função dupla.

Para evitar a condição de conflito de função do grupo de espelhamento e as etapas de recuperação subsequentes, aguarde até que a conexão entre os arrays de storage esteja operacional para forçar a alteração de função.

Estado de mudança de função em andamento

Se dois arrays de storage em uma configuração de espelhamento se tornarem desconectados, e o lado primário de um grupo de consistência de espelhamento for forçado a ser rebaixado para a função secundária, e o lado secundário de um grupo de consistência de espelhamento for forçado a ser promovido para a função primária, então, quando a comunicação for restaurada, os grupos de consistência de espelhamento em ambos os arrays de storage serão colocados no estado de Mudança de Função em Andamento.

O sistema concluirá o processo de mudança de função transferindo os registros de alterações, resincronizando, definindo o estado do grupo de consistência de espelhamento de volta para um estado operacional normal e continuando com as sincronizações periódicas.

Conceitos de sincronização

Como o espelhamento síncrono funciona no SANtricity System Manager

Espelhamento síncrono replica volumes de dados em tempo real para garantir disponibilidade contínua.

> O espelhamento síncrono não está disponível no array de storage EF600/EF600C ou EF300/EF300C.

O espelhamento síncrono atinge um objetivo de ponto de recuperação (RPO) de zero perda de dados ao manter uma cópia dos dados importantes disponível caso ocorra um desastre em um dos dois arrays de storage. A cópia é idêntica aos dados de produção em todos os momentos porque cada vez que uma operação de gravação é feita no volume primário, uma operação de gravação é feita no volume secundário. O host não recebe uma confirmação de que a operação de gravação foi bem-sucedida até que o volume secundário seja atualizado com sucesso com as alterações feitas no volume primário.

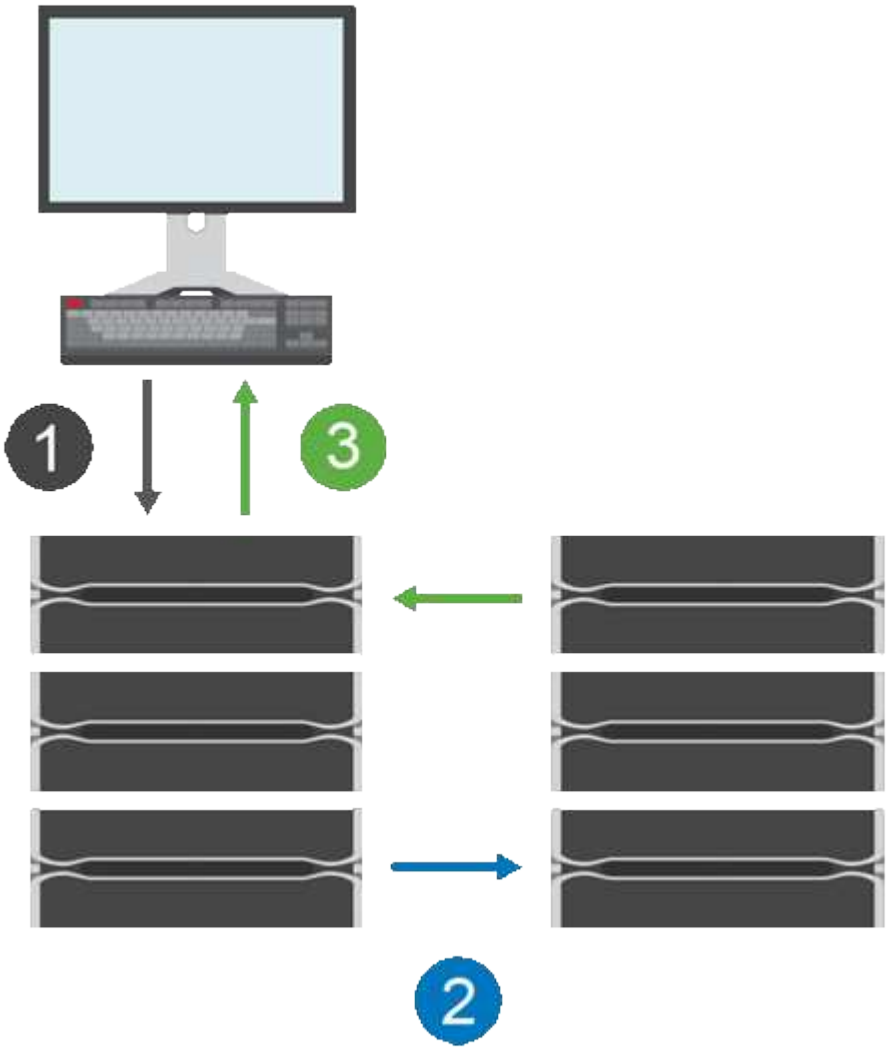
Esse tipo de espelhamento é ideal para continuidade dos negócios, como recuperação de desastres.

Relação de espelhamento síncrono

Um relacionamento de espelhamento síncrono consiste em um volume primário e um volume secundário em arrays de storage separados. O array de storage que contém o volume primário geralmente está localizado no site primário e atende aos hosts ativos. O array de storage que contém o volume secundário geralmente está localizado em um site secundário e armazena uma réplica dos dados. O volume secundário é usado se o array de storage do volume primário estiver indisponível devido, por exemplo, a uma interrupção total de energia, um incêndio ou uma falha de hardware no site primário.

Sessão de espelhamento síncrono

O processo de configuração de espelhamento síncrono envolve configurar volumes em pares. Depois de criar um par espelhado, que consiste em um volume primário em um array de storage e um volume secundário em outro array de storage, você pode iniciar o espelhamento síncrono. As etapas do espelhamento síncrono são mostradas abaixo.



1. Uma gravação é recebida do host.
2. A operação de gravação é confirmada no volume primário, propagada para o sistema remoto e, em seguida, confirmada no volume secundário.
3. O array de storage do volume primário envia uma mensagem de conclusão de E/S para o sistema host *após* ambas as operações de gravação terem sido concluídas com sucesso.

A capacidade reservada é usada para registrar informações sobre a solicitação de gravação recebida de um

host.

Quando o controlador proprietário atual 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. Depois, o controlador inicia uma operação de gravação remota para copiar os blocos de dados afetados para o volume secundário no array de storage remoto.

Como o aplicativo host precisa aguardar a gravação ocorrer no array de storage local e através da rede no array de storage remoto, é necessária uma conexão muito rápida entre o array de storage local e o array de storage remoto para manter a relação de espelhamento 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 ocorrer um desastre no local primário, como uma interrupção ou uma inundação, os dados podem ser acessados rapidamente a partir do local secundário.

O volume secundário fica indisponível para os aplicativos host enquanto a operação de espelhamento síncrono está em andamento, então, em caso de desastre no array de storage local, você pode realizar o failover para o array de storage remoto. Para realizar o failover, promova o volume secundário à função primária. Assim, o host de recuperação poderá acessar o volume recém-promovido e as operações de negócios poderão continuar.

Configurações 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 arrays de storage parar de funcionar, os hosts continuam recebendo confirmações do array de storage local, evitando a perda de acesso. Quando o link de comunicação voltar a funcionar, quaisquer dados não replicados podem ser ressincronizados automaticamente ou manualmente para o array de storage remoto.

Se os dados são resincronizados automaticamente depende da política de resincronização do par espelhado. Uma política de resincronização automática permite que o par espelhado resincronize automaticamente quando o link estiver funcionando novamente. Uma política de resincronização manual exige que você retome a sincronização manualmente após um problema de comunicação. A resincronização manual é a política recomendada.

Você pode editar as configurações de sincronização de um par espelhado somente no array de storage que contém o volume primário.

Dados não sincronizados

Os volumes primário e secundário ficam dessincronizados quando o array de storage do volume primário não consegue gravar dados no volume secundário. Isso pode ser causado pelos seguintes problemas:

- Problemas de rede entre o array de storage local e o array de storage remoto
- Um volume secundário com falha
- Sincronização sendo suspensa manualmente no par espelhado

Par espelhado órfão

Um volume de par espelhado órfão existe quando um volume membro foi removido de um lado (seja o lado primário ou o lado secundário), mas não do outro lado.

Volumes de pares espelhados órfãos são detectados quando a comunicação entre arrays é restaurada e os dois lados da configuração de espelhamento reconciliam os parâmetros de espelhamento.

Você pode remover um par espelhado para corrigir um estado de par espelhado órfão.

Configuração e gerenciamento

Para habilitar e configurar o espelhamento entre dois arrays, você deve usar a interface Unified Manager. Depois que o espelhamento estiver habilitado, você pode gerenciar os pares espelhados e as configurações de sincronização no System Manager.

Saiba mais sobre a terminologia de espelhamento síncrono no software SANtricity

Saiba como os termos de espelhamento síncrono se aplicam ao seu array de storage.

Termo	Descrição
Array de storage local	O array de storage local é o array de storage sobre o qual você está agindo. Quando você vê **Primário** na coluna Função Local, isso indica que o array de storage contém o volume que detém a função primária na relação de espelhamento. Quando você vê **Secundário** na coluna Função Local, isso indica que o array de storage 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 de ponto de recuperação (RPO)	O Recovery Point Objective (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 atual ou atrasado em relação ao volume primário.
Array de storage remoto	O array de storage remoto é geralmente designado como o site secundário, que normalmente contém uma réplica dos dados em uma configuração de espelhamento.
Capacidade reservada	A capacidade reservada é a capacidade física alocada que é usada para qualquer operação de serviço de cópia e objeto de armazenamento. Ela não é diretamente legível pelo host.

Termo	Descrição
Mudança de função	A mudança de função consiste em atribuir a função principal ao volume secundário e vice-versa.
Volume secundário	O volume secundário de um par espelhado geralmente está localizado em um site secundário e contém uma réplica dos dados.
Sincronização	A sincronização ocorre na sincronização inicial entre o array de storage local e o array de storage remoto. A sincronização também ocorre quando os volumes primário e secundário ficam dessincronizados após uma interrupção na comunicação. Quando o link de comunicação volta a funcionar, quaisquer dados não replicados são sincronizados com o array de storage do volume secundário.

Espelhe um volume de forma síncrona no software SANtricity

Você configura espelhamento síncrono usando o seguinte fluxo de trabalho.

Este recurso não está disponível nos sistemas de storage EF600/EF600C ou EF300/EF300C.

1. Realize a configuração inicial no Unified Manager:
   a. Selecione um array de storage local como origem para a transferência de dados.
   b. Selecione um volume primário do array de storage local.
   c. Selecione um array de storage remoto 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 inicial de dados do volume primário para o volume secundário. Dependendo do tamanho do volume, essa transferência inicial pode levar 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 será "Ótimo". Os dois arrays tentam permanecer sincronizados por meio 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 sites deve fornecer largura de banda suficiente.

Requisitos para usar espelhamento síncrono no software SANtricity

Se você planeja usar espelhamento síncrono, tenha em mente os seguintes requisitos.

Unified Manager

Para habilitar e configurar o espelhamento entre dois arrays, você deve usar a interface Unified Manager. Unified Manager é instalado em um sistema host juntamente com o Web Services Proxy.

- O serviço Web Services Proxy deve estar em execução.
- Unified Manager deve estar sendo executado em seu host local por meio de uma conexão HTTPS.
- Unified Manager deve exibir certificados SSL válidos para o array de storage. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando Unified Manager e navegando até **Certificate › Certificate Management**.

Array de storage

> Espelhamento síncrono não está disponível no array de storage EF300/EF300C ou EF600/EF600C.

- Você precisa ter dois arrays de storage.
- Cada array de storage deve ter dois controladores.
- Os dois arrays de storage devem ser detectados no Unified Manager.
- Cada controlador, tanto no array primário quanto no array secundário, deve ter uma porta de gerenciamento Ethernet configurada e deve estar conectado à sua rede.
- Os arrays de storage possuem uma versão mínima de firmware de 7.84. (Cada um deles pode executar diferentes versões de sistema operacional.)
- Você deve saber a senha dos arrays de storage local e remoto.
- Você precisa ter capacidade livre suficiente no array de storage remoto para criar um volume secundário igual ou maior que o volume primário que você deseja espelhar.
- Seus arrays de storage local e remoto estão conectados por meio de uma malha Fibre Channel.

Conexões suportadas

A comunicação para espelhamento síncrono é suportada apenas em controladores com portas de host Fibre Channel (FC).

O espelhamento síncrono utiliza a porta de host de número mais alto em cada controlador, tanto no array de storage local quanto no array de storage remoto. A porta 4 do adaptador de barramento de host (HBA) do controlador é normalmente reservada para a transmissão de dados do espelhamento.

Candidatos a volume espelhado

- Nível RAID, parâmetros de armazenamento em cache e 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. Eles não podem ser volumes finos ou volumes de snapshot.
- O volume secundário deve ser pelo menos tão grande quanto o volume primário.
- Somente o volume primário pode ter snapshots associados a ele e/ou ser o volume de origem ou de destino em uma operação de cópia de volume.
- Um volume pode participar de apenas um relacionamento de espelhamento.
- Há um limite para o número de volumes suportados em um determinado array de storage. Certifique-se de que o número de volumes configurados em seu array de storage seja menor que o limite suportado. Quando o espelhamento síncrono está ativo, os dois volumes de capacidade reservada que são criados são contabilizados no limite de volumes.

Capacidade reservada

- É necessária capacidade reservada para um volume primário e para um volume secundário para registrar 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 tanto o volume primário quanto o volume secundário em um par espelhado exigem capacidade reservada, você deve garantir que haja 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 recursos de segurança, o volume primário e o volume secundário devem ter configurações de segurança compatíveis. Essa restrição não é aplicada; portanto, você deve verificá-la por conta própria.
- Se você estiver usando unidades com recursos de segurança, o volume primário e o volume secundário devem usar o mesmo tipo de unidade. Essa restrição não é obrigatória; portanto, você deve verificar por conta própria.
  - Se o volume primário usar unidades com criptografia de disco completa (FDE), o volume secundário deverá usar unidades com FDE.
  - Se o volume principal usar unidades validadas pelo Federal Information Processing Standards 140-2 (FIPS), o volume secundário também deverá usar unidades validadas pelo Federal Information Processing Standards 140-2 (FIPS).
- Se você estiver usando Data Assurance (DA), o volume primário e o volume secundário devem ter as mesmas configurações de DA.

Saiba mais sobre o status do espelhamento síncrono no SANtricity System Manager

O status de um par espelhado síncrono indica se os dados no volume primário e no volume secundário estão sincronizados. O status do espelhamento é independente do status dos componentes dos volumes no par espelhado.

Este recurso não está disponível nos sistemas de storage EF600/EF600C ou EF300/EF300C.

Pares espelhados síncronos podem ter um dos seguintes status:

- **Otimizado**

  Indica que os volumes no par espelhado estão sincronizados, o que significa que a conexão de fabric entre os arrays de storage está operacional e cada volume está na condição de funcionamento desejada.

- **Sincronizando**

  Mostra o progresso da sincronização de dados entre os pares espelhados. Este status também será exibido durante a sincronização inicial.

  Após uma interrupção na ligação de comunicação, apenas os blocos alterados de dados no volume primário durante a interrupção da ligação são copiados para o volume secundário.

- **Não sincronizado**

  Indica que o array de storage do volume primário não consegue gravar dados recebidos no array remoto.

O host local pode continuar gravando no volume primário, mas as gravações remotas não ocorrem. Diversas condições podem impedir que o array de storage do volume primário grave dados recebidos no volume secundário, tais como:

  - O volume secundário não está acessível.
  - O array de storage remoto não está acessível.
  - A conexão de fabric entre os arrays de storage 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 contatar o volume secundário. Quaisquer gravações no volume primário são registradas permanentemente nos volumes de capacidade reservada do espelho.

- **Falha**

  Indica que a operação de espelhamento síncrono não pode funcionar normalmente devido a uma falha no volume primário, no volume secundário ou na capacidade reservada do espelho.

Saiba mais sobre propriedade de volume no espelhamento síncrono no software SANtricity

Você pode alterar o proprietário preferencial do controlador em um par espelhado.

Este recurso não está disponível para espelhamento síncrono no sistema de storage EF600/EF600C ou EF300/EF300C.

Se o volume primário do par espelhado pertencer ao controlador A, então o volume secundário também será de propriedade do controlador A do array de storage remoto. Alterar o proprietário do volume primário alterará automaticamente o proprietário do volume secundário para garantir que ambos os volumes pertençam ao mesmo controlador. As alterações de propriedade atuais no lado primário se propagam automaticamente para as alterações de propriedade atuais correspondentes no lado secundário.

Por exemplo, um volume primário pertence ao controlador A, e então você altera o proprietário do controlador para o controlador B. Nesse caso, a próxima gravação remota altera o proprietário do controlador do volume secundário do controlador A para B. Como as alterações de propriedade do controlador no lado secundário são controladas pelo lado primário, elas não exigem nenhuma intervenção especial do administrador de storage.

Reinicializações do controlador

Uma reinicialização do controlador causa uma alteração na propriedade do volume no lado primário do controlador proprietário preferencial para o controlador alternativo no array de storage.

Às vezes, uma gravação remota é interrompida por uma reinicialização do controlador ou um ciclo de energia do array de storage antes que possa ser gravada no volume secundário. Nesse caso, o controlador não precisa realizar uma sincronização completa do par espelhado.

Quando uma gravação remota é interrompida durante uma reinicialização do controlador, o novo proprietário do controlador no lado primário lê as informações armazenadas em um arquivo de log no volume de capacidade reservada do proprietário do controlador preferencial. O novo proprietário do controlador então copia os blocos de dados afetados do volume primário para o volume secundário, eliminando a necessidade de uma sincronização completa dos volumes espelhados.

Saiba mais sobre as alterações de função de volume em um par espelhado no SANtricity software

É possível 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 primária.

> O espelhamento síncrono não está disponível no sistema de storage EF600/EF600C ou EF300/EF300C.

Analise as seguintes informações sobre a operação de alteração de função:

- Quando um volume primário é rebaixado para a função secundária, o volume secundário nesse par espelhado é promovido à função primária e vice-versa.
- Quando o volume primário é rebaixado para a função secundária, hosts que foram atribuídos a esse volume não têm mais acesso de gravação a ele.
- Quando o volume secundário é promovido à função de volume primário, quaisquer hosts que estão acessando esse volume agora podem gravar nele.
- Se o array de storage local não conseguir se comunicar com o array de storage remoto, você pode forçar a mudança de função no array de storage local.

Forçar mudança de função

É possível forçar uma mudança de função entre volumes em um par espelhado quando um problema de comunicação entre o array de storage local e o array de storage remoto estiver impedindo a promoção do volume secundário ou o rebaixamento do volume primário.

Você pode forçar o volume no lado secundário a assumir a função primária. Em seguida, o host de recuperação pode acessar o volume recém-promovido e as operações de negócios podem continuar.

> Quando o array de storage remoto se recupera e quaisquer problemas de comunicação são resolvidos, ocorre uma condição de Conflito de Volume Primário no Espelhamento Síncrono. As etapas de recuperação incluem a ressincronização dos volumes. Use o Recovery Guru para recuperar desse erro.

Quando uma promoção forçada é permitida e quando 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 em processo de sincronização inicial.
- O par espelhado está nos estados Falha, Alteração de função pendente ou Alteração de função em andamento ou se algum dos volumes de capacidade reservada associados estiver com falha.

Estado de mudança de função em andamento

Se dois arrays de storage em uma configuração de espelhamento forem desconectados, e o volume primário de um par espelhado for forçado a ser rebaixado para a função secundária, e o volume secundário de um par espelhado for forçado a ser promovido para a função primária, então, quando a comunicação for restaurada, os volumes em ambos os arrays de storage serão colocados no estado Role-Change-In-Progress.

O sistema concluirá o processo de mudança de função transferindo os registros de alterações, resincronizando, definindo o estado do par espelhado de volta ao estado operacional normal e continuando com as sincronizações.

Gerenciar grupos de consistência de espelhamento assíncrono

Testar a comunicação para grupos de consistência de espelhamento no SANtricity System Manager

Você pode testar o link de comunicação para diagnosticar possíveis problemas de comunicação entre o array de storage local e o array de storage remoto associado a um grupo de consistência de espelhamento.

Antes de começar

O grupo de consistência de espelhamento que você deseja testar deve existir nos arrays de storage local e remoto.

Sobre esta tarefa

Você pode executar quatro testes diferentes:

- **Conectividade** — Verifica se os dois controladores possuem um caminho de comunicação. O teste de conectividade envia uma mensagem entre os arrays de storage e, em seguida, valida se o grupo de consistência de espelhamento correspondente no array de storage remoto existe. Também valida se os volumes membros do grupo de consistência de espelhamento no array de storage remoto correspondem aos volumes membros do grupo de consistência de espelhamento no array de storage local.
- **Latência** — Envia um comando SCSI Test Unit para cada volume espelhado no array de storage remoto associado ao grupo de consistência de espelhamento para testar a latência mínima, média e máxima.
- **Largura de banda** — Envia duas mensagens entre arrays para o array de storage remoto para testar a largura de banda mínima, média e máxima, bem como a velocidade de link negociada da porta no array que realiza o teste.
- **Conexões de porta** — Mostra a porta que está sendo usada para espelhamento no array de storage local e a porta que está recebendo os dados espelhados no array de storage remoto.

Passos

1. Selecione o menu: armazenamento [Espelhamento Assíncrono].
2. Selecione a guia **Mirror Consistency Groups** e, em seguida, selecione o mirror consistency group que você deseja testar.
3. Selecione **Test Communication**.

   A caixa de diálogo Test Communication é exibida.

4. Selecione um ou mais testes de comunicação para executar entre os arrays de storage local e remoto associados ao grupo de consistência de espelho selecionado e clique em **Test**.
5. Analise as informações exibidas na janela Results.

Status do teste de comunicação	Descrição
Normal sem erros	O grupo de consistência de espelhamento está se comunicando corretamente.
Status aprovado (mas não normal)	Verifique possíveis problemas de rede ou de conexão e tente o teste novamente.

Status do teste de comunicação	Descrição
Status com falha	A causa da falha é indicada. Consulte o Recovery Guru para corrigir o problema.
Erro de conexão de porta	O motivo pode ser que o array de storage local não esteja conectado ou que não seja possível contatar o array de storage remoto. Consulte o Recovery Guru para corrigir o problema.

Resultados

Após a conclusão do teste de comunicação, esta caixa de diálogo exibe um status Normal, um status Aprovado ou um status Reprovado.

Se o teste de comunicação retornar o status Failed, o teste continuará sendo executado após você fechar esta caixa de diálogo até que a comunicação entre os grupos de consistência de espelhamento seja restaurada.

Suspender ou retomar a sincronização para grupos de consistência de espelhamento no SANtricity System Manager

Você pode suspender ou retomar a sincronização de dados em todos os pares espelhados dentro de um grupo de consistência de espelhamento, 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 impacto no desempenho do aplicativo host, que pode ocorrer enquanto quaisquer dados alterados no array de storage local são copiados para o array de storage remoto.

O estado do grupo de consistência de espelhamento e seus pares espelhados permanecem suspensos até que você use a opção Retomar para retomar a atividade de sincronização.

Passos

1. Selecione o menu: armazenamento [Espelhamento Assíncrono].
2. Selecione a guia **Mirror Consistency Groups**.

   A tabela de Grupos de Consistência Espelhada é exibida e mostra todos os grupos de consistência espelhada associados ao array de storage.

3. Selecione o grupo de consistência de espelhamento que você deseja suspender ou retomar e, em seguida, selecione **Mais › Suspender** ou **Mais › Retomar**.

   O sistema exibe uma confirmação.

4. Selecione **Yes** para confirmar.

Resultados

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.

- Registra todos os dados gravados no lado primário do grupo de consistência de espelhamento enquanto o grupo de espelhamento está suspenso e grava os dados automaticamente no lado secundário do grupo de consistência de espelhamento quando o grupo de espelhamento é retomado. Não é necessária uma sincronização completa.
- Para um grupo de consistência de espelhamento *suspenso*, exibe **suspenso pelo usuário** na tabela Mirror Consistency Groups.
- Para um grupo de consistência de espelhamento *retomado*, os dados gravados nos volumes primários enquanto o grupo de consistência de espelhamento estava suspenso são gravados imediatamente nos volumes secundários. A sincronização periódica é retomada se um intervalo de sincronização automática tiver sido definido.

Alterar as configurações de sincronização para um grupo de consistência em SANtricity System Manager

Você pode alterar as configurações de sincronização e os limites de aviso que o grupo de consistência de espelhamento no array de storage usa quando os dados são sincronizados inicialmente ou quando os dados são ressincronizados 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 espelhamento.

Passos

1. Selecione o menu: armazenamento [Espelhamento Assíncrono].
2. Selecione a guia **Mirror Consistency Groups**.

   A tabela de Grupos de Consistência Espelhada é exibida e mostra todos os grupos de consistência espelhada associados ao array de storage.

3. Selecione o grupo de consistência de espelhamento que deseja editar e, em seguida, selecione **More › Edit Settings**.

   O sistema exibe a caixa de diálogo Edit Settings.

4. Edite as configurações de sincronização e alerta conforme apropriado e, em seguida, clique em **Salvar**.

Detalhes do campo

Campo	Descrição
Sincronize os pares espelhados…	Especifique se você deseja sincronizar os pares espelhados no array de storage remotamente, manualmente ou automaticamente. • **Manualmente** – selecione esta opção para sincronizar manualmente os pares espelhados no array de storage remoto. • **Automaticamente, a cada** – Selecione esta opção para sincronizar automaticamente os pares espelhados no array de storage remoto, especificando o intervalo de tempo desde o início da atualização anterior até o início da próxima atualização. O intervalo padrão é 10 minutos.
Avise-me…	Se você definir o método de sincronização para ocorrer automaticamente, defina os seguintes alertas: • **Sincronização** – Defina o período de tempo após o qual System Manager envia um alerta informando que a sincronização não foi concluída. • **Remote recovery point** – Defina um limite de tempo após o qual System Manager enviará um alerta indicando que os dados do ponto de recuperação no array de storage remoto são mais antigos do que o limite de tempo definido. Defina o limite de tempo a partir do final da atualização anterior. • **Limite de capacidade reservada** – Defina uma quantidade de capacidade reservada a partir da qual System Manager enviará um alerta informando que você está se aproximando do limite de capacidade reservada. Defina o limite como uma porcentagem da capacidade restante.

Resultados

System Manager altera as configurações de sincronização para cada par espelhado no grupo de consistência de espelhamento.

Ressincronizar manualmente os grupos de consistência de espelhamento no SANtricity System Manager

Você pode iniciar manualmente a ressincronização para todos os pares espelhados dentro de um grupo de consistência de espelhamento.

Passos

1. Selecione o menu: armazenamento [Espelhamento Assíncrono].
2. Selecione a guia **Mirror Consistency Groups**.

   A tabela de Mirror Consistency Group é exibida e mostra todos os mirror consistency groups associados ao array de storage.

3. Selecione o grupo de consistência de espelhamento que você deseja ressincronizar e, em seguida, selecione **Mais › Ressincronizar manualmente**.

   O sistema exibe uma confirmação.

4. Selecione **Yes** para confirmar.

Resultados

O sistema executa as seguintes ações:

- Inicia a resincronização dos dados em todos os pares espelhados dentro do grupo de consistência de espelhamento selecionado.
- Atualiza os dados modificados do array de storage local para o array de storage remoto.

Visualize a quantidade de dados dessincronizados entre grupos de consistência espelhados no SANtricity System Manager

Você pode visualizar a quantidade de dados dessincronizados entre os grupos de consistência de espelhamento no array de storage local e no array de storage remoto. Enquanto o grupo de consistência de espelhamento estiver no status "Dessincronizado", nenhuma atividade de espelhamento ocorrerá.

Sobre esta tarefa

Você pode executar essa tarefa quando o grupo de consistência de espelhamento selecionado contiver pares espelhados e quando a sincronização não estiver em andamento.

Passos

1. Selecione o menu: armazenamento [Espelhamento Assíncrono].
2. Selecione a guia **Mirror Consistency Groups**.

   A tabela de Mirror Consistency Group é exibida e mostra todos os mirror consistency groups associados ao array de storage.

3. Clique em **More › Ver quantidade de dados não sincronizados**.

   Se existirem dados não sincronizados, os valores da tabela refletem isso. A coluna quantidade de dados lista a quantidade de dados não sincronizados em MiB.

Atualizar endereços IP do array de storage remoto no SANtricity System Manager

Você pode atualizar o endereço IP iSCSI do seu array de storage remoto para restabelecer a conexão com o array de storage local.

Antes de começar

Tanto o array de storage local quanto o array de storage remoto devem ser configurados para espelhamento assíncrono usando uma conexão iSCSI.

Passos

1. Selecione o menu: armazenamento [Espelhamento Assíncrono].
2. Selecione a guia **Mirror Consistency Groups**.

A tabela Grupos de Consistência de Espelho exibe todos os grupos de consistência de espelho associados ao array de storage.

3. Selecione o grupo de consistência de espelhamento que você 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 do seu array de storage remoto.

Resultados

O sistema redefine o endereço IP do array de storage remoto para restabelecer a conexão com o array de storage local.

Altere a função do grupo de consistência de espelhamento para primário ou secundário no SANtricity System Manager

Você pode alterar a função entre grupos de consistência de espelhamento para fins administrativos ou em caso de desastre no array de storage.

Sobre esta tarefa

Os grupos de consistência de espelhamento criados no array de storage local detêm a função primária. Os grupos de consistência de espelhamento criados no array de storage remoto detêm a função secundária. Você pode rebaixar o grupo de consistência de espelhamento local para a função secundária ou promover o grupo de consistência de espelhamento remoto para a função primária.

Passos

1. Selecione o menu: armazenamento [Espelhamento Assíncrono].
2. Selecione a guia **Mirror Consistency Groups**.

   A tabela de Mirror Consistency Group é exibida e mostra todos os mirror consistency groups associados ao array de storage.

3. Selecione o grupo de consistência de espelhamento para o qual você deseja alterar a função e, em seguida, selecione **Mais › Alterar função para <Primary | Secondary>**.

   O sistema exibe uma confirmação.

4. Confirme que deseja alterar a função do grupo de consistência de espelhamento e clique em **Alterar função**.

> O sistema exibe a caixa de diálogo "Não é possível contatar o array de storage" quando uma alteração de função é solicitada, mas o array de storage remoto não pode ser contatado. Clique em **Sim** para forçar a alteração de função.

Resultados

System Manager executa as seguintes ações:

- A tabela Grupo de Consistência de Espelhamento exibe o status "pendente" ou "em andamento" ao lado do grupo de consistência de espelhamento que está passando pela alteração de função. Você pode cancelar uma operação de Alteração de Função pendente clicando no link **Cancelar** encontrado na célula da tabela.

- Se for possível contatar o grupo de consistência de espelhamento associado, as funções entre os grupos de consistência de espelhamento são alteradas. System Manager promove o grupo de consistência de espelhamento secundário para a função primária ou rebaixa o grupo de consistência de espelhamento primário para a função secundária (dependendo da sua seleção). A alteração de função afeta todos os pares espelhados dentro do grupo de consistência de espelhamento selecionado.

Exclua um grupo de consistência de espelhamento no SANtricity System Manager

Você pode excluir grupos de consistência de espelhamento que não são mais necessários no array de storage local e no array de storage remoto.

Antes de começar

Todos os pares espelhados devem ser removidos do grupo de consistência de espelhamento.

Passos

1. Selecione o menu: armazenamento [Espelhamento Assíncrono].
2. Selecione a guia **Mirror Consistency Groups**.

   A tabela de Mirror Consistency Group é exibida e mostra todos os mirror consistency groups associados ao array de storage.

3. Selecione o grupo de consistência de espelhamento que deseja excluir e, em seguida, selecione **Tarefas incomuns › Excluir**.

   O sistema exibe uma confirmação.

4. Selecione **Sim** para excluir o grupo de consistência de espelhamento.

Resultados

System Manager executa as seguintes ações:

- Exclui o grupo de consistência de espelhamento no array de storage local primeiro e, em seguida, exclui o grupo de consistência de espelhamento no array de storage remoto.
- Remove o grupo de consistência de espelhamento da tabela de Mirror Consistency Group.

Depois que você terminar

Ocasionalmente, pode haver casos em que o grupo de consistência de espelhamento seja excluído com sucesso do array de storage local, mas um erro de comunicação impeça que o grupo de consistência de espelhamento seja excluído do array de storage remoto. Nesse caso, você deve acessar o array de storage remoto para excluir o grupo de consistência de espelhamento correspondente.

Gerenciar pares espelhados assíncronos

Remover relacionamentos de espelhamento assíncrono no SANtricity System Manager

Você remove um par espelhado para remover a relação de espelhamento do volume primário no array de storage local e do volume secundário no array de storage remoto.

Sobre esta tarefa

Revise as seguintes informações sobre pares espelhados órfãos:

- Um par espelhado órfão existe quando um volume membro em um grupo de espelhamento de consistência foi removido de um lado (seja do lado do array de storage local ou do lado do array de storage remoto), mas não do outro lado.
- Pares espelhados órfãos são detectados quando a comunicação entre arrays é restaurada e os dois lados da configuração de espelhamento reconciliam os parâmetros do espelhamento.
- Você pode remover um par espelhado para corrigir um estado de par espelhado órfão.

Passos

1. Selecione o menu: armazenamento [Espelhamento Assíncrono].
2. Selecione a guia **Par Espelhado**.

   A tabela de pares espelhados é exibida e mostra todos os pares espelhados associados ao array de storage.

3. Selecione o par espelhado que você deseja remover e, em seguida, clique em **Remover**.
4. Confirme que deseja remover o par espelhado e, em seguida, clique em **Remover**.

Resultados

System Manager executa as seguintes ações:

- Remove a relação de espelhamento do grupo de consistência de espelhamento no array de storage local e no array de storage remoto, e exclui a capacidade reservada.
- Retorna o volume primário e o volume secundário para volumes acessíveis ao host e não espelhados.
- Atualiza o bloco de Espelhamento Assíncrono com a remoção do par espelhado assíncrono.

Aumentar a capacidade reservada no SANtricity System Manager

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

Para operações de Snapshot, normalmente é 40 por cento do volume base; para operações de espelhamento assíncrono, normalmente é 20 por cento 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 volume deve ter um status Ótimo e não deve estar em nenhum estado de modificação.
- Deve haver capacidade livre no pool ou volume group que você deseja usar para aumentar a capacidade.

  Se não houver capacidade livre em nenhum pool ou grupo de volume, você pode adicionar capacidade não atribuída na forma de drives não utilizados a um pool ou grupo de volume.

Sobre esta tarefa

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

- Grupo de Snapshot
- Volume de Snapshot

- Volume membro do grupo de consistência
- Volume de par espelhado

Use uma porcentagem alta se você acredita que o volume principal sofrerá muitas alterações ou se a vida útil de uma determinada operação de serviço de cópia for muito longa.

Não é possível aumentar a capacidade reservada para um volume de snapshot que seja somente leitura. Apenas volumes de snapshot que sejam de leitura e gravação requerem capacidade reservada.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione a guia **Capacidade Reservada**.
3. Selecione o objeto de storage para o qual deseja aumentar a capacidade reservada e clique em **Aumentar capacidade**.

   A caixa de diálogo Increase Reserved Capacity é exibida.

4. Use a caixa de rotação para ajustar a porcentagem de capacidade.

   Se não houver capacidade livre no pool ou grupo de volume que contém o objeto de armazenamento selecionado, e o array de storage tiver capacidade não atribuída, você pode criar um novo pool ou grupo de volume. Você pode então tentar novamente esta operação usando a nova capacidade livre nesse pool ou grupo de volume.

5. Clique em **Increase**.

Resultados

System Manager executa as seguintes ações:

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

Altere as configurações de capacidade reservada para um volume de par espelhado no SANtricity System Manager

Você pode alterar as configurações de um volume de par espelhado para ajustar o ponto percentual em que SANtricity System Manager envia uma notificação de alerta quando a capacidade reservada para um volume de par espelhado está quase cheia.

Passos

1. Selecione o menu: Storage [Pools & Volume Groups].
2. Selecione a guia **Capacidade Reservada**.
3. Selecione o par de volumes espelhados que deseja editar e clique em **Visualizar/Editar Settings**.

   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

Configuração	Descrição
Avise-me quando…	Use o seletor giratório para ajustar o ponto percentual em que System Manager envia uma notificação de alerta quando a capacidade reservada para um par espelhado estiver quase cheia. Quando a capacidade reservada para o par espelhado excede o limite especificado, System Manager envia um alerta, permitindo que você aumente a capacidade reservada. Alterar a configuração de alerta para um par espelhado altera a configuração de alerta para todos os pares espelhados que pertencem ao mesmo grupo de consistência de espelhamento.

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

Conclua um par espelhado para volumes primários criados em um sistema legado no SANtricity System Manager

Se você criou um volume primário em um array de storage legado que não pode ser gerenciado pelo SANtricity System Manager, você pode criar o volume secundário nesse array com SANtricity System Manager.

Sobre esta tarefa

É possível realizar 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 arrays de storage que usam System Manager, poderá ignorar esta tarefa, pois já concluiu o par espelhado na sequência de criação de par espelhado.
- Execute esta tarefa no array de storage remoto.

Passos

1. Selecione o menu: armazenamento [Espelhamento Assíncrono].
2. Selecione a guia **Par Espelhado**.

   A tabela de pares espelhados é exibida e mostra todos os pares espelhados associados ao array de storage.

3. Localize o volume do par espelhado com o status de Incompleto e clique no link **Concluir par espelhado** exibido na coluna do par espelhado.
4. Escolha se deseja concluir a sequência de criação do par espelhado automaticamente ou manualmente selecionando um dos seguintes botões de opção:
   - **Automático** — Criar novo volume secundário.

     Aceite as configurações padrão para o lado remoto do par espelhado selecionando um pool existente ou grupo de volume onde deseja criar o volume secundário. Use esta opção recomendada para alocar

a capacidade reservada para o volume secundário com as configurações padrão.

- **Manual** — Selecione um volume existente.

  Defina seus próprios parâmetros para o volume secundário.

  i. Clique em **Avançar** 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. Faça uma das seguintes opções:
    - Aceite as configurações padrão.

      A configuração padrão para capacidade reservada é 20% da capacidade do volume base, e geralmente essa capacidade é suficiente.

    - Defina suas próprias configurações de capacidade reservada para atender às suas necessidades de storage relacionadas ao espelhamento assíncrono.

      A capacidade necessária varia dependendo da frequência e do tamanho das gravações de E/S no volume primário e de quanto tempo você precisa manter essa capacidade. Em geral, escolha uma capacidade maior para capacidade reservada se uma ou ambas estas condições existirem:

      - Você pretende manter o par espelhado por um longo período de tempo.
      - Uma grande porcentagem dos blocos de dados será alterada no volume primário devido à intensa atividade de E/S. Utilize dados históricos de desempenho ou outros utilitários do sistema operacional para ajudar a determinar a atividade típica de E/S no volume primário.

5. Selecione **Complete**.

Resultados

System Manager executa as seguintes ações:

- Cria o volume secundário no array de storage remoto e aloca capacidade reservada para o lado remoto do par espelhado.
- Inicia a sincronização inicial entre o array de storage local e o array de storage remoto.
- Se o volume que está sendo espelhado for um volume fino, somente os blocos alocados serão transferidos para o volume secundário durante a sincronização inicial. Essa transferência reduz a quantidade de dados que deve ser transferida para concluir a sincronização inicial.
- Cria a capacidade reservada para o par espelhado no array de storage local e no array de storage remoto.

Gerenciar pares espelhados de sync

Testar a comunicação para espelhamento síncrono no SANtricity System Manager

Você pode testar a comunicação entre um array de storage local e um array de storage remoto para diagnosticar possíveis problemas de comunicação em um par espelhado que participa do espelhamento síncrono.

Sobre esta tarefa

Dois testes diferentes são realizados:

- **Comunicação** — Verifica se os dois arrays de storage possuem um caminho de comunicação. O teste de comunicação valida se o array de storage local pode se comunicar com o array de storage remoto e se o volume secundário associado ao par espelhado existe no array de storage remoto.
- **Latência** — Envia um comando de unidade de teste SCSI para o volume secundário no array de storage remoto associado ao par espelhado para testar a latência mínima, média e máxima.

Passos

1. Selecione o menu: Storage [Espelhamento Síncrono].
2. Selecione o volume espelhado que deseja testar e, em seguida, selecione **Test Communication**.
3. Analise as informações exibidas na janela Results e, se necessário, siga a ação corretiva indicada.

> Se o teste de comunicação falhar, o teste continuará sendo executado após você fechar esta caixa de diálogo até que a comunicação entre o par espelhado seja restabelecida.

Suspender e retomar a sincronização de pares espelhados no SANtricity System Manager

Você pode usar a opção Suspender e a opção Retomar 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 o menu: Storage [Espelhamento Síncrono].
2. Selecione o par espelhado que você deseja suspender ou retomar e, em seguida, selecione **More › Suspend** ou **More › Resume**.

   O sistema exibe uma confirmação.
3. Selecione **Yes** para confirmar.

Resultados

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 Mirrored Pair.
  - Registra quaisquer dados que foram gravados no volume primário do par espelhado enquanto a sincronização estava suspensa.
- Para um par espelhado *retomado*, grava os dados automaticamente no volume secundário do par espelhado quando a sincronização é retomada. Uma sincronização completa não é necessária.

Altere a função entre volumes em um par espelhado no SANtricity System Manager

É possível realizar uma reversão de função entre os dois volumes em um par espelhado que participam do espelhamento síncrono. Essa tarefa pode ser necessária para fins

administrativos ou em caso de desastre no array de storage.

Sobre esta tarefa

Você pode rebaixar o volume primário para a função de secundário ou promover o volume secundário para a função de primário. Todos os hosts que acessam o volume primário têm permissão de leitura/gravação para o volume. Quando o volume primário se torna um volume secundário, somente as gravações remotas iniciadas pelo controlador primário são gravadas no volume.

Passos

1. Selecione o menu: Storage [Espelhamento Síncrono].
2. Selecione o par espelhado que contém os volumes para os quais deseja alterar a função e, em seguida, selecione **More › Change Role**.

   O sistema exibe uma confirmação.

3. Confirme que deseja alterar a função dos volumes e, em seguida, selecione **Alterar função**.

> Se o array de storage local não conseguir se comunicar com o array de storage remoto, o sistema exibirá a caixa de diálogo Cannot Contact Storage Array quando uma alteração de função for solicitada, mas o array de storage remoto não puder ser contatado. Clique em **Yes** para forçar a alteração de função.

Resultados

System Manager executa a seguinte ação:

- Se o volume associado no par espelhado puder ser contatado, as funções entre os volumes se invertem. System Manager promove o volume secundário no par espelhado à função primária ou rebaixa o volume primário no par espelhado à função secundária (dependendo da sua seleção).

Alterar as configurações de sincronização para um par espelhado no SANtricity System Manager

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 de um par espelhado somente no array de storage que contém o volume primário.

Passos

1. Selecione o menu: Storage [Espelhamento Síncrono].
2. Selecione o par espelhado que deseja editar e, em seguida, selecione **More › Edit settings**.

   O sistema exibe a caixa de diálogo View/Edit Settings.

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 taxas de sincronização

Existem cinco taxas de prioridade de sincronização:

- Mais baixo
- Baixo
- Médio
- Alto
- Mais alto

Se a prioridade de sincronização estiver definida para a taxa mais baixa, a atividade de E/S terá prioridade e a operação de ressincronização levará mais tempo. Se a prioridade de sincronização estiver definida para a taxa mais alta, a operação de ressincronização terá prioridade, mas a atividade de E/S para o array de storage pode ser afetada.

4. Edite a política de ressincronização conforme apropriado.

   Você pode ressincronizar os pares espelhados no array de storage remoto manualmente ou automaticamente.

   - **Manual** (opção recomendada) — Selecione esta opção para exigir que a sincronização seja retomada manualmente após a restauração da comunicação com um par espelhado. Esta opção oferece a melhor oportunidade para recuperação de dados.
   - **Automático** — selecione esta opção para iniciar a ressincronização automaticamente após a comunicação ser restaurada em um par espelhado.
5. Selecione **Save**.

Remover relações de espelhamento síncrono no SANtricity System Manager

Você remove um par espelhado para remover a relação de espelhamento do volume primário no array de storage local e do volume secundário no array de storage remoto.

Sobre esta tarefa

Você também pode remover um par espelhado para corrigir um estado de par espelhado órfão. Consulte as seguintes informações sobre pares espelhados órfãos:

- Um par espelhado órfão existe quando um volume membro foi removido de um lado (local/remoto) mas não do outro lado.
- Pares espelhados órfãos são detectados quando a comunicação entre arrays é restaurada.

Passos

1. Selecione o menu: Storage [Espelhamento Síncrono].
2. Selecione o par espelhado que deseja remover e, em seguida, selecione o **Tarefas incomuns › Remover**.

   A caixa de diálogo Remover relacionamento de espelhamento é exibida.
3. Confirme que deseja remover o par espelhado e, em seguida, clique em **Remover**.

Resultados

System Manager executa as seguintes ações:

- Remove a relação de espelhamento do par espelhado no array de storage local e no array de storage remoto.
- Retorna o volume primário e o volume secundário para volumes acessíveis ao host e não espelhados.
- Atualiza o bloco de espelhamento síncrono com a remoção do par espelhado síncrono.

Desativar espelhamento

Desativar espelhamento assíncrono no SANtricity System Manager

Você pode desativar o espelhamento assíncrono nos arrays de storage locais e remotos para restabelecer o uso normal das portas dedicadas nos arrays de storage.

Antes de começar

- Você deve ter excluído todos os relacionamentos de espelhamento. Verifique se todos os grupos de consistência de espelhamento e pares espelhados foram excluídos dos arrays de storage local e remoto.
- O array de storage local e o array de storage remoto devem ser conectados por meio de uma estrutura Fibre Channel ou interface iSCSI.

Sobre esta tarefa

Ao desativar o espelhamento assíncrono, nenhuma atividade de espelhamento poderá ocorrer nos arrays de storage local e remoto.

Passos

1. Selecione o menu: armazenamento [Espelhamento Assíncrono].
2. Selecione o menu: tarefas incomuns [Desativar].

   O sistema exibe uma confirmação.

3. Selecione **Yes** para confirmar.

Resultados

- Os canais de host HBA do controlador que eram dedicados à comunicação de espelhamento assíncrono agora podem aceitar solicitações de leitura e gravação do host.
- Nenhum dos volumes neste array de storage pode participar de relações de espelhamento como volumes primários ou volumes secundários.

Desativar espelhamento síncrono no SANtricity System Manager

Você pode desativar o recurso de espelhamento síncrono em um array de storage para restabelecer o uso normal da porta 4 do adaptador de barramento de host (HBA) host, que era reservada para a transmissão de dados do espelhamento.

Antes de começar

Você deve ter excluído todos os relacionamentos de espelhamento síncrono. Verifique se todos os pares espelhados foram excluídos do array de storage.

Passos

1. Selecione o menu: Storage [Espelhamento Síncrono].
2. Selecione o menu: tarefas incomuns [Desativar].

   O sistema exibe uma confirmação.

3. Selecione **Yes** para confirmar.

Resultados

- A porta 4 do host HBA do controlador, que era dedicada à comunicação de espelhamento síncrono, agora pode aceitar solicitações de leitura e gravação do host.
- Os volumes de capacidade reservada no array de storage são eliminados.

Perguntas frequentes sobre espelhamento assíncrono para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

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 momento e copia apenas os dados que foram alterados desde a última captura de imagem.

Com espelhamento síncrono, o estado do volume primário não é capturado em um determinado momento, mas sim reflete todas as alterações que foram feitas no volume primário para o volume secundário. O volume secundário é idêntico ao volume primário em todos os momentos porque, com esse tipo de espelhamento, 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 sucesso com as alterações feitas no volume primário.

Com espelhamento assíncrono, o array de storage remoto não está totalmente sincronizado com o array de storage local, portanto, se o aplicativo precisar fazer a transição para o array de storage remoto devido a uma perda do array de storage local, algumas transações poderão ser perdidas.

Comparação entre recursos de espelhamento:

Espelhamento assíncrono	Espelhamento síncrono
Método de replicação	• **Ponto no tempo** O espelhamento é feito sob demanda ou automaticamente de acordo com uma programação definida pelo usuário. As programações podem ser definidas com granularidade de minutos. O tempo mínimo entre sincronizações é 10 minutos.

Espelhamento assíncrono	Espelhamento síncrono
• **Contínuo** O espelhamento é executado automaticamente continuamente, copiando dados de cada gravação do host.	**Capacidade reservada**
• **Múltiplo** É necessário um volume de capacidade reservada para cada par espelhado.	• **Único** É necessário um único volume de capacidade reservada para todos os volumes espelhados.
Comunicação	• **iSCSI e Fibre Channel** Suporta interfaces iSCSI e Fibre Channel entre arrays de storage.
• **Fibre Channel** Suporta apenas interfaces Fibre Channel entre arrays de storage.	**Distância**
• **Ilimitado** Suporte para distâncias praticamente ilimitadas entre o array de storage local e o array de storage remoto, sendo a distância normalmente limitada apenas pelas capacidades da rede e pela tecnologia de extensão de canal.	• **Restrito** Normalmente, deve estar a cerca de 10 km (6,2 milhas) do array de storage local para atender aos requisitos de latência e desempenho do aplicativo.

Por que não consigo acessar o recurso de espelhamento que escolhi?

O espelhamento é configurado na interface SANtricity Unified Manager.

O espelhamento síncrono não está disponível no array de storage EF600/EF600C ou EF300/EF300C.

Para habilitar e configurar o espelhamento entre dois arrays, verifique o seguinte:

- O serviço Web Services Proxy deve estar em execução. (Unified Manager é instalado em um sistema host juntamente com o Web Services Proxy.)
- Unified Manager deve estar sendo executado em seu host local por meio de uma conexão HTTPS.
- Os dois arrays de storage que você deseja usar para espelhamento devem ser detectados no Unified Manager.
- Unified Manager deve ter certificados SSL válidos para os storage arrays. Você pode aceitar um certificado autoassinado ou instalar certificados assinados por CA a partir 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 preciso saber antes de criar um grupo de consistência de espelhamento?

Siga estas diretrizes antes de criar um grupo de consistência de espelhamento.

> O espelhamento síncrono não está disponível no sistema de storage EF600/EF600C ou EF300/EF300C.

Você cria um grupo de consistência no Unified Manager no assistente Criar Pares Espelhados.

Atenda aos seguintes requisitos para Unified Manager:

- O serviço Web Services Proxy deve estar em execução.
- Unified Manager deve estar sendo executado em seu host local por meio de uma conexão HTTPS.
- Unified Manager deve exibir certificados SSL válidos para o array de storage. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando Unified Manager e navegando até **Certificate › Certificate Management**.

Certifique-se também de atender aos seguintes requisitos para arrays de storage:

- Os dois arrays de storage devem ser detectados no Unified Manager.
- Cada array de storage deve ter dois controladores.
- Cada controlador, tanto no array primário quanto no array secundário, deve ter uma porta de gerenciamento Ethernet configurada e deve estar conectado à sua rede.
- Os arrays de storage possuem uma versão mínima de firmware de 7.84. (Cada um deles pode executar diferentes versões de sistema operacional.)
- Você deve saber a senha dos arrays de storage local e remoto.
- Seus arrays de storage locais e remotos estão conectados por meio de uma estrutura Fibre Channel ou interface iSCSI.

Espelhamento assíncrono - o que preciso saber antes de criar um par espelhado?

Você configura pares espelhados na interface SANtricity Unified Manager e, em seguida, gerencia os pares no SANtricity System Manager.

Antes de criar um par espelhado, siga estas orientações.

- Você precisa ter dois arrays de storage.
- Cada array de storage deve ter dois controladores.
- Cada controlador, tanto no array primário quanto no array secundário, deve ter uma porta de gerenciamento Ethernet configurada e deve estar conectado à sua rede.
- Seus arrays de storage locais e remotos estão conectados por meio de uma estrutura Fibre Channel ou interface iSCSI.
- Os arrays de storage possuem uma versão mínima de firmware de 7.84. (Cada um deles pode executar diferentes versões de sistema operacional.)

- Você deve saber a senha dos arrays de storage local e remoto.
- Você precisa ter capacidade livre suficiente no array de storage remoto para criar um volume secundário igual ou maior que o volume primário que você deseja espelhar.
- Você instalou o Web Services Proxy e Unified Manager. Os pares espelhados são configurados na interface do Unified Manager.
- Os dois arrays de storage são detectados no Unified Manager.
- Seu array de storage deve conter pelo menos um grupo de consistência de espelhamento. Você cria um grupo de consistência no Unified Manager no assistente Criar Pares Espelhados.

O que 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 só pode aumentar a capacidade reservada em incrementos de 8 GiB.

Para operações de espelhamento assíncrono, a capacidade reservada geralmente corresponde a 20% do volume base. Escolha uma capacidade reservada maior se uma ou ambas estas condições existirem:

- Você pretende manter o par espelhado por um longo período de tempo.
- Uma grande porcentagem dos blocos de dados será alterada no volume primário devido à intensa atividade de E/S. Utilize dados históricos de desempenho ou outros utilitários do sistema operacional para ajudar a determinar a atividade típica de E/S no volume primário.

Você pode aumentar a capacidade reservada para um par espelhado realizando uma destas ações:

- Ajuste a porcentagem de capacidade para um volume de par espelhado selecionando **Storage › Pools and Volumes Groups** e, em seguida, clicando na guia **Reserved Capacity**.
- Crie um novo volume usando a capacidade livre disponível em um pool ou volume group.

  Se não houver capacidade livre em nenhum pool ou grupo de volume, você pode adicionar capacidade não configurada na forma de unidades não utilizadas a um pool ou grupo de volume.

Por que não consigo aumentar a capacidade reservada com a quantidade solicitada?

Você pode aumentar a capacidade reservada apenas em incrementos de 4 GiB.

Revise as seguintes diretrizes:

- Você deve ter capacidade livre suficiente no pool ou grupo de volume para que ele possa ser expandido se necessário.

  Se não houver capacidade livre em nenhum pool ou grupo de volume, você pode adicionar capacidade não atribuída na forma de drives não utilizados a um pool ou grupo de volume.

- O volume no pool ou grupo de volume deve ter um status Ótimo e não deve estar em nenhum estado de modificação.
- Deve haver capacidade livre no pool ou volume group que você deseja usar para aumentar a capacidade.

Para operações de espelhamento assíncrono, a capacidade reservada normalmente corresponde a 20 por cento do volume base. Use uma porcentagem maior se você acredita que o volume base sofrerá muitas alterações ou se a expectativa de vida útil da operação de serviço de cópia de um objeto de storage for muito

longa.

Por que eu alteraria essa porcentagem?

A capacidade reservada é normalmente de 40% do volume base para operações de snapshot e de 20% do volume base para operações de espelhamento assíncrono.

Normalmente, essa capacidade é suficiente. A capacidade necessária varia, dependendo da frequência e do tamanho das gravações de E/S no volume base e de 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 estas condições existirem:

- Se a vida útil da operação de serviço de cópia de um determinado objeto de storage for muito longa.
- Se uma grande porcentagem dos blocos de dados for alterada no volume base devido à intensa atividade de E/S. Utilize dados históricos de desempenho ou outros utilitários do sistema operacional para ajudar a determinar a atividade típica de E/S no volume base.

Por que vejo mais de um candidato para capacidade reservada?

Se houver mais de um volume em um pool ou grupo de volume que atenda à porcentagem de capacidade que você selecionou para o objeto de storage, você verá vários candidatos.

Você pode atualizar a lista de candidatos recomendados alterando a porcentagem de espaço físico em disco 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 Disponível exibidos na tabela?

A tabela lista os valores Não Disponível quando os dados localizados no array de storage remoto não estão disponíveis para exibição.

Para exibir os dados do array de storage remoto, inicie System Manager a partir do Unified Manager.

Por que não vejo todos os meus pools e grupos de volume?

Ao criar um volume secundário para o par espelhado assíncrono, o sistema exibe uma lista de todos os pools e grupos de volume elegíveis para esse par espelhado assíncrono. Qualquer pool ou grupo de volume que não seja elegível para uso não é exibido nessa lista.

Pools ou grupos de volume podem não ser elegíveis por qualquer um dos seguintes motivos.

- Os recursos de segurança de um pool ou grupo de volume 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 são elegíveis para uso não são exibidos nessa lista. Volumes podem não ser elegíveis por qualquer um dos seguintes motivos:

- O volume não está otimizado.
- 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 de bandeja, tamanho de 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 array de storage remoto?

Ao selecionar um volume secundário no array de storage remoto, uma lista mostra todos os volumes elegíveis para esse par espelhado.

Quaisquer volumes que não são elegíveis para uso não são exibidos nessa lista. Volumes podem não ser elegíveis por qualquer um dos seguintes motivos:

- O volume não está otimizado.
- 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 você estiver usando Data Assurance (DA), o volume primário e o volume secundário devem ter as mesmas configurações de DA.
  - Se o volume principal estiver habilitado para DA, o volume secundário também deve estar habilitado para DA.
  - Se o volume principal não estiver habilitado para DA, o volume secundário não deve estar habilitado para DA.

Por que eu atualizaria o endereço IP do meu array de storage remoto?

Você atualiza o endereço IP do array de storage remoto quando o endereço IP de uma porta iSCSI muda e o array de storage local não consegue se comunicar com o array de storage remoto.

Ao estabelecer uma relação de espelhamento assíncrono com uma conexão iSCSI, tanto o array de storage local quanto o array de storage remoto armazenam um registro do endereço IP do array de storage remoto na configuração de espelhamento assíncrono. Se o endereço IP de uma porta iSCSI for alterado, o array de storage remoto que estiver tentando usar essa porta encontrará um erro de comunicação.

O array de storage com o endereço IP alterado envia uma mensagem para cada array de storage remoto associado aos grupos de consistência de espelhamento que estão configurados para espelhar por meio de uma conexão iSCSI. Os arrays de storage que recebem essa mensagem atualizam automaticamente seu endereço IP de destino remoto.

Se o array de storage com o endereço IP alterado não conseguir enviar sua mensagem entre arrays para um array de storage remoto, o sistema enviará um alerta sobre o problema de conectividade. Use a opção Atualizar Endereço IP Remoto para restabelecer a conexão com o array de storage local.

Perguntas frequentes sobre espelhamento síncrono para o SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma

pergunta.

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 momento e copia apenas os dados que foram alterados desde a última captura de imagem.

Com espelhamento síncrono, o estado do volume primário não é capturado em um determinado momento, mas sim reflete todas as alterações que foram feitas no volume primário para o volume secundário. O volume secundário é idêntico ao volume primário em todos os momentos porque, com esse tipo de espelhamento, 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 sucesso com as alterações feitas no volume primário.

Com espelhamento assíncrono, o array de storage remoto não está totalmente sincronizado com o array de storage local, portanto, se o aplicativo precisar fazer a transição para o array de storage remoto devido a uma perda do array de storage local, algumas transações poderão ser perdidas.

Comparação entre recursos de espelhamento:

Espelhamento assíncrono	Espelhamento síncrono
Método de replicação	• **Ponto no tempo** O espelhamento é feito sob demanda ou automaticamente de acordo com uma programação definida pelo usuário. As programações podem ser definidas com granularidade de minutos. O tempo mínimo entre sincronizações é 10 minutos.
• **Contínuo** O espelhamento é executado automaticamente continuamente, copiando dados de cada gravação do host.	**Capacidade reservada**
• **Múltiplo** É necessário um volume de capacidade reservada para cada par espelhado.	• **Único** É necessário um único volume de capacidade reservada para todos os volumes espelhados.
Comunicação	• **iSCSI e Fibre Channel** Suporta interfaces iSCSI e Fibre Channel entre arrays de storage.

Espelhamento assíncrono	Espelhamento síncrono
• **Fibre Channel** Suporta apenas interfaces Fibre Channel entre arrays de storage.	**Distância**
• **Ilimitado** Suporte para distâncias praticamente ilimitadas entre o array de storage local e o array de storage remoto, sendo a distância normalmente limitada apenas pelas capacidades da rede e pela tecnologia de extensão de canal.	• **Restrito** Normalmente, deve estar a cerca de 10 km (6,2 milhas) do array de storage 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.

Os volumes que não são elegíveis para uso não são exibidos nessa lista. Volumes podem não ser elegíveis por qualquer um dos seguintes motivos:

- O volume é um volume não padrão, como um volume Snapshot ou um volume fino.
- O volume não está otimizado.
- O volume já está participando de uma relação de espelhamento.

Espelhamento síncrono - Por que não vejo todos os volumes no array de storage remoto?

Ao selecionar um volume secundário no array de storage remoto, uma lista mostra todos os volumes elegíveis para esse par espelhado.

Quaisquer volumes que não são elegíveis para uso não são exibidos nessa lista. Volumes podem não ser elegíveis por qualquer um dos seguintes motivos:

- O volume é um volume não padrão, como um volume Snapshot ou um volume fino.
- O volume não está otimizado.
- O volume já está participando de uma relação de espelhamento.
- Se você estiver usando Data Assurance (DA), o volume primário e o volume secundário devem ter as mesmas configurações de DA.
  - Se o volume principal estiver habilitado para DA, o volume secundário também deve estar habilitado para DA.
  - Se o volume principal não estiver habilitado para DA, o volume secundário não deve estar habilitado para DA.

Espelhamento síncrono - o que preciso saber antes de criar um par espelhado?

Você configura pares espelhados na interface SANtricity Unified Manager e, em seguida, gerencia os pares no SANtricity System Manager.

Antes de criar um par espelhado, siga estas orientações:

- Você precisa ter dois arrays de storage.
- Cada array de storage deve ter dois controladores.
- Cada controlador, tanto no array primário quanto no array secundário, deve ter uma porta de gerenciamento Ethernet configurada e deve estar conectado à sua rede.
- Seus arrays de storage local e remoto estão conectados por meio de uma malha Fibre Channel.
- Os arrays de storage possuem uma versão mínima de firmware de 7.84. (Cada um deles pode executar diferentes versões de sistema operacional.)
- Você deve saber a senha dos arrays de storage local e remoto.
- Você precisa ter capacidade livre suficiente no array de storage remoto para criar um volume secundário igual ou maior que o volume primário que você deseja espelhar.
- Você instalou o Web Services Proxy e Unified Manager. Os pares espelhados são configurados na interface do Unified Manager.
- Os dois arrays de storage são detectados no Unified Manager.

Qual o impacto da prioridade de sincronização 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 controlador proprietário do volume primário executa essa operação em segundo plano. Ao mesmo tempo, o controlador proprietário processa gravações de E/S locais no volume primário e gravações remotas associadas no volume secundário. Como a ressincronização desvia recursos de processamento do controlador da atividade de E/S, a ressincronização pode ter um impacto no desempenho do aplicativo host.

Tenha 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 taxas de prioridade de sincronização

Estas taxas de prioridade estão disponíveis:

- Mais baixo
- Baixo
- Médio
- Alto
- Mais alto

A taxa de prioridade mais baixa oferece suporte ao desempenho do sistema, mas a ressincronização demora mais. A taxa de prioridade mais alta oferece suporte à ressincronização, mas o desempenho do sistema pode ser comprometido.

Essas diretrizes aproximam, de forma geral, as diferenças entre as prioridades.

Taxa de prioridade para sincronização completa	Tempo decorrido em comparação com a taxa de sincronização mais alta
Mais baixo	Aproximadamente oito vezes mais longo do que na taxa de prioridade mais alta.
Baixo	Aproximadamente seis vezes mais longo do que na taxa de prioridade mais alta.
Médio	Aproximadamente três vezes e meia mais longo do que na taxa de prioridade mais alta.
Alto	Aproximadamente duas vezes mais longo do que na taxa de prioridade mais alta.

O tamanho do volume e as cargas de 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 oferece a melhor oportunidade para recuperar dados.

Se você utiliza uma política de ressincronização automática e ocorrerem problemas intermitentes de comunicação durante a ressincronização, os dados no volume secundário podem ser corrompidos temporariamente. Quando a ressincronização é concluída, os dados são corrigidos.

Armazenamento remoto

Saiba mais sobre o recurso Remote Storage no SANtricity System Manager

Se você tiver o recurso de Remote Storage, poderá importar dados de um sistema de storage remoto para seu array de storage.

O que é o recurso de storage remoto?

O recurso *Remote Storage* permite importar dados de um sistema de storage remoto para um sistema de storage E-Series local. O sistema remoto pode ser outro sistema E-Series ou um sistema de outro fornecedor. Esse recurso é útil quando você deseja agilizar a migração de dados com o mínimo de tempo de inatividade, como durante atualizações de equipamentos.

Para usar o storage remoto, esse recurso deve ser ativado no Submodel ID (SMID).

Saiba mais:

- "Como funciona o storage remoto"
- "Terminologia de storage remoto"
- "Requisitos de storage remoto"
- "Requisitos de volume de storage remoto"

Como faço para importar dados com esse recurso?

Usando o assistente de Remote Storage, você mapeia um dispositivo de storage (a origem da importação de dados) para um volume de destino no sistema E-Series. Este assistente está disponível no **Storage › Remote storage**.

Saiba mais:

- "Importar storage remoto"
- "Gerenciar o progresso da importação de dados"

Conceitos

Como o armazenamento remoto funciona no software SANtricity

O recurso de armazenamento remoto permite importar dados de um sistema de storage remoto para um sistema de storage E-Series local. Esse recurso é útil quando você deseja agilizar a migração de dados com o mínimo de tempo de inatividade, como durante atualizações de equipamentos.

Para configurar o recurso de armazenamento remoto, você deve configurar o hardware e, em seguida, usar System Manager para criar um objeto de armazenamento remoto. Assim que essa configuração for concluída, o processo de importação começa.

Configuração de hardware

Utilize o seguinte fluxo de trabalho para preparar as conexões de hardware.

Essas etapas são descritas com mais detalhes no guia do usuário para o recurso Remote Storage, que está disponível no centro de documentação E-Series e SANtricity em "Visão geral dos volumes de storage remoto", e no "Relatório técnico de storage remoto".

> SANtricity Remote Storage Volumes atualmente não é suportado em sistemas E4000.

No sistema de storage E-Series:

1. Certifique-se de que cada controlador tenha uma conexão iSCSI com o sistema de storage remoto. Com essa conexão, o sistema E-Series local 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 tenha uma capacidade igual ou superior à do volume de origem no sistema de storage remoto, tenha um tamanho de bloco correspondente e não esteja mapeado. Consulte "Criar volumes".
3. Obtenha o iSCSI Qualified Name (IQN) do sistema E-Series local a partir da interface do System Manager. O IQN será usado posteriormente para configurar o sistema E-Series local como host no sistema de storage remoto. No System Manager, acesse: **Settings › Sistema › iSCSI settings › Target IQN**.

No sistema de storage remoto:

1. Configure o sistema E-Series local como host no sistema remoto, utilizando seu IQN. Certifique-se de definir o tipo de host apropriado, conforme a seguir:
   - Se o sistema remoto for um modelo E-Series, consulte "Visão geral de hosts e clusters de hosts". Use

um tipo de host "Factory Default".

- Se o sistema remoto for de outro fornecedor, selecione um tipo de host apropriado com base nas opções disponíveis.

2. Interrompa todas as operações de E/S, desmonte todos os sistemas de arquivos e remova todas as atribuições a hosts ou aplicativos para o volume de origem.
3. Atribua o volume ao host do sistema de storage E-Series local recém-criado.
4. Para o volume de origem selecionado, reúna as seguintes informações do sistema de storage remoto para que a importação possa ser criada:
   - iSCSI Qualified Name (IQN)
   - endereço IP iSCSI
   - Número LUN do volume de origem

Configuração do System Manager

Utilize o seguinte fluxo de trabalho para criar um objeto de storage remoto para a importação:

1. Usando o assistente de Remote Storage na interface do System Manager, mapeie um dispositivo de storage remoto (a origem para a importação de dados) para um volume de destino no sistema E-Series. Ao selecionar **Concluir**, o processo de importação começa.
2. Acompanhe a importação na caixa de diálogo Exibir operações ou no painel Operações em andamento. Se necessário, você também pode pausar e retomar o processo.
3. Opcionalmente, interrompa a conexão entre os volumes de origem e destino quando a importação for concluída ou mantenha a conexão para importações futuras.

Aprenda sobre a terminologia de armazenamento remoto no software SANtricity

Saiba como os termos de armazenamento remoto se aplicam ao seu array de storage.

Termo	Descrição
IQN	Identificador iSCSI Qualified Name (IQN), que é um nome exclusivo para um iniciador iSCSI ou alvo.
LUN	Número da 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 storage remoto	O dispositivo físico ou lógico onde os dados são inicialmente armazenados no sistema remoto. Em um sistema de storage E-Series, isso é chamado de "volume".
Objeto de storage remoto	Um objeto que contém informações que permitem ao sistema E-Series identificar e conectar-se ao sistema de storage remoto. Essas informações incluem o IQN e os endereços IP do sistema de storage remoto. O objeto de storage remoto representa a comunicação entre o sistema de storage remoto e o sistema E-Series.

Termo	Descrição
Volume de storage remoto	Um volume padrão no sistema E-Series que permite o acesso a dados de um dispositivo de storage remoto.
Volume	Um contêiner no qual os dados são armazenados. É o componente lógico criado para que o host acesse os dados.

Saiba mais sobre os requisitos do recurso Remote Storage no software SANtricity

Antes de usar o recurso Remote Storage, revise os seguintes requisitos e restrições.

Protocolos suportados

Os seguintes protocolos são suportados:

- iSCSI
- IPv4

Para obter informações atualizadas sobre suporte e configuração do E-Series, consulte o "NetApp Ferramenta de Matriz de Interoperabilidade".

Requisitos de hardware

O sistema de storage E-Series deve incluir:

- Dois controladores (modo duplex)
- Conexões iSCSI para ambos os controladores E-Series se comunicarem com o sistema de storage remoto através de uma ou mais conexões iSCSI
- SANtricity OS 11.71 ou superior
- Recurso de storage remoto ativado 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 Remote Storage possui as seguintes restrições:

- O espelhamento deve ser desativado.
- O volume de destino no sistema E-Series não deve ter Snapshots.
- O volume de destino no sistema E-Series não deve ser mapeado para nenhum host antes do início da importação.
- O volume de destino no sistema E-Series deve ter resource-provisioning desativado.
- O mapeamento direto do volume de storage remoto para um host ou vários hosts não é suportado.
- Web Services Proxy não é suportado.
- Segredos CHAP do iSCSI não são suportados.

- SMcli não é suportado.
- VMware Datastore não é compatível.
- Apenas um sistema de storage no par de relacionamento/importação pode ser atualizado por vez quando houver um par de importação presente.

Saiba mais sobre os requisitos de volume de armazenamento remoto no software SANtricity

Os volumes usados para importação devem atender aos requisitos de tamanho, status e outros critérios.

Volume de storage remoto

O volume de origem de uma importação é chamado de "remote storage volume". Esse volume deve atender aos seguintes critérios:

- Não pode fazer parte de outra importação
- Deve ter um status online

Após o início da importação, o firmware do controlador cria um volume de storage remoto em segundo plano. Devido a esse processo em segundo plano, o volume de storage remoto não pode ser gerenciado no System Manager e só pode ser usado para a operação de importação.

Após sua criação, o volume de storage remoto é tratado como qualquer outro volume padrão no sistema E-Series, com as seguintes exceções:

- Podem ser usados como proxies para o dispositivo de storage remoto.
- Não podem ser usados como candidatos para outras cópias de volume ou Snapshots.
- Não é possível alterar a configuração de Data Assurance enquanto a importação estiver em andamento.
- Não podem ser mapeados para nenhum host, porque 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 estar associado a vários volumes de armazenamento remoto. O volume de armazenamento remoto é identificado exclusivamente por meio de uma combinação dos seguintes:

- Identificador de objeto de storage remoto
- Número LUN do dispositivo de storage remoto

Candidatos a volume de destino

O volume alvo é o volume de destino no sistema E-Series local. O volume de destino deve atender aos seguintes critérios:

- Deve ser um volume RAID/DDP.
- Deve ter uma capacidade igual ou superior ao volume de storage remoto.
- Deve ter um tamanho de bloco que seja o mesmo do volume de storage remoto.
- Deve possuir um estado válido (optimal).
- Não pode haver nenhuma das seguintes relações: cópia de volume, cópias de Snapshot, espelhamento

assíncrono ou síncrono.

- Não pode estar passando por nenhuma operação de reconfiguração: Expansão Dinâmica de Volume, Expansão Dinâmica de Capacidade, Tamanho Dinâmico de Segmento, Migração Dinâmica de RAID, Redução Dinâmica de Capacidade ou Desfragmentação.
- Não pode ser mapeado para um host antes do início da importação (no entanto, pode ser mapeado após a importação ser concluída).
- Não é possível ter o Flash Read Cached (FRC) ativado.

System Manager verifica automaticamente esses requisitos como parte do assistente de Import Remote Storage. Somente os volumes que atendem a todos os requisitos são exibidos para seleção do volume de destino.

Gerenciar armazenamento remoto

Importar storage remoto no SANtricity System Manager

Para iniciar uma importação de storage de um sistema remoto para um sistema de storage E-Series local, use o assistente Import Remote Storage.

Antes de começar

- O sistema de storage E-Series deve ser configurado para se comunicar com o sistema de storage remoto.

> A configuração de hardware é descrita no guia do usuário para o recurso Remote Storage, que está disponível no centro de documentação E-Series e SANtricity em "Configurar hardware", e no "Relatório técnico de storage remoto".

- Para o sistema de storage remoto, reúna as seguintes informações:
  - IQN iSCSI
  - Endereços IP iSCSI
  - Número LUN do dispositivo de storage remoto (volume de origem)
- Para o sistema de storage E-Series local, crie ou selecione um volume a ser usado para a importação de dados. Consulte "Criar volumes". O volume de destino deve atender aos seguintes requisitos:
  - Corresponde ao tamanho do bloco do dispositivo de storage (o volume de origem).
  - Possui capacidade igual ou superior à do dispositivo de storage remoto.
  - Encontra-se em estado Ótimo e está disponível.

Para obter uma lista completa de requisitos, consulte "Requisitos de volume de storage remoto".

- **Recomendado:** Faça backup dos volumes no sistema de storage remoto antes de iniciar o processo de importação.

Sobre esta tarefa

Nesta tarefa, você cria um mapeamento entre o dispositivo de storage remoto e um volume no sistema de storage E-Series. Ao concluir a configuração, a importação é iniciada.

Como muitas variáveis podem afetar a operação de importação e seu tempo de conclusão, recomendamos que você primeiro execute importações de "teste" menores. Use esses testes para garantir que todas as conexões funcionem conforme o esperado e que a operação de importação seja concluída em um tempo adequado.

Passos

1. Selecione o menu: storage [remote storage].
2. Clique em **Importar armazenamento remoto**.

   É exibido um assistente para importar storage remoto.

3. Na **Etapa 1a** do painel Configurar Origem, insira as informações de conexão. Se desejar adicionar outra conexão iSCSI, clique em **Adicionar outro endereço IP** para incluir um endereço IP adicional para o storage remoto. Quando terminar, clique em **Avançar**.

   Detalhes do campo

Configuração	Descrição
Nome	Insira um nome para o dispositivo de storage remoto para identificá-lo na interface do System Manager. Um nome pode ter até 30 caracteres e pode conter apenas letras, números e os seguintes caracteres especiais: sublinhado (_), hífen (-) e cerquilha (#). Um nome não pode conter espaços.
Propriedades da conexão iSCSI	Insira as propriedades de conexão do dispositivo de storage remoto: • **iSCSI Qualified Name (IQN)**: Insira o iSCSI IQN. • **Endereço IP**: digite o endereço IPv4. • **Porta**: insira o número da porta a ser usada para comunicação entre os dispositivos de origem e destino. Por padrão, o número da porta é 3260.

   Após clicar em **Avançar**, a **Etapa 1b** do painel Configurar Fonte é exibida.

4. No campo **LUN**, selecione o número LUN do dispositivo de storage remoto a ser usado como origem e clique em **Avançar**.

   O painel Configurar Destino é aberto e exibe os volumes candidatos que podem servir como destino para a importação. Alguns volumes não são exibidos na lista de candidatos devido ao tamanho do bloco, capacidade ou disponibilidade do 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 **Avançar**. Confirme a operação na próxima caixa de diálogo digitando `continue`, e em seguida clicando em **Continuar**.

   Se o volume de destino tiver uma capacidade maior que o volume de origem, essa capacidade adicional não será informada ao host conectado ao sistema E-Series. Para usar a nova capacidade, você deve executar uma operação de expansão do sistema de arquivos no host após a conclusão da operação de

importação e a desconexão.

Após confirmar a configuração na caixa de diálogo, o painel de revisão é exibido.

6. No painel Review, verifique se as configurações estão corretas e clique em **Concluir** para iniciar a importação.

   Outra caixa de diálogo será aberta perguntando se você deseja iniciar outra importação.

7. Se necessário, clique em **Sim** para criar outra importação de storage remoto. Clicar em **Sim** retorna à **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 **Não** para sair da caixa de diálogo.

   Assim que o processo de importação se inicia, todo o volume de destino é sobrescrito com os dados copiados. Se o host gravar novos dados no volume de destino durante esse processo, esses novos dados são propagados de volta para o dispositivo remoto (volume de origem).

8. Veja o progresso da operação na caixa de diálogo View Operations, no painel Remote Storage.

Resultados

O tempo necessário para concluir a operação de importação depende do tamanho do sistema de storage remoto, da prioridade definida para a importação e da quantidade de carga de E/S em ambos os sistemas de storage e seus respectivos volumes.

Após a conclusão da importação, o volume local torna-se uma duplicata do dispositivo de storage remoto.

Depois que você terminar

Quando estiver pronto para desvincular os dois volumes, selecione **Desconectar** no objeto de importação na visualização Operações em Andamento. Assim que a relação for desconectada, o desempenho do volume local retorna ao normal e não é mais afetado pela conexão remota.

Gerencie o progresso das importações de storage remoto no SANtricity System Manager

Após o início do processo de importação, você pode visualizar e tomar medidas sobre o seu progresso.

Sobre esta tarefa

Para cada operação de importação, a caixa de diálogo Operações em Andamento exibe uma porcentagem de conclusão e o tempo restante estimado. As ações incluem alterar a prioridade da importação, interromper e retomar operações e desconectar-se da operação.

Você também pode visualizar as operações em andamento na página inicial (**Home › Mostrar operações em andamento**).

Passos

1. Na página Remote Storage, selecione **View Operations**.

   A caixa de diálogo Operações em andamento é exibida.

2. Se desejar, utilize os links na coluna **Ações** para interromper e retomar, alterar a prioridade ou desconectar de uma operação.
   - **Alterar Prioridade** — Selecione **Alterar Prioridade** para alterar a prioridade de processamento de uma operação em andamento ou pendente. Atribua uma prioridade à operação e clique em **OK**.

- **Parar** — Selecione **Parar** para pausar a cópia de dados do dispositivo de storage remoto. A relação entre o par de importação permanece intacta e você pode selecionar **Retomar** quando estiver pronto para continuar a operação de importação.
- **Retomar** — Selecione **Retomar** para iniciar um processo interrompido ou com falha a partir do ponto em que parou. Em seguida, aplique uma prioridade à operação Retomar e clique em **OK**. Esta operação *não* reinicia a importação desde o início. Se você quiser reiniciar o processo desde o início, será necessário selecionar **Desconectar** e, em seguida, recriar a importação por meio do assistente Import Remote Storage.
- **Desconectar** — Selecione **Desconectar** para interromper a relação entre os volumes de origem e destino de uma operação de importação que foi interrompida, concluída ou falhou.

Modifique as configurações de conexão para storage remoto no SANtricity System Manager

Você pode editar, adicionar ou excluir configurações de conexão para qualquer configuração de storage por meio da opção View/Edit Settings.

Sobre esta tarefa

Alterar as propriedades de conexão afetará as importações em andamento. Para evitar interrupções, faça alterações nas propriedades de conexão somente quando as importações não estiverem em execução.

Passos

1. Selecione o menu: storage [remote storage].
2. Na lista, selecione o objeto de storage remoto que deseja modificar.
3. Clique em **Ver/Editar Settings**.

   A caixa de diálogo Configurações de storage remoto é exibida.

4. Clique na guia **Connection Properties**.

   São exibidas as configurações de endereço IP e porta configuradas para a importação do storage remoto.

5. Execute uma das seguintes ações:
   - **Editar** — Clique em **Editar** ao lado do item de linha correspondente para o objeto de storage remoto. Insira o endereço IP revisado e/ou as informações de porta nos campos.
   - **Adicionar** — Clique em **Adicionar** e, em seguida, insira o novo endereço IP e as informações da porta nos campos fornecidos. Clique em **Adicionar** para confirmar e, em seguida, a nova conexão aparecerá na lista de objetos de storage 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 storage remoto.
6. Clique em **Salvar**.

   As configurações de conexão modificadas são aplicadas ao objeto de storage remoto.

Remova um objeto de storage remoto no SANtricity System Manager

Após a conclusão de uma importação, você pode remover um objeto de storage remoto se não quiser mais que os dados sejam copiados entre os dispositivos local e remoto.

Antes de começar

Certifique-se de que não haja importações associadas ao objeto de storage remoto que você planeja remover.

Sobre esta tarefa

Ao remover um objeto de storage remoto, as conexões entre os dispositivos local e remoto são removidas.

Passos

1. Selecione o menu: storage [remote storage].
2. Na lista, selecione o objeto de storage remoto que você deseja remover.
3. Clique em **Remover**.

   A caixa de diálogo Confirm Remove Remote Storage Connection é exibida.

4. Confirme a operação digitando `remove` e depois clicando em **Remover**.

   O objeto de storage remoto selecionado foi removido.

Perguntas frequentes sobre storage remoto para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

O que preciso saber antes de criar uma conexão de storage remoto?

Para configurar o recurso Remote Storage, você deve conectar diretamente o dispositivo remoto e os sistemas de storage de destino via iSCSI.

Para configurar a conexão do sistema iSCSI, consulte:

- "Configurar portas iSCSI"
- "Relatório técnico de storage remoto"

Por que estou sendo solicitado a remover meus volumes remotos?

Quando atinge o número máximo de volumes remotos, o sistema de storage detecta automaticamente quaisquer volumes remotos não utilizados e solicita que você os remova.

Em alguns casos, os volumes remotos não utilizados não são removidos durante o processo de criação. Antes de iniciar qualquer operação de importação adicional, verifique se seus sistemas estão otimizados e se as conexões de rede estão estáveis.

Por que não vejo todos os meus volumes no meu array de destino?

Ao configurar uma importação para o recurso Remote Storage, você pode notar que alguns volumes não aparecem na lista de candidatos a destino devido ao tamanho do bloco, capacidade ou disponibilidade do volume.

Para aparecer na lista, os candidatos a volume devem ter:

- Capacidade que é igual ou superior ao volume remoto.
- Tamanho do bloco que é o mesmo do volume remoto.

- Status atual de Optimal.

Os volumes candidatos são excluídos da lista se eles tiverem:

- Qualquer uma das seguintes relações: cópia de volume, snapshot ou espelhamento.
- Operação de reconfiguração em andamento.
- Mapeamento para outro dispositivo (host ou host cluster).
- Leitura do flash cache ativada.

O que preciso saber sobre o volume remoto em uma importação?

Ao usar o recurso Remote Storage, esteja ciente de que o volume remoto é a origem de onde os dados se originam.

Quando a importação está em andamento, os dados são transferidos do volume remoto para o volume de destino no sistema de storage de destino. Esses dois volumes devem ter o mesmo tamanho de bloco.

O que preciso saber antes de iniciar uma importação de storage remoto?

O recurso de Remote Storage permite copiar dados de um sistema de storage remoto para um volume em um sistema de storage E-Series. Antes de usar esse recurso, revise as seguintes diretrizes.

Configuração

Antes de criar a importação de storage remoto, você deve concluir as seguintes ações e verificar as seguintes condições:

- Certifique-se de que cada controlador do sistema de storage E-Series tenha uma conexão iSCSI com o sistema de storage remoto.
- No seu sistema de storage E-Series local, crie um volume de destino para a operação de importação. Certifique-se de que o volume tenha uma capacidade igual ou superior à do volume de origem, tenha um tamanho de bloco que corresponda ao do volume de origem e que não esteja mapeado. Consulte "Criar volumes".
- Configurar o sistema de storage E-Series como host no sistema remoto usando seu iSCSI Qualified Name (IQN). Você pode visualizar o IQN em **Settings › Sistema › iSCSI settings › Target IQN**. Além disso, certifique-se de definir o tipo de host apropriado com base no sistema que está sendo usado.
- Interrompa todas as operações de I/Os, desmonte todos os sistemas de arquivos e remova todas as atribuições a hosts ou aplicativos para o volume selecionado no sistema de storage remoto.
- Atribua o volume ao sistema de storage remoto ao host do novo sistema de storage E-Series local.
- Reúna as seguintes informações do sistema de storage remoto para que a importação possa ser criada:
  - iSCSI Qualified Name (IQN)
  - endereço IP iSCSI
  - O número LUN do dispositivo de storage remoto, de onde os dados de origem se originam
- Assim que o processo de importação é iniciado, todo o volume de destino local é sobrescrito com os dados copiados. Quaisquer novos dados gravados no volume de destino local são propagados para o volume no dispositivo de storage remoto após a criação da importação. Portanto, recomendamos que você faça backup dos volumes no sistema de storage 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, em seguida, vá para a página **Remote Storage**. Selecione **Import** para iniciar uma nova importação. Para obter instruções detalhadas, consulte "Importar storage remoto".

   Se você deseja realizar uma importação offline, não mapeie o volume de destino até que a importação seja concluída.

2. Monitore 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 storage (volume de origem), da prioridade definida para a importação e da quantidade de carga de E/S em ambos os sistemas de storage e seus respectivos volumes.

   Após a conclusão da importação, o volume de destino é uma duplicata do volume de origem.

3. Quando estiver pronto para romper o relacionamento de mapeamento, execute uma **Disconnect** no objeto de importação no painel **Operations In Progress**.

Assim que a importação for desconectada, o desempenho do destino local retorna ao normal e não é mais afetado pela conexão remota.

Restrições

O recurso Remote Storage possui as seguintes restrições:

- O espelhamento deve ser desativado.
- O volume de destino no sistema E-Series não deve ter Snapshots.
- O volume de destino no sistema E-Series não deve ser mapeado para nenhum host antes do início da importação.
- O volume de destino no sistema E-Series deve ter resource-provisioning desativado.
- O mapeamento direto do volume de storage remoto para um host ou vários hosts não é suportado.
- Web Services Proxy não é suportado.
- Segredos CHAP do iSCSI não são suportados.
- SMcli não é suportado.
- VMware Datastore não é compatível.
- Apenas um sistema de storage no par de relacionamento/importação pode ser atualizado por vez quando houver um par de importação presente.

Informações adicionais

Informações adicionais sobre o recurso Remote Storage estão disponíveis em "Relatório técnico de storage remoto".

Componentes de hardware

Visualize e gerencie componentes de hardware no SANtricity System Manager

Você pode verificar o status do componente na página Hardware e executar algumas funções relacionadas a esses componentes.

Quais componentes posso gerenciar?

Você pode verificar o status dos componentes e executar algumas funções relacionadas a esses componentes:

- **Prateleiras** — Uma *prateleira* é um componente que contém o hardware do array de storage (controladores, fontes de alimentação/ventoinhas e unidades). As prateleiras estão disponíveis em três tamanhos para acomodar até 12, 24 ou 60 unidades.
- **Controladores** — Um *controlador* é o conjunto de hardware e firmware que implementa as funções do array de storage e de gerenciamento. Inclui a memória cache, o suporte a unidades e as portas para conexões com o host.
- **Unidades** — Uma unidade pode ser um disco rígido (HDD) ou uma unidade de estado sólido (SSD). Dependendo do tamanho do gabinete, é possível instalar até 12, 24 ou 60 unidades.

Saiba mais:

- "Página de hardware"
- "Terminologia de hardware"

Como faço para visualizar os componentes de hardware?

Acesse a página Hardware, que fornece uma representação gráfica dos componentes físicos do array de storage. Você pode alternar entre as visualizações frontal e traseira dos gabinetes do array selecionando a guia **Unidades** ou **Controladores** no canto superior direito da visualização do gabinete.

Saiba mais:

- "Visualizar o status e as configurações dos componentes da prateleira"
- "Exibir configurações do controlador"
- "Visualizar o status e as configurações da unidade"

Informações relacionadas

Saiba mais sobre conceitos relacionados a hardware:

- "Estados do controlador"
- "Estados da unidade"
- "Proteção contra perda de prateleira e proteção contra perda de gaveta"

Conceitos

Página de hardware e componentes do SANtricity System Manager

A página Hardware fornece uma representação gráfica dos componentes físicos do array de storage. A partir daqui, você pode verificar o status dos componentes e executar algumas funções relacionadas a esses componentes.

Prateleiras

Um shelf é um componente que contém o hardware do array de storage (controladores, fontes de alimentação/ventoinhas e unidades de disco). Existem dois tipos de shelf:

- **Compartimento do controlador** — Contém as unidades, as fontes de alimentação/ventoinhas e os controladores.
- **Compartimento de unidades** (ou **compartimento de expansão**) — Contém unidades, fontes de alimentação/ventoinhas e dois módulos de entrada/saída (IOMs). Os IOMs, também conhecidos como módulos de serviço ambiental (ESMs), incluem portas SAS que conectam o compartimento de unidades ao compartimento do controlador.

As prateleiras estão disponíveis em três tamanhos para acomodar até 12, 24 ou 60 unidades. Cada prateleira inclui um número de identificação, que é atribuído pelo firmware do controlador. O número de identificação aparece no canto superior esquerdo da visualização da prateleira.

A visualização da prateleira na página Hardware mostra os componentes da parte frontal ou traseira. Você pode alternar entre as duas visualizações selecionando as abas **Unidades** ou **Controladores** no canto superior direito da visualização da prateleira. Você também pode selecionar **Mostrar todos os frontais** ou **Mostrar todos os traseiros** na parte inferior da página. As visualizações frontal e traseira mostram o seguinte:

- **Componentes frontais** — Unidades e baias de unidade vazias.
- **Componentes traseiros** — Controladores e compartimentos de alimentação/ventoinhas (para compartimentos de controladores) ou os IOMs e compartimentos de alimentação/ventoinhas (para compartimentos de unidades).

Você pode executar as seguintes funções relacionadas aos compartimentos de expansão:

- Acenda a luz localizadora da prateleira, para que você possa encontrar a localização física da prateleira no armário ou rack.
- Altere o número de ID exibido no canto superior esquerdo da visualização da shelf.
- Veja as configurações do compartimento, como os tipos de unidades instaladas e o número de série.
- Mova as visualizações das prateleiras para cima ou para baixo para corresponder ao layout físico no array de storage.

Controladores

Um controlador é o conjunto de hardware e firmware que implementa as funções do array de storage e de gerenciamento. Ele inclui a memória cache, o suporte a unidades e o suporte à interface com o host.

Você pode executar as seguintes funções relacionadas aos controladores:

- Configure as portas de gerenciamento para endereços IP e velocidade.
- Configure as conexões de host iSCSI (se você tiver hosts iSCSI).

- Configure um servidor de Protocolo de Tempo de Rede (NTP) e um servidor de Sistema de Nomes de Domínio (DNS).
- Visualizar o status e as configurações do controlador.
- Permita que usuários de fora da rede local iniciem uma sessão SSH e alterem as configurações do controlador.
- Coloque o controlador offline, online ou em modo de serviço.

Unidades

O array de storage pode incluir discos rígidos (HDDs) ou unidades de estado sólido (SSDs). Dependendo do tamanho do compartimento, até 12, 24 ou 60 unidades podem ser instaladas no compartimento.

Você pode executar as seguintes funções relacionadas a unidades:

- Acenda a luz localizadora da unidade, para que você possa encontrar a localização física da unidade no compartimento.
- Visualizar o status e as configurações da unidade.
- Reatribua uma unidade (substitua logicamente uma unidade com falha por uma unidade não atribuída) e reconstrua manualmente a unidade, se necessário.
- Faça uma unidade falhar manualmente para que você possa substituí-la. (Fazer uma unidade falhar permite que você copie o conteúdo da unidade antes de substituí-la.)
- Atribuir ou remover a atribuição de hot spares.
- Apagar unidades.

Aprenda sobre a terminologia de hardware usada no software SANtricity

Os seguintes termos de hardware aplicam-se a arrays de storage.

Termos gerais de hardware:

Componente	Descrição
Baía	Uma baia é um slot no compartimento onde uma unidade ou outro componente é instalado.
Controlador	Um controlador consiste em uma placa, firmware e software. Ele controla as unidades e implementa as funções do System Manager.
Compartimento do controlador	Um gabinete de controladores contém um conjunto de unidades de disco e um ou mais compartimentos de controladores. Um compartimento de controladores abriga os controladores, as placas de interface do host (HICs) e as baterias.
Drive	Um drive é um dispositivo mecânico eletromagnético ou um dispositivo de memória de estado sólido que fornece o storage físico para os dados.
Compartimento de unidade	Um compartimento de unidades, também chamado de compartimento de expansão, contém um conjunto de unidades e dois módulos de entrada/saída (IOMs). Os IOMs contêm portas SAS que conectam um compartimento de unidades a um compartimento de controlador ou a outros compartimentos de unidades.
IOM (ESM)	Um IOM é um módulo de entrada/saída que inclui portas SAS para conectar o compartimento de unidades ao compartimento do controlador. Em modelos de controladores anteriores, o IOM era chamado de módulo de serviço ambiental (ESM).
Fonte de alimentação/ventilador	Um compartimento para fonte de alimentação/ventilador é um conjunto que desliza para dentro de um compartimento. Ele inclui uma fonte de alimentação e um ventilador integrado.
SFP	Um SFP é um transceptor Small Form-factor Pluggable (SFP).
Compartimento	Um shelf é um compartimento instalado em um gabinete ou rack. Ele contém os componentes de hardware para o array de storage. Existem dois tipos de shelf: um controller shelf e um drive shelf. Um controller shelf inclui controladores e unidades. Um drive shelf inclui módulos de entrada/saída (IOMs) e unidades.
Array de storage	Um array de storage inclui os compartimentos, controladores, unidades, software e firmware.

Termos do controlador:

Componente	Descrição
Controlador	Um controlador consiste em uma placa, firmware e software. Ele controla as unidades e implementa as funções do System Manager.
Compartimento do controlador	Um gabinete de controladores contém um conjunto de unidades de disco e um ou mais compartimentos de controladores. Um compartimento de controladores abriga os controladores, as placas de interface do host (HICs) e as baterias.
DHCP	Dynamic Host Configuration Protocol (DHCP) é um protocolo usado em redes de Protocolo de Internet (IP) para distribuir dinamicamente parâmetros de configuração de rede, como endereços IP.
DNS	O Sistema de Nomes de Domínio (DNS) é um sistema de nomenclatura para dispositivos conectados à Internet ou a uma rede privada. O servidor DNS mantém um diretório de nomes de domínio e os traduz para endereços de Protocolo de Internet (IP).
Configurações duplex	Duplex é uma configuração de módulo com dois controladores dentro do array de storage. Os sistemas duplex são totalmente redundantes em relação aos controladores, caminhos de volume lógico e caminhos de disco. Se um controlador falhar, o outro controlador assume sua E/S para manter a disponibilidade. Os sistemas duplex também possuem ventiladores e fontes de alimentação redundantes.
Conexões full-duplex / half-duplex	Full-duplex e half-duplex referem-se a 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 por 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 gabinete de controlador. As portas de host integradas ao controlador são chamadas de portas de host baseboard. As portas de host integradas à HIC são chamadas de portas HIC.
Resposta ICMP PING	O Protocolo de Mensagens de Controle da Internet (ICMP) é um protocolo usado pelos sistemas operacionais de computadores em rede para enviar mensagens. As mensagens ICMP determinam se um host está acessível e quanto tempo leva para que os pacotes sejam enviados e recebidos desse host.
Endereço MAC	Os identificadores de controle de acesso ao meio (endereços MAC) são usados pelo Ethernet para distinguir entre canais lógicos separados que conectam duas portas na mesma interface de rede física de transporte.

Componente	Descrição
cliente de gerenciamento	Um cliente de gerenciamento é o computador onde um navegador está instalado para acessar System Manager.
MTU	A Maximum Transmission Unit (MTU) é o maior pacote ou quadro que pode ser enviado em uma rede.
NTP	O Network Time Protocol (NTP) é um protocolo de rede para sincronização de clock entre sistemas de computador em redes de dados.
Configurações simplex	O simplex é uma configuração de módulo com um único controlador dentro do array de storage. Um sistema simplex não oferece redundância de controlador ou de caminho de disco, mas possui ventiladores e fontes de alimentação redundantes.
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 de unidade:

Componente	Descrição
DA	O Data Assurance (DA) é um recurso que verifica e corrige erros que podem ocorrer durante a transferência de dados pelos controladores até as unidades de disco. O Data Assurance pode ser ativado no nível do pool ou do grupo de volume, com hosts que utilizam uma interface de I/O compatível com DA, como Fibre Channel.
Recurso de segurança da unidade	Drive Security é um recurso do array de storage que fornece uma camada extra de segurança com unidades Full Disk Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS). Quando essas unidades são usadas com o recurso Drive Security, elas exigem uma chave de segurança para acesso aos seus dados. Quando as unidades são fisicamente removidas do array, elas não podem operar até serem instaladas em outro array; nesse momento, elas estarão em um estado Security Locked até que a chave de segurança correta seja fornecida.
Compartimento de unidade	Um compartimento de unidades, também chamado de compartimento de expansão, contém um conjunto de unidades e dois módulos de entrada/saída (IOMs). Os IOMs contêm portas SAS que conectam um compartimento de unidades a um compartimento de controlador ou a outros compartimentos de unidades.
DULBE	O erro Deallocated or Unwritten Logical Block Error (DULBE) é uma opção em unidades NVMe que permite que o array de storage EF300 ou EF600 suporte volumes com recursos provisionados.
Unidades FDE	Unidades com criptografia de disco completa (FDE) realizam criptografia na unidade de disco no nível do hardware. O disco rígido contém um chip ASIC que criptografa os dados durante as gravações e os descriptografa durante as leituras.
Unidades FIPS	Unidades FIPS utilizam o Federal Information Processing Standards (FIPS) 140-2 nível 2. Essencialmente, são unidades FDE que seguem os padrões do governo dos Estados Unidos para garantir algoritmos e métodos de criptografia robustos. Unidades FIPS possuem padrões de segurança mais elevados do que unidades FDE.
HDD	Os discos rígidos (HDDs) são dispositivos de storage que utilizam discos metálicos giratórios com revestimento magnético.
Hot spare	Hot spares atuam como unidades de espera em grupos de volume RAID 1, RAID 5 ou RAID 6. São unidades totalmente funcionais que não contêm dados. Se uma unidade falhar no grupo de volume, o controlador reconstrói automaticamente os dados da unidade com falha para um hot spare.

Componente	Descrição
NVMe	Non-Volatile Memory Express (NVMe) é uma interface projetada para dispositivos de storage baseados em flash, como unidades SSD. NVMe reduz a sobrecarga de E/S e inclui melhorias de desempenho em comparação com interfaces de dispositivos lógicos anteriores.
SAS	Serial Attached SCSI (SAS) é um protocolo serial ponto a ponto que conecta controladores diretamente a unidades de disco.
Unidades com capacidade de segurança	Unidades com capacidade de segurança podem ser unidades Full Disk Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS), que criptografam os dados durante as gravações e descriptografam os dados durante as leituras. Essas unidades são consideradas secure-*capable* porque podem ser usadas para segurança adicional usando o recurso Drive Security. Se o recurso Drive Security estiver habilitado para grupos de volume e pools usados com essas unidades, as unidades se tornam secure-*enabled*.
Unidades com segurança ativada	Unidades com segurança habilitada são usadas com o recurso Drive Security. Quando você habilita o recurso Drive Security e, em seguida, aplica Drive Security a um pool ou grupo de volume em unidades secure-capable, as unidades passam a ser secure-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 foi fisicamente removida do array de storage.
SSD	Discos de estado sólido (SSDs) são dispositivos de storage que utilizam memória de estado sólido (flash) para armazenar dados de forma permanente. SSDs emulam discos rígidos convencionais e estão disponíveis com as mesmas interfaces que os discos rígidos utilizam.

Termos iSCSI:

Termo	Descrição
CHAP	O método Challenge Handshake Authentication Protocol (CHAP) valida a identidade de destinos 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. Ele controla as unidades e implementa as funções do System Manager.
DHCP	Dynamic Host Configuration Protocol (DHCP) é um protocolo usado em redes de Protocolo de Internet (IP) para distribuir dinamicamente parâmetros de configuração de rede, como endereços IP.
IB	InfiniBand (IB) é um padrão de comunicação para transmissão de dados entre servidores de alto desempenho e sistemas de storage.
Resposta ICMP PING	O Protocolo de Mensagens de Controle da Internet (ICMP) é um protocolo usado pelos sistemas operacionais de computadores em rede para enviar mensagens. As mensagens ICMP determinam se um host está acessível e quanto tempo leva para que os pacotes sejam enviados e recebidos desse host.
IQN	Um identificador iSCSI Qualified Name (IQN) é um nome exclusivo para um iniciador iSCSI ou destino iSCSI.
iSER	iSCSI Extensions for RDMA (iSER) é um protocolo que estende o protocolo iSCSI para operação em transportes RDMA, como InfiniBand ou Ethernet.
iSNS	O Internet Storage Name Service (iSNS) é um protocolo que permite a detecção automatizada, o gerenciamento e a configuração de dispositivos iSCSI e Fibre Channel em redes TCP/IP.
Endereço MAC	Os identificadores de controle de acesso ao meio (endereços MAC) são usados pelo Ethernet para distinguir entre canais lógicos separados que conectam duas portas na mesma interface de rede física de transporte.
Cliente de gerenciamento	Um cliente de gerenciamento é o computador onde um navegador está instalado para acessar System Manager.
MTU	A Maximum Transmission Unit (MTU) é o maior pacote ou quadro que pode ser enviado em uma rede.
RDMA	Remote Direct Memory Access (RDMA) é uma tecnologia que permite que computadores em rede troquem dados na memória principal sem envolver o sistema operacional de nenhum dos computadores.

Termo	Descrição
Sessão de detecção automatizada sem nome	Quando a opção para sessões de descoberta sem nome está habilitada, os iniciadores iSCSI não precisam especificar o IQN de destino para recuperar as informações do controlador.

Termos NVMe:

Termo	Descrição
InfiniBand	InfiniBand (IB) é um padrão de comunicação para transmissão de dados entre servidores de alto desempenho e sistemas de storage.
Espaço de nomes	Um namespace é um storage NVM formatado para acesso em bloco. É análogo a uma unidade lógica em SCSI, que se relaciona a um volume no array de storage.
ID do namespace	O ID do namespace é o identificador exclusivo do controlador NVMe para o namespace e pode ser definido com um valor entre 1 e 255. É análogo a um número de unidade lógica (LUN) em SCSI.
NQN	NVMe Qualified Name (NQN) é usado para identificar o destino de armazenamento remoto (o array de storage).
NVM	A memória não volátil (NVM) é memória persistente usada em muitos tipos de dispositivos de storage.
NVMe	Non-Volatile Memory Express (NVMe) é uma interface projetada para dispositivos de storage baseados em flash, como unidades SSD. NVMe reduz a sobrecarga de E/S e inclui melhorias de desempenho em comparação com interfaces de dispositivos lógicos anteriores.
NVMe-oF	Non-Volatile Memory Express over Fabrics (NVMe-oF) é uma especificação que permite que comandos e dados NVMe sejam transferidos por uma rede entre um host e um array de storage.
Controlador NVMe	Um controlador NVMe é criado durante o processo de conexão do host. Ele fornece um caminho de acesso entre um host e os namespaces no array de storage.
Fila NVMe	Uma fila é usada para transmitir comandos e mensagens pela interface NVMe.
Subsistema NVMe	O array de storage com uma conexão de host NVMe.
RDMA	O acesso direto à memória remota (RDMA) permite uma movimentação de dados mais direta para dentro e para 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 o acesso direto à memória remota (RDMA) em uma rede Ethernet.

Termo	Descrição
SSD	Discos de estado sólido (SSDs) são dispositivos de storage que utilizam memória de estado sólido (flash) para armazenar dados de forma permanente. SSDs emulam discos rígidos convencionais e estão disponíveis com as mesmas interfaces que os discos rígidos utilizam.

Gerenciar componentes de prateleira

Visualizar os componentes de hardware no SANtricity System Manager

A página Hardware oferece funções de classificação e filtragem que facilitam a localização de componentes.

Passos

1. Selecione **Hardware**.
2. Utilize as funções descritas na tabela a seguir para visualizar os componentes de hardware.

Função	Descrição
Vistas de drives, controladores e componentes	Para alternar entre as visualizações da prateleira frontal e traseira, selecione **Unidades** ou **Controladores & Componentes** no canto direito (o link que aparece depende da visualização atual). A visualização **Unidades** mostra as unidades e quaisquer baias de unidade vazias. A visualização **Controladores & Componentes** mostra os controladores e quaisquer módulos IOM (ESM), compartimentos de alimentação/ventoinhas ou baias de controlador vazias. Na parte inferior da página, você também pode selecionar **Mostrar todas as unidades**.
Filtros de visualização de unidades	Se o array de storage contiver unidades com diferentes tipos de atributos físicos e lógicos, a página **Hardware** inclui filtros de visualização de unidades. Esses campos de filtro ajudam você a localizar rapidamente unidades específicas, limitando os tipos de unidade 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 no array de storage**) para ver uma lista suspensa de atributos lógicos (por exemplo, atribuição de grupo de volume). Você pode usar esses filtros juntos ou separadamente. Se o array de storage contiver unidades que compartilham os mesmos atributos físicos, o campo **Qualquer tipo de unidade** à esquerda não será exibido. Se as unidades estiverem todas na mesma localização lógica, o campo **Em qualquer lugar no array de storage** à direita não será exibido.
Legenda	Os componentes são exibidos em determinadas cores para representar seus estados de função. Para expandir e recolher as descrições desses estados, clique em **Legend**.

Função	Descrição
Mostrar detalhes do ícone de status	Os indicadores de status podem incluir descrições textuais para os estados de disponibilidade. Clique em **Mostrar detalhes do ícone de status** para exibir ou ocultar esse texto de status.
Prateleira/ícones de prateleira	Cada visualização da 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 na parte superior para ver o status e as propriedades de componentes individuais: controladores, IOMs (ESMs), fontes de alimentação, ventoinhas, temperatura, baterias e SFPs.
Ordem da prateleira	As prateleiras podem ser reorganizadas na página de Hardware. Use as setas para cima e para baixo no canto superior direito de cada visualização de prateleira para alterar a ordem superior/inferior das prateleiras.

Exibir ou ocultar o status do componente em SANtricity System Manager

Você pode exibir descrições de status para unidades, controladores, ventoinhas e fontes de alimentação.

Passos

1. Selecione **Hardware**.
2. Para visualizar os componentes da parte traseira ou frontal:
   - Se você deseja visualizar o controlador e os componentes do compartimento de alimentação/ventoinha, mas os drives estão sendo exibidos, clique na guia **Controllers & Components**.
   - Se você deseja visualizar as unidades, mas os componentes do controlador e do compartimento de alimentação/ventoinha estão sendo exibidos, clique na guia **Drives**.
3. Para visualizar ou ocultar as descrições de status 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 visualização da shelf (selecione a caixa de seleção).
   - Para ocultar as descrições pop-over, clique novamente em **Mostrar detalhes do ícone de status** (desmarque a caixa de seleção).
4. Se você quiser ver detalhes completos do status, selecione o componente na visualização da prateleira e, em seguida, selecione **View settings**.
5. Se você quiser visualizar as descrições dos componentes coloridos, selecione **Legend**.

Exibir vistas frontal e traseira no SANtricity System Manager

A página de hardware pode mostrar a vista frontal ou a vista traseira das prateleiras.

Sobre esta tarefa

A vista traseira mostra os controladores/IOMs e os compartimentos dos ventiladores de alimentação. A vista frontal mostra as unidades.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

   O gráfico muda para mostrar os controladores em vez das unidades de disco.

3. Se a imagem mostrar os controladores, clique na guia **Drives**.

   O gráfico muda para mostrar as unidades em vez dos controladores.

4. Opcionalmente, você pode selecionar **Mostrar toda a frente** ou **Mostrar toda a parte de trás**, localizados na parte inferior da página.

Alterar a ordem de visualização das prateleiras no SANtricity System Manager

Você pode alterar a ordem das prateleiras exibidas na página Hardware para corresponder à ordem física das prateleiras em um armário.

Passos

1. Selecione **Hardware**.
2. ${post_edited_translations.segment}

Ative a luz localizadora de prateleira no SANtricity System Manager

Para localizar fisicamente uma prateleira exibida na página de Hardware, você pode acender a luz localizadora da prateleira.

Passos

1. Selecione **Hardware**.
2. Selecione a lista suspensa para a Prateleira do Controlador ou Prateleira da Unidade e, em seguida, selecione **Ligar luz indicadora**.

   A luz indicadora da prateleira acende.

3. Quando você localizar fisicamente a prateleira, retorne à caixa de diálogo e selecione **Desligar**.

Alterar IDs de shelf no SANtricity System Manager

O ID da prateleira é um número que identifica exclusivamente uma prateleira no array de storage. As prateleiras são numeradas consecutivamente, começando com 00 ou 01, no canto superior esquerdo de cada visualização da prateleira.

Sobre esta tarefa

O firmware do controlador atribui automaticamente o ID da prateleira, mas você pode alterar esse número se quiser criar um esquema de organização diferente.

Passos

1. Selecione **Hardware**.
2. Selecione a lista suspensa para a Prateleira do Controlador ou Prateleira da Unidade e, em seguida, selecione **Alterar ID**.
3. Na caixa de diálogo Change Shelf ID, selecione a lista suspensa para exibir os números disponíveis.

Esta caixa de diálogo não exibe os IDs atualmente atribuídos às prateleiras ativas.

4. Selecione um número disponível e clique em **Save**.

   Dependendo do número selecionado, a ordem das prateleiras pode ser reorganizada na página Hardware. Se desejar, você pode usar as setas para cima/para baixo no canto superior direito de cada prateleira para reajustar a ordem.

Visualize o status e as configurações dos componentes da prateleira em SANtricity System Manager

A página Hardware fornece o status e as configurações dos componentes do shelf, incluindo as fontes de alimentação, os ventiladores e as baterias.

Sobre esta tarefa

Os componentes disponíveis dependem do tipo de shelf:

- **Compartimento para unidades** — Contém um conjunto de unidades de disco, fontes de alimentação/ventoinhas, módulos de entrada/saída (IOMs) e outros componentes de suporte em uma única prateleira.
- **Compartimento do controlador** — Contém um conjunto de unidades de disco, um ou dois canisters de controlador, canisters de fonte de alimentação/ventoinha e outros componentes de suporte em um único compartimento.

Passos

1. Selecione **Hardware**.
2. Selecione a lista suspensa para Controller Shelf ou Drive Shelf e, em seguida, selecione **Exibir configurações**.

   A caixa de diálogo Configurações dos Componentes da Prateleira é aberta, com guias que mostram o status e as configurações relacionadas aos componentes da prateleira. Dependendo do tipo de prateleira selecionado, algumas guias descritas na tabela podem não aparecer.

Aba	Descrição
Compartimento	A guia **Shelf** mostra as seguintes propriedades: • **ID da Prateleira** — Identifica exclusivamente uma prateleira no array de storage. O firmware do controlador atribui esse número, mas você pode alterá-lo selecionando **Shelf › Change ID**. • **Shelf path redundancy** — Especifica se as conexões entre o shelf e o controlador possuem métodos alternativos (Sim) ou não (Não). • **Tipos de unidade atuais** — Mostra o tipo de tecnologia integrada às unidades (por exemplo, uma unidade SAS com capacidade de segurança). Se houver mais de um tipo de unidade, ambas as tecnologias serão exibidas. • **Número de série** — Mostra o número de série da shelf.

Aba	Descrição
IOMs (ESMs)	A aba **IOMs (ESMs)** mostra o status do módulo de entrada/saída (IOM), também 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 da unidade e o controlador. O status pode ser Ideal, Falha, Ideal (Conexão Incorreta) ou Não Certificado. Outras informações incluem a versão do firmware e a versão das configurações de configuração. Selecione **Mostrar mais configurações** para ver as taxas de dados máxima e atual, e o estado da comunicação do cartão (Sim ou Não). Você também pode visualizar esse status selecionando o ícone IOM, ao lado da lista suspensa Shelf.
Fontes de alimentação	A aba **Fontes de Alimentação** mostra o status do canister 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. Você também pode visualizar esse status selecionando o ícone da fonte de alimentação, ao lado da lista suspensa Shelf.
Ventiladores	A aba **Ventiladores** mostra o status do compartimento do ventilador e do próprio ventilador. O status pode ser Ótimo, Falha, Removido ou Desconhecido. Você também pode visualizar esse status selecionando o ícone de ventilador ao lado da lista suspensa Prateleira.
Temperatura	A aba **Temperatura** mostra o status da temperatura dos componentes da prateleira, como sensores, controladores e canisters de fonte de alimentação/ventilador. O status pode ser Ótimo, Temperatura nominal excedida, Temperatura máxima excedida ou Desconhecido. Você também pode visualizar esse status selecionando o ícone de Temperatura, ao lado da lista suspensa Shelf.
Baterias	A aba **Baterias** mostra o status das baterias do controlador. O status pode ser Ideal, Falha, Removido ou Desconhecido. Outras informações incluem a idade da bateria, dias até a substituição, ciclos de aprendizado e semanas entre ciclos de aprendizado. Você também pode visualizar esse status selecionando o ícone de Baterias, ao lado da lista suspensa Shelf.

Aba	Descrição
SFPs	A aba **SFPs** mostra o status dos transceptores Small Form-factor Pluggable (SFP) nos controladores. O status pode ser Ótimo, Falha ou Desconhecido. Selecione **Mostrar mais configurações** para ver o número de peça, o número de série e o fornecedor dos SFPs. Você também pode visualizar esse status selecionando o ícone SFP ao lado da lista suspensa Prateleira.

3. Clique em **Close**.

Atualizar os ciclos de aprendizagem da bateria no SANtricity System Manager

Um ciclo de aprendizagem é um ciclo automático para calibrar o indicador inteligente de bateria. Os ciclos são programados para iniciar automaticamente, no mesmo dia e horário, em intervalos de 8 semanas (por controlador). Se você quiser definir uma programação diferente, 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 a Controller Shelf e, em seguida, selecione **View settings**.
3. Selecione a guia **Baterias**.
4. Selecione **Update battery learn cycles**.

   A caixa de diálogo Update Battery Learn Cycles é aberta.

5. Nas listas suspensas, selecione um novo dia e horário.
6. Clique em **Salvar**.

Gerenciar controladores

Saiba mais sobre os estados do controlador no SANtricity System Manager

Você pode colocar um controlador em três estados diferentes: online, offline e modo de serviço.

Estado online

O estado online é o estado normal de funcionamento do controlador. Significa que o controlador está operando normalmente e está disponível para operações de I/O.

Ao colocar um controlador online, seu status é definido como ótimo.

Estado offline

O estado offline é normalmente usado para preparar um controlador para substituição quando existem dois controladores no array de storage. 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 somente emitindo outro comando explícito ou substituindo o controlador com falha. Você só pode colocar um controlador offline se houver dois controladores no array de storage.

Quando um controlador está no estado offline, as seguintes condições são verdadeiras:

- O controlador não está disponível para I/O.
- Você não pode gerenciar o array de storage 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 o modo de cache de gravação direta.

Modo de serviço

O Service Mode é normalmente usado apenas pelo suporte técnico para mover todos os volumes do array de storage para um controlador, permitindo que o outro controlador seja diagnosticado. Um controlador deve ser colocado manualmente em Service Mode e deve ser colocado manualmente online novamente após a conclusão da operação de serviço.

Quando um controlador está em modo de serviço, as seguintes condições são verdadeiras:

- O controlador não está disponível para I/O.
- O suporte técnico pode acessar o controlador através da porta serial ou da 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 o modo de cache de gravação direta.

Saiba mais sobre a atribuição de endereço IP para controladoras E-Series

Por padrão, os controladores são enviados 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 autoconfiguração sem estado do IPv6.

> O IPv6 está 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 System Manager.

Quando a porta de rede está em estado "link down", ou seja, desconectada de uma LAN, o sistema reporta sua configuração como estática, exibindo um endereço IP de 0.0.0.0 (versões anteriores), ou DHCP habilitado sem endereço IP reportado (versões posteriores). Após a porta de rede estar em estado "link up" (ou seja, conectada a uma LAN), ela tenta obter um endereço IP através de DHCP.

Se o controlador não conseguir obter um endereço DHCP em uma determinada porta de rede, ele retorna para um endereço IP padrão, o que pode levar 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:

- Reserve a porta 2 nos controladores para uso do suporte técnico. Não altere as configurações de rede padrão (DHCP ativado).
- Para configurar endereços IP estáticos para os controladores E4000, E2800 e E5700, use SANtricity System Manager. Para configurar endereços IP estáticos para os controladores E2700 e E5600, use SANtricity Storage Manager. Após a configuração de um endereço IP estático, ele permanece definido durante todos os eventos de queda/retorno de link.
- Para usar o DHCP para atribuir o endereço IP do controlador, conecte o controlador a uma rede que possa processar solicitações DHCP. Use um lease DHCP permanente.

Os endereços padrão não são mantidos em caso de queda de link. Quando uma porta de rede em um controlador está configurada para usar DHCP, o controlador tenta obter um endereço DHCP a cada reconexão de link, incluindo inserções de cabos, reinicializações e ciclos de energia. Sempre que uma tentativa de DHCP falha, o endereço IP estático padrão para essa porta é utilizado.

Configurar a porta de gerenciamento no SANtricity System Manager

O controlador inclui uma porta Ethernet utilizada para gerenciamento do sistema. Se necessário, você pode alterar seus parâmetros de transmissão e endereços IP.

Sobre esta tarefa

Durante este procedimento, você seleciona a porta 1 e, em seguida, determina a velocidade e o método de endereçamento da porta. A porta 1 conecta-se à rede onde o cliente pode acessar o controlador e System Manager.

Não utilize a porta 2 em nenhum dos controladores. A porta 2 é reservada para uso do suporte técnico.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

   O gráfico muda para mostrar os controladores em vez das unidades de disco.

3. Clique no controlador com a porta de gerenciamento que você deseja configurar.

   O menu de contexto do controlador é exibido.

4. Selecione **Configurar portas de gerenciamento**.

   A caixa de diálogo Configure Management Ports é aberta.

5. Certifique-se de que a porta 1 esteja visível e clique em **Next**.
6. Selecione as configurações da porta de configuração e clique em **Next**.

   Detalhes do campo

Campo	Descrição
Velocidade e modo duplex	Mantenha a configuração de negociação automática se desejar que o System Manager determine os parâmetros de transmissão entre o array de storage e a rede; ou, se souber a velocidade e o modo da sua rede, selecione os parâmetros na lista suspensa. Somente as combinações válidas de velocidade e modo duplex aparecem na lista.
Habilitar IPv4 / Habilitar IPv6	Selecione uma ou ambas as opções para ativar o suporte para redes IPv4 e IPv6.

   Se você selecionar **Enable IPv4**, uma caixa de diálogo será aberta para selecionar as configurações de IPv4 após você clicar em **Next**. Se você selecionar **Enable IPv6**, uma caixa de diálogo será aberta para selecionar as configurações de IPv6 após você clicar em **Next**. Se você selecionar ambas as opções, a caixa de diálogo para as configurações de IPv4 será aberta primeiro e, em seguida, após você clicar em **Next**, a caixa de diálogo para as configurações de IPv6 será aberta.

7. Configurar as definições de IPv4 e/ou IPv6, seja automaticamente ou manualmente.

Detalhes do campo

Campo	Descrição
Obter automaticamente a configuração do servidor DHCP	Selecione esta opção para obter a configuração automaticamente.
Especificar manualmente a configuração estática	Selecione esta opção e, em seguida, insira o endereço IP do controlador. (Se desejar, você pode copiar 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 alterar a configuração do endereço IP, perderá o caminho de gerenciamento para o array de storage. Se você usa SANtricity Unified Manager para gerenciar arrays globalmente em sua rede, abra a interface de usuário e acesse o **Manage › Discover**. Se você usa SANtricity Storage Manager, você deve remover o dispositivo da Enterprise Management Window (EMW), adicioná-lo novamente à EMW selecionando o **Edit › Add Storage Array** e, em seguida, inserir o novo endereço IP.

8. Clique em **Concluir**.

Resultados

A configuração da porta de gerenciamento é exibida nas configurações do controlador, guia Portas de Gerenciamento.

Configurar os endereços do servidor NTP no SANtricity System Manager

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

- É necessário instalar e configurar um servidor NTP em 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, também deverá configurar um servidor DNS para resolver o endereço do servidor NTP. Você precisa configurar o servidor DNS apenas nos controladores onde configurou o NTP e forneceu um nome de domínio.

Sobre esta tarefa

O NTP permite que o array de storage sincronize automaticamente os relógios do controlador com um host externo usando Simple Network Time Protocol (SNTP). O controlador consulta periodicamente o servidor NTP e então usa os resultados para atualizar seu relógio interno de hora do dia. Se apenas um controlador tiver

NTP habilitado, o controlador alternativo sincroniza periodicamente seu relógio com o controlador que tem NTP habilitado. Se nenhum dos controladores tiver NTP habilitado, os controladores sincronizam periodicamente seus relógios entre si.

> Não é necessário configurar o NTP em ambos os controladores; no entanto, fazê-lo melhora a capacidade do array de storage de permanecer sincronizado durante falhas de hardware ou de comunicação.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

   O gráfico muda para mostrar os controladores em vez das unidades de disco.
3. Clique no controlador que deseja configurar.

   O menu de contexto do controlador é exibido.
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 servidores NTP a partir do servidor DHCP** — Os endereços de servidores NTP detectados são exibidos.

     > Se o array de storage estiver configurado para usar um endereço NTP estático, nenhum servidor NTP aparece.

   - **Especificar manualmente os endereços do servidor NTP** — Insira o endereço do servidor NTP principal e um endereço de servidor NTP de backup. O servidor de backup é opcional. (Esses campos de endereço aparecem depois que você seleciona o botão de opção.) O endereço do servidor pode ser um nome de domínio totalmente qualificado, endereço IPv4 ou endereço IPv6.
7. **Opcional:** Insira as informações do servidor e 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**.

${post_edited_translations.segment}

O Domain Name System (DNS) é usado para resolver nomes de domínio totalmente qualificados para os controladores e um servidor Network Time Protocol (NTP). As portas de gerenciamento no array de storage podem suportar protocolos IPv4 ou IPv6 simultaneamente.

Antes de começar

- ${post_edited_translations.segment}
- Você conhece o endereço do servidor DNS primário e um servidor DNS de backup opcional. Esses endereços podem ser endereços IPv4 ou endereços IPv6.

Sobre esta tarefa

Este procedimento descreve como especificar um endereço de servidor DNS primário e de backup. O servidor DNS de backup pode ser opcionalmente configurado para usar se um servidor DNS primário falhar.

> Se você já configurou as portas de gerenciamento do array de storage com Dynamic Host Configuration Protocol (DHCP), e você tem um ou mais servidores DNS ou NTP associados à configuração DHCP, então você não precisa configurar manualmente DNS ou NTP. Neste caso, o array de storage já deveria ter obtido os endereços do servidor DNS/NTP automaticamente. No entanto, você ainda deve seguir as instruções abaixo para abrir a caixa de diálogo e certificar-se de que os endereços corretos são detectados.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

   O gráfico muda para mostrar os controladores em vez das unidades de disco.
3. ${post_edited_translations.segment}

   O menu de contexto do controlador é exibido.
4. ${post_edited_translations.segment}

   ${post_edited_translations.segment}
5. Selecione uma das seguintes opções:
   - **Obter automaticamente endereços de servidor DNS do servidor DHCP** — Os endereços de servidor DNS detectados são exibidos.

     > Se o array de storage estiver configurado para usar um endereço DNS estático, nenhum servidor DNS será exibido.

   - **Especifique manualmente os endereços do servidor DNS** — Insira o endereço de um servidor DNS primário e o endereço de um servidor DNS de backup. O servidor de backup é opcional. (Esses campos de endereço aparecem depois que você seleciona o botão de opção.) Esses endereços podem ser endereços IPv4 ou endereços IPv6.
6. Clique em **Salvar**.
7. Repita estas etapas para o outro controlador.

Resultados

A configuração de DNS é exibida nas configurações do controlador, guia **DNS / NTP**.

Visualizar configurações do controlador no SANtricity System Manager

Você pode visualizar informações sobre um controlador, como o status das interfaces do

host, interfaces de disco e portas de gerenciamento.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

   O gráfico muda para mostrar os controladores em vez das unidades de disco.

3. Execute uma das seguintes ações para exibir as configurações do controlador:
   - Clique no controlador para exibir o menu de contexto e, em seguida, selecione **View settings**.
   - 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 Controller Settings é aberta.

4. Selecione as abas para mover entre as configurações da propriedade.

   Algumas abas têm um link para **Mostrar mais configurações** no canto superior direito.

Detalhes do campo

Aba	Descrição
Base	Exibe o status do controlador, o nome do modelo, o número de peça de substituição, a versão atual do firmware e a versão da memória estática não volátil de acesso aleatório (NVSRAM).
Cache	Exibe as configurações de cache do controlador, que incluem o cache de dados, o cache do processador e o dispositivo de backup de cache. O dispositivo de backup de cache é usado para fazer backup dos dados no cache caso você perca energia no controlador. O status pode ser Ideal, Falha, Removido, Desconhecido, Protegido contra gravação ou Incompatível.
Interfaces de host	Exibe 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. A localização da placa de interface do host (HIC) pode ser na placa-mãe ou em um slot (baia). "Placa-mãe" indica que as portas da HIC estão integradas ao controlador. "Slot" indica que as portas estão na HIC opcional.
Interfaces de unidade	Exibe as informações da interface da unidade e o status do link de cada porta. A interface da unidade é a conexão entre o controlador e as unidades, como SAS.
Portas de gerenciamento	Exibe os detalhes da porta de gerenciamento, como o nome do host usado para acessar o controlador e se o login remoto foi habilitado. A porta de gerenciamento conecta o controlador ao cliente de gerenciamento, que é onde um navegador está instalado para acessar System Manager.
DNS / NTP	Mostra o método de endereçamento e os endereços IP do servidor DNS e do servidor NTP, caso esses servidores tenham sido configurados no System Manager. O Sistema de Nomes de Domínio (DNS) é um sistema de nomenclatura para dispositivos conectados à Internet ou a uma rede privada. O servidor DNS mantém um diretório de nomes de domínio e os traduz para endereços de Protocolo de Internet (IP). O Network Time Protocol (NTP) é um protocolo de rede para sincronização de clock entre sistemas de computador em redes de dados.

5. Clique em **Close**.

Configurar o login remoto (SSH) no SANtricity System Manager

Ao habilitar o login remoto, você permite que 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 insiram uma chave SSH e/ou 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 suporte técnico deve usar o recurso Remote Login.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

   O gráfico muda para mostrar os controladores em vez das unidades de disco.

3. Clique no controlador para o qual deseja configurar o login remoto.

   O menu de contexto do controlador é exibido.

4. Selecione **Configurar login remoto (SSH)**. (Para as versões 11.73 e anteriores do SANtricity, este item de menu é **Change remote login**.)

   A caixa de diálogo é aberta para habilitar o login remoto.

5. Selecione a caixa de seleção **Enable remote login**.

   Essa configuração oferece login remoto com três opções para autorização:

   - **Somente senha**. Para esta opção, você concluiu e pode clicar em **Salvar**. Se você tiver um sistema duplex, poderá habilitar o login remoto no segundo controlador seguindo os passos anteriores.
   - **Chave SSH ou senha**. Para esta opção, prossiga para a próxima etapa.
   - **Senha e chave SSH**. Para esta opção, selecione a caixa de seleção **Exigir chave pública e senha autorizadas para login remoto** e prossiga para a próxima etapa.

6. Preencha o campo **Chave pública autorizada**. Este campo contém uma lista de chaves públicas autorizadas, no formato do arquivo **authorized_keys** do OpenSSH.

   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 # e linhas vazias são ignoradas. Para obter mais informações sobre o formato do arquivo, consulte "Configurando chaves autorizadas para OpenSSH".
   - Um arquivo **authorized_keys** deve ser semelhante ao seguinte exemplo:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDJlG20rYTk4ok+xFjkPHYp/R0LfJqEYDLXA5AJ4
9w3DvAWLrUg+1CpNq76WSqmQBmoG9jgbcAB5ABGdswdeMQZHilJcu29iJ3OKKv6SlCulA
j1tHymwtbdhPuipd2wIDAQAB
```

7. Quando terminar, clique em **Save**.
8. Para sistemas duplex, você pode habilitar o login remoto no segundo controlador seguindo os passos acima. Se estiver configurando a opção para senha e chave SSH, certifique-se de selecionar novamente a caixa de seleção **Exigir chave pública autorizada e senha para login remoto**.
9. Após o suporte técnico concluir a resolução de problemas, você pode desativar o login remoto retornando à caixa de diálogo Configurar Login Remoto e desmarcando a caixa de seleção **Ativar login remoto**. Se o login remoto estiver ativado em um segundo controlador, uma caixa de diálogo de confirmação será exibida e permitirá que você desative o login remoto também no segundo controlador.

   Desativar o login remoto encerra quaisquer sessões SSH em andamento e rejeita quaisquer novas solicitações de login.

Coloque um controlador online no SANtricity System Manager

Se um controlador estiver no estado offline ou em modo de serviço, você pode colocá-lo online novamente.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

   O gráfico muda para mostrar os controladores em vez das unidades de disco.

3. Clique em um controlador que esteja no estado offline ou em modo de serviço.

   O menu de contexto do controlador é exibido.

4. Selecione **Place online** e confirme que deseja realizar a operação.

Resultados

A detecção de um caminho preferencial restaurado pelo driver multipath pode levar até 10 minutos.

Quaisquer volumes originalmente pertencentes a este controlador são automaticamente movidos de volta para o controlador à medida que solicitações de E/S são recebidas para cada volume. Em alguns casos, pode ser necessário redistribuir os volumes manualmente com o comando **Redistribuir volumes**.

Coloque um controlador offline no SANtricity System Manager

Se você receber essa instrução, poderá colocar um controlador offline.

Antes de começar

- Seu array de storage deve ter dois controladores. O controlador que você não está colocando offline deve estar online (no estado ideal).

- Certifique-se de que nenhum volume esteja em uso ou que você tenha um driver multipath instalado em todos os hosts que utilizam esses volumes.

Sobre esta tarefa

Não coloque um controlador offline, a menos que seja instruído a fazê-lo pelo Recovery Guru ou suporte técnico.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

   O gráfico muda para mostrar os controladores em vez das unidades de disco.

3. Clique no controlador que você deseja colocar offline.

   O menu de contexto do controlador é exibido.

4. Selecione **Place offline** e confirme que deseja realizar a operação.

Resultados

Pode levar alguns minutos para System Manager atualizar o status do controlador para offline. Não inicie nenhuma outra operação até que o status seja atualizado.

Coloque um controlador em modo de serviço no SANtricity System Manager

Se você receber instruções para isso, pode colocar um controlador em modo de serviço.

Antes de começar

- O array de storage deve ter dois controladores. O controlador que você não estiver colocando em modo de serviço deve estar online (em estado ideal).
- Certifique-se de que nenhum volume esteja em uso ou que você tenha um driver multipath instalado em todos os hosts que utilizam esses volumes.

Colocar um controlador em modo de serviço pode reduzir significativamente o desempenho. Não coloque um controlador em modo de serviço a menos que seja instruído a fazê-lo por suporte técnico.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

   O gráfico muda para mostrar os controladores em vez das unidades de disco.

3. Clique no controlador que você deseja colocar em modo de serviço.

   O menu de contexto do controlador é exibido.

4. Selecione **Colocar em modo de serviço** e confirme que você deseja realizar a operação.

Reinicializar (reiniciar) um controlador no SANtricity System Manager

Alguns problemas exigem uma reinicialização do controlador (reinicializar). Você pode reinicializar o controlador mesmo que não tenha acesso físico a ele.

Antes de começar

- O array de storage deve ter dois controladores. O controlador que você não está reinicializando deve estar online (no estado ideal).
- Certifique-se de que nenhum volume esteja em uso ou que você tenha um driver multipath instalado em todos os hosts que utilizam esses volumes.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

   O gráfico muda para mostrar os controladores em vez das unidades de disco.

3. Clique no controlador que você deseja reinicializar.

   O menu de contexto do controlador é exibido.

4. Selecione **Reset** e confirme que deseja realizar a operação.

Gerenciar portas iSCSI

Configurar as portas iSCSI no SANtricity System Manager

Se o seu controlador incluir uma conexão de host iSCSI, você pode configurar as configurações da porta iSCSI na página Hardware.

Antes de começar

- Seu controlador deve incluir portas iSCSI; caso contrário, as configurações de iSCSI não estarão disponíveis.
- Você deve saber a velocidade da rede (a taxa de transferência de dados entre as portas e o host).

> As configurações e funções do iSCSI só aparecem se o seu array de storage for compatível com iSCSI.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

   O gráfico muda para mostrar os controladores em vez das unidades de disco.

3. Clique no controlador com as portas iSCSI que você deseja configurar.

   O menu de contexto do controlador é exibido.

4. Selecione **Configurar portas iSCSI**.

A opção **Configurar portas iSCSI** só aparece se o System Manager detectar portas iSCSI no controlador.

A caixa de diálogo Configurar portas iSCSI é aberta.

5. Na lista suspensa, selecione a porta que deseja configurar e clique em **Next**.
6. Selecione as configurações da porta de configuração e clique em **Next**.

   Para visualizar todas as configurações de porta, clique no link **Mostrar mais configurações de porta** à direita da caixa de diálogo.

Detalhes do campo

Configuração da porta	Descrição
Velocidade da porta Ethernet configurada (aparece apenas para determinados tipos de placas de interface de host)	Selecione a velocidade que corresponda à capacidade de velocidade do SFP na porta.
Modo Forward Error Correction (FEC) (Aparece apenas para determinados tipos de Host Interface Cards)	Se desejar, selecione um dos modos FEC para a porta do host especificada. O modo Reed Solomon não suporta a velocidade de porta de 25 Gbps.
Habilitar IPv4 / Habilitar IPv6	Selecione uma ou ambas as opções para ativar o suporte para redes IPv4 e IPv6. Se você quiser desativar o acesso à porta, desmarque ambas as caixas de seleção.
Porta de escuta TCP (Disponível ao clicar em **Mostrar mais configurações de porta**.)	Se necessário, insira um novo número de porta. A porta de escuta é o número da porta TCP que o controlador usa para escutar logins iSCSI de iniciadores iSCSI do host. A porta de escuta padrão é 3260. Você deve inserir 3260 ou um valor entre 49152 e 65535.
Tamanho do MTU (Disponível clicando em **Mostrar mais configurações de porta**.)	Se necessário, insira um novo tamanho em bytes para o Maximum Transmission Unit (MTU). O tamanho padrão da Unidade Máxima de Transmissão (MTU) é de 1500 bytes por quadro. Você deve inserir um valor entre 1500 e 9000.
Habilitar respostas ICMP PING	Selecione esta opção para ativar o Internet Control Message Protocol (ICMP). Os sistemas operacionais de computadores em rede usam esse protocolo para enviar mensagens. Essas mensagens ICMP determinam se um host está acessível e quanto tempo leva para enviar e receber pacotes desse host.

Se você selecionou **Habilitar IPv4**, uma caixa de diálogo é aberta para selecionar as configurações de IPv4 após você clicar em **Avançar**. Se você selecionou **Habilitar IPv6**, uma caixa de diálogo é aberta para selecionar as configurações de IPv6 após você clicar em **Avançar**. Se você selecionou ambas as opções, a caixa de diálogo para as configurações de IPv4 é aberta primeiro e, em seguida, após você clicar em **Avançar**, a caixa de diálogo para as configurações de IPv6 é aberta.

7. Configure as definições de 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

Configuração da porta	Descrição
Obter configuração automaticamente	Selecione esta opção para obter a configuração automaticamente.
Especificar manualmente a configuração estática	Selecione esta opção e, em seguida, insira um endereço estático nos campos. (Se desejar, você pode copiar 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 ao clicar em **Mostrar mais configurações**.)	Selecione esta opção para ativar uma VLAN e insira seu 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, pelos mesmos roteadores ou por ambos.
Ative a prioridade Ethernet (Disponível ao clicar em **Mostrar mais configurações**.)	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). Em um ambiente de rede local (LAN) compartilhada, como Ethernet, várias estações podem disputar o acesso à rede. O acesso é feito por ordem de chegada. Duas estações podem tentar acessar a rede ao mesmo tempo, o que faz com que ambas recuem e esperem antes de tentar novamente. Esse processo é minimizado para Ethernet comutado, onde apenas uma estação é conectada a uma porta do switch.

8. Clique em **Concluir**.

Configurar autenticação iSCSI no SANtricity System Manager

Para maior segurança em uma rede iSCSI, você pode configurar autenticação entre controladores (alvos) e hosts (iniciadores).

System Manager usa o método Challenge Handshake Authentication Protocol (CHAP), que valida a identidade dos targets e initiators 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 (iSCSI hosts) antes ou depois de definir o segredo CHAP para os alvos (controladores). Antes de seguir as instruções desta tarefa, você deve aguardar 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 digitá-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).

- **Two-way authentication** — Use esta configuração para permitir que tanto o controlador quanto os hosts iSCSI realizem 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, que os hosts iSCSI autentiquem a identidade do controlador.

> As configurações e funções do iSCSI só são exibidas na página Configurações se o seu array de storage for compatível com iSCSI.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em Configurações iSCSI, clique em **Configurar autenticação**.

   A caixa de diálogo Configurar autenticação é exibida, mostrando o método atualmente configurado. Ela também mostra se algum host possui segredos CHAP configurados.

3. Selecione uma das seguintes opções:
   - **Sem autenticação** — Se você não deseja que o controlador autentique a identidade dos iSCSI hosts, selecione esta opção e clique em **Concluir**. A caixa de diálogo será fechada e você terá concluído a configuração.
   - **One-way autenticação** — 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 Target CHAP.
   - **Two-way authentication** — Para permitir que tanto o controlador quanto os hosts iSCSI realizem autenticação, selecione esta opção e clique em **Avançar** para exibir a caixa de diálogo Configurar CHAP de destino.
4. Para autenticação unidirecional ou bidirecional, insira ou confirme o segredo CHAP do controlador (o alvo). O segredo CHAP deve ter entre 12 e 57 caracteres ASCII imprimíveis.

   > Se o segredo CHAP do controlador já tiver sido configurado anteriormente, os caracteres no campo são mascarados. Se necessário, você pode substituir os caracteres existentes (os novos caracteres não são mascarados).

5. Faça uma das seguintes ações:
   - Se você estiver configurando autenticação *unidirecional*, clique em **Concluir**. A caixa de diálogo será fechada e a configuração estará finalizada.
   - Se você estiver configurando autenticação *bidirecional*, clique em **Avançar** para exibir a caixa de diálogo Configurar CHAP do Iniciador.
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 caracteres ASCII imprimíveis. Se você não quiser configurar autenticação bidirecional para um host específico, deixe o campo Segredo CHAP do Iniciador em branco.

   > Se o segredo CHAP de um host já tiver sido configurado anteriormente, os caracteres no campo são mascarados. Se necessário, você pode substituir os caracteres existentes (os novos caracteres não são mascarados).

7. Clique em **Concluir**.

Resultados

A autenticação ocorre durante a sequência de login iSCSI entre os controladores e os hosts iSCSI, a menos

que você tenha especificado nenhuma autenticação.

Ative as configurações de descoberta iSCSI no SANtricity System Manager

Você pode habilitar configurações relacionadas à descoberta de dispositivos de armazenamento em uma rede iSCSI.

As Configurações de Descoberta de Destino permitem que você registre as informações iSCSI do array de storage usando o protocolo Internet Storage Name Service (iSNS) e também determine se deve permitir sessões de descoberta sem nome.

Antes de começar

Se o servidor iSNS usar um endereço IP estático, esse endereço deverá estar disponível para o registro no iSNS. Tanto IPv4 quanto IPv6 são suportados.

Sobre esta tarefa

Você pode habilitar as seguintes configurações relacionadas à descoberta iSCSI:

- **Habilitar o servidor iSNS para registrar um alvo** — Quando habilitado, o array de storage registra seu Nome Qualificado iSCSI (IQN) e informações de porta no servidor iSNS. Essa configuração permite a descoberta iSNS, para que um iniciador possa recuperar o IQN e as informações de porta do servidor iSNS.
- **Habilitar sessões de descoberta sem nome** — Quando as sessões de descoberta sem nome estão habilitadas, o iniciador (host iSCSI) não precisa fornecer o IQN do alvo (controlador) durante a sequência de login para uma conexão do tipo descoberta. Quando desabilitadas, os hosts precisam fornecer o IQN para estabelecer uma sessão de descoberta com o controlador. No entanto, o IQN do alvo é sempre necessário para uma sessão normal (com suporte a E/S). Desabilitar essa configuração pode impedir que hosts iSCSI não autorizados se conectem ao controlador usando apenas seu endereço IP.

> As configurações e funções do iSCSI só são exibidas na página Configurações se o seu array de storage for compatível com iSCSI.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **configurações iSCSI**, clique em **Exibir/Editar configurações de descoberta de destino**.

   A caixa de diálogo Configurações de Descoberta de Destino é exibida. Abaixo do campo **Ativar servidor iSNS**…, a caixa de diálogo indica se o controlador já está registrado.

3. Para registrar o controlador, selecione **Habilitar servidor iSNS para registrar meu destino** e, em seguida, selecione uma das seguintes:
   - **Obter configuração automaticamente do servidor DHCP** — Selecione esta opção se você quiser configurar o servidor iSNS usando um servidor DHCP (Dynamic Host Configuration Protocol). Esteja ciente de que, se você usar esta opção, todas as portas iSCSI no controlador também devem ser configuradas para usar DHCP. Se necessário, atualize as configurações da porta iSCSI do controlador para habilitar esta opção.

     > Para que o servidor DHCP forneça o endereço do servidor iSNS, você deve configurar o servidor DHCP para usar a Opção 43 — “Vendor Specific Information.” Esta opção precisa conter o endereço IPv4 do servidor iSNS nos bytes de dados 0xa-0xd (10-13).

- **Especificar configuração estática manualmente** — Selecione esta opção se você quiser inserir um endereço IP estático para o servidor iSNS. (Se desejar, 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 TCP de escuta (use o padrão 3205 ou insira um valor entre 49152 e 65535).

4. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - Quando desabilitado, as sessões de descoberta são impedidas, a menos que o iniciador forneça o IQN de destino. Desabilitar sessões de descoberta sem nome fornece segurança adicional.
5. Clique em **Salvar**.

Resultados

Uma barra de progresso aparece enquanto o System Manager tenta registrar o controlador com o servidor iSNS. Este processo pode levar até cinco minutos.

Visualize pacotes de estatísticas iSCSI no SANtricity System Manager

Você pode visualizar dados sobre as conexões iSCSI com seu array de storage.

Sobre esta tarefa

System Manager exibe esses tipos de estatísticas iSCSI. Todas as estatísticas são somente leitura e não podem ser definidas.

> Os tipos de estatísticas exibidos no System Manager são baseados nas estatísticas disponíveis para o seu array de storage.

- **Ethernet MAC estatísticas** — Fornece estatísticas para o controle de acesso à mídia (MAC). 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.
- **Estatísticas Ethernet TCP/IP** — 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, aplicativos em hosts em rede podem criar conexões entre si, pelas quais podem trocar dados em pacotes. O IP é um protocolo orientado a dados que comunica dados através de uma inter-rede comutação de pacotes. As estatísticas IPv4 e as estatísticas IPv6 são exibidas separadamente.
- **Ethernet Kernel statistics** — Fornece estatísticas para os drivers do kernel da plataforma do dispositivo iSCSI. As estatísticas do kernel exibem dados de rede semelhantes aos da opção de estatísticas TCP/IP. No entanto, os dados das estatísticas do kernel são coletados dos drivers do kernel da plataforma, em vez de diretamente do hardware iSCSI.
- **Estatísticas do destino/iniciador local (protocolo)** — Exibe estatísticas do destino iSCSI, que fornece acesso em nível de bloco à sua mídia de armazenamento, e mostra as estatísticas iSCSI do array de storage quando usado como iniciador em operações de espelhamento assíncrono.
- **DCBX Operational States estatísticas** — Exibe os estados operacionais dos vários recursos do Data Center Bridging Exchange (DCBX).
- **LLDP TLV estatísticas** — Exibe as estatísticas do Link Layer Discovery Protocol (LLDP) Type Length Value (TLV).
- **DCBX TLV estatísticas** — Exibe as informações que identificam as portas do host do array de storage em um ambiente de Data Center Bridging (DCB). Essas informações são compartilhadas com os pares da rede para fins de identificação e capacidade.

Você pode visualizar cada uma dessas estatísticas como estatísticas brutas ou como estatísticas de linha de base. Estatísticas brutas são todas as estatísticas que foram coletadas desde que os controladores foram iniciados. Estatísticas de linha de base são estatísticas de ponto no tempo que foram coletadas desde que você definiu o tempo de linha de base.

Passos

1. Selecione menu: guia Suporte [Support Center > Diagnostics].
2. Selecione **Exibir pacotes de estatísticas iSCSI**.
3. Clique em uma aba para visualizar os diferentes conjuntos de estatísticas.
4. Para definir a linha de base, clique em **Set new baseline**.

   A definição da linha de base estabelece um novo ponto de partida para a coleta das estatísticas. A mesma linha de base é usada para todas as estatísticas iSCSI.

Visualizar sessões iSCSI no SANtricity System Manager

Você pode visualizar informações detalhadas sobre as conexões iSCSI com seu array de storage. As sessões iSCSI podem ocorrer com hosts ou arrays de storage remotos em uma relação de espelhamento assíncrono.

Passos

1. Selecione o menu: configurações [Sistema].
2. Selecione **Visualizar/Encerrar sessões iSCSI**.

   Uma lista das sessões iSCSI atuais aparece.

3. **Opcional:** Para ver informações adicionais sobre uma sessão iSCSI específica, selecione uma sessão e clique em **Ver detalhes**.

Detalhes do campo

Item	Descrição
Identificador de sessão (SSID)	Uma sequência 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 de sessão. O iniciador especifica o ISID durante o login.
Grupo de portais alvo	O destino iSCSI.
Tag de grupo de portal de destino (TPGT)	A parte de destino do identificador de sessão. Um identificador numérico de 16 bits para um grupo de portais de destino iSCSI.
Nome do iniciador iSCSI	O nome exclusivo mundial do iniciador.
Rótulo do iniciador iSCSI	O rótulo do usuário definido no System Manager.
Alias do iniciador iSCSI	Um nome que também pode ser associado a um nó iSCSI. O alias permite que uma organização associe uma string amigável ao nome iSCSI. No entanto, o alias não substitui o nome iSCSI. O alias do iniciador iSCSI só pode ser definido no host, não no System Manager
Host	Um servidor que envia entrada e saída para o array de storage.
ID de conexão (CID)	Um nome único para uma conexão dentro da sessão entre o iniciador e o destino. O iniciador gera esse ID e o apresenta ao destino durante solicitações de login. O ID da conexão também é apresentado durante logouts que encerram conexões.
Identificador da porta	A porta do controlador associada à conexão.
Endereço IP do iniciador	O endereço IP do iniciador.
Parâmetros de login negociados	Os parâmetros que são transacionados durante o login da sessão iSCSI.
Método de autenticação	A técnica para autenticar usuários que desejam acessar a rede iSCSI. Os valores válidos são **CHAP** e **None**.
Método de resumo do cabeçalho	A técnica para exibir os possíveis valores de cabeçalho para a sessão iSCSI. HeaderDigest e DataDigest podem ser **None** ou **CRC32C**. O valor padrão para ambos é **None**.

Item	Descrição
Método de resumo de dados	A técnica para exibir os possíveis valores de dados para a sessão iSCSI. HeaderDigest e DataDigest podem ser **None** ou **CRC32C**. O valor padrão para ambos é **None**.
Conexões máximas	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 destino.
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.
R2T inicial	O status inicial de pronto para transferência. O status pode ser **Sim** ou **Não**.
Comprimento máximo de rajada	A carga máxima SCSI em bytes para esta sessão iSCSI. O comprimento máximo do burst pode ser de 512 a 262.144 (256 KB). O valor padrão é **262.144 (256 KB)**.
Primeira duração da rajada	A carga SCSI em bytes para dados não solicitados para esta sessão iSCSI. O comprimento da primeira rajada pode ser de 512 a 131.072 (128 KB). O valor padrão é **65.536 (64 KB)**.
Tempo de espera padrão	O número mínimo de segundos a aguardar antes de tentar estabelecer uma conexão após o término ou a reinicialização de uma conexão. O valor padrão para o tempo de espera pode variar de 0 a 3600. O padrão é **2**.
Tempo padrão de retenção	O número máximo de segundos que a conexão ainda é possível após o término ou a reinicialização da conexão. O tempo padrão de retenção pode ser de 0 a 3600. O valor padrão é **20**.
Máximo de R2T pendente	O número máximo de "prontos para transferência" pendentes para esta sessão iSCSI. O valor máximo de prontos para transferência pendentes pode ser de 1 a 16. O padrão é **1**.
Nível de recuperação de erros	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 recebidos	A quantidade máxima de dados que o iniciador ou o destino podem receber em qualquer unidade de dados de carga (PDU) iSCSI.
Nome do destino	O nome oficial do destino (não o pseudônimo). O nome do destino no 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 **Save**.

   O arquivo está salvo na pasta Downloads do seu navegador com o nome de arquivo `iscsi-session-connections.txt`.

Encerrar sessão iSCSI no SANtricity System Manager

Você pode encerrar uma sessão iSCSI que não seja mais necessária. As sessões iSCSI podem ocorrer com hosts ou arrays de storage remotos em uma relação de espelhamento assíncrono.

Sobre esta tarefa

Você pode querer encerrar uma sessão iSCSI pelos seguintes motivos:

- **Acesso não autorizado** — Se um iniciador iSCSI estiver conectado e não deveria ter acesso, você pode encerrar a sessão iSCSI para forçar o iniciador iSCSI a sair do array de storage. O iniciador iSCSI pode ter se conectado porque o método de autenticação None estava disponível.
- **Tempo de inatividade do sistema** — Se você precisar desligar um array de storage e perceber que os iniciadores iSCSI ainda estão conectados, você pode encerrar as sessões iSCSI para desconectá-los do array de storage.

Passos

1. Selecione o menu: configurações [Sistema].
2. Selecione **Visualizar/Encerrar sessões iSCSI**.

   Uma lista das sessões iSCSI atuais aparece.

3. Selecione a sessão que você deseja encerrar.
4. Clique em **Encerrar sessão** e confirme que deseja realizar a operação.

Configurar iSER sobre portas InfiniBand no SANtricity System Manager

Se o seu controlador incluir uma porta iSER sobre InfiniBand, você pode configurar a conexão de rede com o host.

Antes de começar

- Seu controlador deve incluir uma porta iSER sobre InfiniBand; caso contrário, as configurações de iSER sobre InfiniBand não estarão disponíveis no System Manager.
- Você deve saber o endereço IP da conexão do host.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

O gráfico muda para mostrar os controladores em vez das unidades de disco.

3. Clique no controlador com a porta iSER sobre InfiniBand que você deseja configurar.

   O menu de contexto do controlador é exibido.

4. Selecione **Configurar iSER em InfiniBand ports**.

   A caixa de diálogo Configurar iSER sobre InfiniBand portas 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, reinicie a porta iSER sobre InfiniBand clicando em **Sim**.

Visualize estatísticas de iSER sobre InfiniBand no SANtricity System Manager

Se o controlador do seu array de storage incluir uma porta iSER sobre InfiniBand, você pode visualizar dados sobre as conexões do host.

Sobre esta tarefa

System Manager exibe os seguintes tipos de estatísticas de iSER sobre InfiniBand. Todas as estatísticas são somente leitura e não podem ser definidas.

- **Estatísticas do alvo local (protocolo)** — Fornece estatísticas para o iSER sobre InfiniBand alvo, mostrando o acesso em nível de bloco à sua mídia de armazenamento.
- **iSER sobre estatísticas da interface InfiniBand** — Fornece estatísticas para todas as portas iSER na interface InfiniBand, incluindo estatísticas de desempenho e informações sobre erros de link associadas a cada porta do switch.

Você pode visualizar cada uma dessas estatísticas como estatísticas brutas ou como estatísticas de linha de base. Estatísticas brutas são todas as estatísticas que foram coletadas desde que os controladores foram iniciados. Estatísticas de linha de base são estatísticas de ponto no tempo que foram coletadas desde que você definiu o tempo de linha de base.

Passos

1. Selecione o menu: configurações [Sistema].
2. Selecione **Exibir iSER em InfiniBand Estatísticas**.
3. Clique em uma aba para visualizar os diferentes conjuntos de estatísticas.
4. **Opcional:** Para definir a linha de base, clique em **Definir nova linha de base**.

   A definição da linha de base estabelece um novo ponto de partida para a coleta das estatísticas. A mesma linha de base é usada para todas as estatísticas de iSER sobre InfiniBand.

Gerenciar portas NVMe

Saiba mais sobre NVMe e o software SANtricity

Alguns controladores incluem uma porta para implementar NVMe (Non-Volatile Memory Express) sobre fabrics. NVMe permite comunicação de alto desempenho entre hosts e o array de storage.

O que é NVMe?

NVM significa "Memória Não Volátil" e é memória persistente usada em muitos tipos de dispositivos de storage. *NVMe* (NVM Express) é uma interface ou protocolo padronizado projetado especificamente para comunicação de alto desempenho com múltiplas filas em dispositivos NVM.

O que é NVMe over Fabrics?

NVMe over Fabrics (NVMe-oF) é uma especificação tecnológica que permite que comandos e dados baseados em mensagens NVMe sejam transferidos entre um computador host e um array de storage por meio de uma rede. Um array de storage (chamado de *subsistema*) pode ser acessado por um host usando uma fabric. Os comandos NVMe são habilitados e encapsulados em camadas de abstração de transporte tanto no lado do host quanto no lado do subsistema. Isso estende a interface NVMe de alto desempenho completamente do host ao storage e padroniza e simplifica o conjunto de comandos.

O armazenamento NVMe-oF é apresentado a um host como um dispositivo de storage local. O volume (chamado de *namespace*) pode ser montado em um sistema de arquivos como qualquer outro dispositivo de storage. Você pode usar a API REST, o SMcli ou SANtricity System Manager para provisionar seu armazenamento conforme necessário.

O que é um Nome Qualificado NVMe (NQN)?

O Nome Qualificado NVMe (NQN) é usado para identificar o destino de armazenamento remoto. O nome qualificado NVMe para o array de storage é sempre atribuído pelo subsistema e não pode ser modificado. Existe apenas um Nome Qualificado NVMe para todo o array. O Nome Qualificado NVMe é limitado a 223 caracteres de comprimento. Você pode compará-lo a um Nome Qualificado iSCSI.

O que é um namespace e um ID de namespace?

Um namespace é o equivalente a uma unidade lógica em SCSI, que se relaciona a um volume no array. O ID do namespace (NSID) é equivalente a um número de unidade lógica (LUN) em SCSI. Você cria o NSID no momento da criação do namespace e pode defini-lo para um valor entre 1 e 255.

O que é um controlador NVMe?

Semelhante a um nexo SCSI I_T, que representa o caminho do iniciador do host até o destino do sistema de storage, um controlador NVMe criado durante o processo de conexão do host fornece um caminho de acesso entre um host e os namespaces no array de storage. Um NQN para o host mais um identificador de porta do host identificam 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 define o ID do namespace para o host usando SANtricity System Manager. Em seguida, quando o controlador NVMe é criado, a lista de IDs de namespace acessíveis pelo controlador NVMe é criada e usada para configurar as conexões permitidas.

Configurar NVMe sobre InfiniBand portas no SANtricity System Manager

Se o seu controlador incluir uma conexão NVMe sobre InfiniBand, você pode configurar as configurações da porta NVMe na página Hardware.

Antes de começar

- Seu controlador deve incluir uma porta de host NVMe sobre InfiniBand; caso contrário, as configurações de NVMe sobre InfiniBand não estarão disponíveis no System Manager.
- Você deve saber o endereço IP da conexão do host.

As configurações e funções do NVMe over InfiniBand aparecem somente se o controlador do seu array de storage incluir uma porta NVMe over InfiniBand.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

   O gráfico muda para mostrar os controladores em vez das unidades de disco.

3. Clique no controlador com a porta NVMe over InfiniBand que você deseja configurar.

   O menu de contexto do controlador é exibido.

4. Selecione **Configurar NVMe sobre InfiniBand ports**.

   A caixa de diálogo Configurar NVMe sobre InfiniBand portas é aberta.

5. Selecione a porta HIC que deseja configurar na lista suspensa e, em seguida, insira o endereço IP.

   Se você estiver configurando um array de storage EF600 com um HIC compatível com 200Gb, esta 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 atinja o desempenho máximo. Se você não atribuir um endereço IP à porta virtual, o HIC funcionará com aproximadamente metade de sua velocidade possível.

6. Clique em **Configurar**.
7. Conclua a configuração e, em seguida, reinicie a porta NVMe over InfiniBand clicando em **Sim**.

Configurar as portas NVMe sobre RoCE no SANtricity System Manager

Se o seu controlador incluir uma conexão para NVMe sobre RoCE (RDMA sobre Converged Ethernet), você pode configurar as configurações da porta NVMe na página Hardware.

Antes de começar

- Seu controlador deve incluir uma porta host NVMe over RoCE; caso contrário, as configurações de NVMe over RoCE não estarão disponíveis no System Manager.
- Você deve saber o endereço IP da conexão do host.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

   O gráfico muda para mostrar os controladores em vez das unidades de disco.

3. Clique no controlador com a porta NVMe over RoCE que você deseja configurar.

   O menu de contexto do controlador é exibido.

4. Selecione **Configurar NVMe over RoCE ports**.

A caixa de diálogo Configurar NVMe sobre portas RoCE é aberta.

5. Na lista suspensa, selecione a porta HIC que você deseja configurar.
6. Clique em **Next**.

   Para visualizar todas as configurações de porta, clique no link **Mostrar mais configurações de porta** à direita da caixa de diálogo.

   Detalhes do campo

Configuração da porta	Descrição
Velocidade da porta Ethernet configurada	Selecione a velocidade que corresponda à capacidade de velocidade do SFP na porta.
Habilitar IPv4 / Habilitar IPv6	Selecione uma ou ambas as opções para ativar o suporte para redes IPv4 e IPv6. Se você quiser desativar o acesso à porta, desmarque ambas as caixas de seleção.
Tamanho do MTU (Disponível clicando em **Mostrar mais configurações de porta**.)	Se necessário, insira um novo tamanho em bytes para o Maximum Transmission Unit (MTU). O tamanho padrão da Unidade Máxima de Transmissão (MTU) é de 1500 bytes por quadro. Você deve inserir um valor entre 1500 e 9000.

   Se você selecionou **Habilitar IPv4**, uma caixa de diálogo é aberta para selecionar as configurações de IPv4 após você clicar em **Avançar**. Se você selecionou **Habilitar IPv6**, uma caixa de diálogo é aberta para selecionar as configurações de IPv6 após você clicar em **Avançar**. Se você selecionou ambas as opções, a caixa de diálogo para as configurações de IPv4 é aberta primeiro e, em seguida, após você clicar em **Avançar**, a caixa de diálogo para as configurações de IPv6 é aberta.

7. Configurar as definições de IPv4 e/ou IPv6, seja automaticamente ou manualmente.

Detalhes do campo

Configuração da porta	Descrição
Obter configuração automaticamente	Selecione esta opção para obter a configuração automaticamente.
Especificar manualmente a configuração estática	Selecione esta opção e insira um endereço estático nos campos. (Se desejar, você pode copiar 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 array de storage EF600 com um HIC compatível com 200Gb, esta 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 atinja o desempenho máximo. Se você não atribuir um endereço IP à porta virtual, o HIC funcionará com aproximadamente metade de sua velocidade máxima.

8. Clique em **Concluir**.

Visualize estatísticas NVMe over Fabrics no SANtricity System Manager

Você pode visualizar dados sobre as conexões NVMe over Fabrics com seu array de storage.

Sobre esta tarefa

System Manager exibe esses tipos de estatísticas NVMe over Fabrics. Todas as estatísticas são somente leitura e não podem ser definidas.

- **Estatísticas do subsistema NVMe** — Exibe estatísticas do controlador NVMe e sua fila. O controlador NVMe fornece um caminho de acesso entre um host e os namespaces no array de storage. Você pode revisar as estatísticas do subsistema NVMe para itens como falhas de conexão, reinicializações e desligamentos.
- **Estatísticas da interface RDMA** — Fornece estatísticas para todas as portas NVMe over Fabrics na interface RDMA, incluindo estatísticas de desempenho e informações sobre erros de link associadas a cada porta do switch. Esta guia só aparece quando as portas NVMe over Fabrics estão disponíveis.

Você pode visualizar cada uma dessas estatísticas como estatísticas brutas ou como estatísticas de linha de base. Estatísticas brutas são todas as estatísticas que foram coletadas desde que os controladores foram iniciados. Estatísticas de linha de base são estatísticas de ponto no tempo que foram coletadas desde que você definiu o tempo de linha de base.

Passos

1. Selecione o menu: configurações [Sistema].
2. Selecione **Exibir estatísticas de NVMe over Fabrics**.
3. **Opcional:** Para definir a linha de base, clique em **Definir nova linha de base**.

   A definição da linha de base estabelece um novo ponto de partida para a coleta das estatísticas. A mesma

linha de base é usada para todas as estatísticas NVMe.

Gerenciar unidades

Saiba mais sobre os estados de drive no SANtricity System Manager

SANtricity System Manager reporta vários estados para as unidades.

Estados de acessibilidade

Estado	Definição
Ignorado	${post_edited_translations.segment}
Incompatível	${post_edited_translations.segment} • ${post_edited_translations.segment} • ${post_edited_translations.segment} • ${post_edited_translations.segment}
Removido	A unidade foi removida incorretamente do array de storage.
${post_edited_translations.segment}	${post_edited_translations.segment}
Sem resposta	A unidade não está respondendo a comandos.

Estados de função

Estado	Definição
Atribuído	A unidade é um membro de um pool ou grupo de volume.
Hot spare em uso	A unidade está sendo usada atualmente como substituta de uma unidade que apresentou falha. Hot spares são usadas apenas em grupos de volume, não em pools.
Hot spare em espera	A unidade está pronta para ser usada como substituta de uma unidade que apresentou falha. Hot spares são usadas apenas em grupos de volume, não em pools.
Não atribuído	A unidade não faz parte 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.
Falha iminente	Foi detectado que o disco rígido pode falhar em breve. Os dados no disco rígido ainda estão disponíveis.
Offline	A unidade geralmente não está disponível para armazenamento de dados porque faz parte de um grupo de volume que está sendo exportado ou está passando por uma atualização de firmware.
Ideal	A unidade está funcionando normalmente.

Saiba mais sobre Solid State Disks (SSDs) no SANtricity System Manager

Discos de estado sólido (SSDs) são dispositivos de storage que utilizam memória de estado sólido (flash) para armazenar dados de forma permanente. SSDs emulam discos rígidos convencionais e estão disponíveis com as mesmas interfaces que os discos rígidos utilizam.

Vantagens dos SSDs

As vantagens dos SSDs em relação aos discos rígidos incluem:

- Inicialização mais rápida (sem spin up)
- Latência mais baixa
- Maior número de operações de entrada/saída por segundo (IOPS)
- Maior confiabilidade com menos peças móveis
- Menor consumo de energia
- Menos calor produzido e menos necessidade de refrigeração

Identificando SSDs

Na página de Hardware, você pode localizar os SSDs na visualização da prateleira frontal. Procure por baias de unidade que exibem um ícone de raio, o que indica que um SSD está instalado.

Grupos de volume

Todas as unidades em um grupo de volume devem ser do mesmo tipo de mídia (todas SSDs ou todas hard drives). Grupos de volume não podem conter uma mistura de tipos de mídia ou tipos de interface.

Armazenamento em cache

O armazenamento em cache de gravação do controlador está sempre ativado para SSDs. O armazenamento em cache de gravação melhora o desempenho e prolonga a vida útil do SSD.

Além do cache do controlador, você pode implementar o recurso de cache SSD para melhorar o desempenho geral do sistema. No cache SSD, os dados são copiados dos volumes e armazenados em dois volumes RAID internos (um por controlador).

Filtrar a visualização de unidades no SANtricity System Manager

Se o array de storage incluir unidades com diferentes tipos de atributos físicos e lógicos, a página Hardware fornece campos de filtro que ajudam a limitar a visualização das unidades e localizar unidades específicas.

Sobre esta tarefa

Os filtros de unidade podem limitar a visualização apenas a determinados tipos de unidades físicas (por exemplo, todas as SAS), com determinados atributos de segurança (por exemplo, secure-capable), em determinados locais lógicos (por exemplo, Volume Group 1). Você pode usar esses filtros em conjunto 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 array de storage** 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 e recursos de segurança disponíveis.

   Os tipos de unidade podem incluir:

   - Tipo de mídia de unidade (SSD, HDD)
   - Tipo de interface da unidade
   - Capacidade da unidade (da maior para a menor)
   - Velocidade da unidade (da mais alta para a mais baixa) Os atributos de segurança podem incluir:
   - Compatível com segurança
   - Habilitado para segurança
   - Compatível com DA (Data Assurance)
   - Compatível com FIPS
   - Compatível com FIPS (FIPS 140-2)
   - Compatível com FIPS (FIPS 140-3)

     Se algum desses atributos for igual para todas as unidades, ele não será exibido na lista suspensa. Por exemplo, se o array de storage incluir todas as unidades SSD com interfaces SAS e velocidades de 15000 RPM, mas algumas SSDs tiverem capacidades diferentes, a lista suspensa exibirá apenas as capacidades como opção de filtro.

   Ao selecionar uma opção no campo, as unidades que não correspondem aos seus critérios de filtro ficam acinzentadas na visualização gráfica.

3. Na segunda caixa de filtro, clique na seta suspensa para exibir os locais lógicos disponíveis para as unidades.

> Se precisar limpar os critérios de filtro, selecione **Limpar** no canto direito das caixas de filtro.

Locais lógicos podem incluir:

- Pools
- Grupos de volume
- Hot spare
- Cache SSD
- Não atribuído

  Ao selecionar uma opção no campo, as unidades que não correspondem aos seus critérios de filtro ficam acinzentadas na visualização gráfica.

4. Opcionalmente, você pode selecionar **Ligar luzes de localização** no canto direito dos campos de filtro para ligar as luzes de localização das unidades exibidas.

   Esta ação ajuda você a localizar fisicamente as unidades no array de storage.

Ative a luz localizadora de unidade no SANtricity System Manager

Na página Hardware, você pode ativar a luz indicadora para encontrar a localização física de uma unidade no array de storage.

Sobre esta tarefa

Você pode localizar unidades individuais ou múltiplas exibidas na página de Hardware.

Passos

1. Selecione **Hardware**.
2. Para localizar uma ou mais unidades, faça um dos seguintes:
   - **Unidade única** — Na imagem da prateleira, encontre a unidade que deseja localizar fisicamente no array. (Se a imagem mostrar os controladores, clique na guia **Unidades**.) Clique na unidade para exibir o menu de contexto e selecione **Ligar luz indicadora**.

     A luz indicadora da unidade acende. Quando você localizar fisicamente a unidade, retorne à caixa de diálogo e selecione **Desligar**.

   - **Várias unidades** — Nos campos de filtro, selecione um tipo de unidade física na lista suspensa à esquerda e um tipo de unidade lógica na lista suspensa à direita. O número de unidades que correspondem aos seus critérios é exibido no canto direito dos campos. Em seguida, você pode clicar em **Ligar luzes indicadoras** ou selecionar **Localizar todas as unidades filtradas** no menu de contexto. Quando você localizar fisicamente as unidades, retorne à caixa de diálogo e selecione **Desligar**.

Visualize o status e as configurações da unidade no SANtricity System Manager

Você pode visualizar o status e as configurações das unidades, como o tipo de mídia, o tipo de interface e a capacidade.

Passos

1. Selecione **Hardware**.
2. Se a imagem 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 deseja visualizar o status e as configurações.

   O menu de contexto da unidade é aberto.

4. Selecione **View settings**.

   A caixa de diálogo Drive Settings é aberta.

5. Para ver todas as configurações, clique em **Mostrar mais configurações** no canto superior direito da caixa de diálogo.

Detalhes do campo

Configurações	Descrição
Status	Exibe os status Ideal, Offline, Falha não crítica e Falha. O status Ideal indica a condição de funcionamento desejada.
Modo	Exibe Atribuído, Não atribuído, Hot Spare Standby ou Hot Spare em uso.
Localização	Mostra a prateleira e o número do compartimento onde a unidade está localizada.
Atribuído a/Pode proteger para/Protegendo	Se a unidade estiver atribuída a um pool, grupo de volume 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 estiver atribuída a um hot spare e seu modo for Standby, este campo exibirá "Pode proteger para." Se o hot spare puder proteger um ou mais grupos de volume, os nomes dos grupos de volume aparecerão. Se não puder proteger um grupo de volume, exibirá 0 grupos de volume. Se a unidade estiver atribuída a um hot spare e seu modo for "Em uso", este campo exibirá "Protegendo". O valor é o nome do grupo de volume afetado. Se a unidade não estiver atribuída, este campo não aparece.
Tipo de mídia	Exibe o tipo de mídia de gravação que a unidade utiliza, que pode ser um disco rígido (HDD) ou um disco de estado sólido (SSD).
Percentual de endurance utilizada (exibido apenas se houver unidades SSD presentes)	A quantidade de dados gravados na unidade até o momento, dividida pelo limite teórico total de gravação.
Tipo de interface	Exibe o tipo de interface que a unidade utiliza, como SAS.
Redundância de caminho de disco	Mostra se as conexões entre a unidade e o controlador são redundantes (Yes) ou não (No).
Capacidade (GiB)	Mostra a capacidade utilizável (capacidade total configurada) da unidade.
Velocidade (RPM)	Mostra a velocidade em RPM (não aparece para SSDs).
Taxa de transferência de dados atual	Mostra a taxa de transferência de dados entre a unidade e o array de storage.
Tamanho do setor lógico (bytes)	Mostra o tamanho do setor lógico que a unidade usa.

Configurações	Descrição
Tamanho do setor físico (bytes)	Mostra o tamanho físico do setor que a unidade utiliza. Normalmente, o tamanho físico do setor é de 4096 bytes para discos rígidos.
Versão do firmware da unidade	Mostra o nível de revisão do firmware da unidade.
Identificador mundial	Exibe o identificador hexadecimal exclusivo do disco rígido.
ID do produto	Exibe o identificador do produto, que é atribuído pelo fabricante.
Número de série	Exibe o número de série da unidade.
Fabricante	Mostra o fornecedor da unidade.
Data de fabricação	Mostra a data em que a unidade foi fabricada. Não disponível para unidades NVMe.
Compatível com segurança	Indica se a unidade é secure-capable (Sim) ou não (Não). Unidades secure-capable podem ser unidades Full Disk Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS) (nível 140-2 ou 140-3), que criptografam os dados durante gravações e descriptografam os dados durante leituras. Essas unidades são consideradas secure-*capable* porque podem ser usadas para segurança adicional usando o recurso Drive Security. Se o recurso Drive Security estiver habilitado para grupos de volume e pools usados com essas unidades, as unidades se tornam secure-*enabled*.
Habilitado para segurança	Mostra se a unidade está secure-enabled (Yes) ou não (No). Unidades secure-enabled são usadas com o recurso Drive Security. Quando você habilita o recurso Drive Security e, em seguida, aplica Drive Security a um pool ou grupo de volume em unidades secure-capable, as unidades se tornam secure-enabled. O acesso de leitura/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 foi fisicamente removida do array de storage.
Acessível para leitura/gravação	Mostra se a unidade está acessível para leitura/gravação (Sim) ou não (Não).

Configurações	Descrição
Identificador da chave de segurança da unidade	Exibe a chave de segurança para unidades com segurança habilitada. Drive Security é um recurso do array de storage que fornece uma camada extra de segurança com unidades Full Disk Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS). Quando essas unidades são usadas com o recurso Drive Security, elas exigem uma chave de segurança para acesso aos seus dados. Quando as unidades são fisicamente removidas do array, elas não podem operar até serem instaladas em outro array, momento em que ficarão em estado Security Locked até que a chave de segurança correta seja fornecida.
Compatível com Data Assurance (DA)	Mostra se o recurso Data Assurance (DA) está ativado (Sim) ou não (Não). Data Assurance (DA) é um recurso que verifica e corrige erros que podem ocorrer durante a transferência de dados pelos controladores até as unidades. Data Assurance pode ser ativado no nível do pool ou do grupo de volume, com hosts que utilizam uma interface de I/O compatível com DA, como Fibre Channel.
DULBE capaz	Indica se a opção para Erro de Bloco Lógico Desalocado ou Não Escrito (DULBE) está habilitada (Sim) ou não (Não). DULBE é uma opção em unidades NVMe que permite que o EF300 ou EF600 array de storage suporte volumes com recursos provisionados.

6. Clique em **Close**.

Substituir uma unidade logicamente no SANtricity System Manager

Se uma unidade falhar ou se você quiser substituí-la por qualquer outro motivo, você pode substituir logicamente a unidade com falha por uma unidade não atribuída ou uma hot spare totalmente integrada.

Sobre esta tarefa

Quando você substitui logicamente uma unidade, ela é atribuída e então passa a ser 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 ausentes
- Unidades SSD que o Recovery Guru notificou que estão perto do fim de sua vida útil
- Discos rígidos que o Recovery Guru notificou que apresentam falha iminente
- Unidades atribuídas (disponíveis apenas para unidades em um grupo de volume, não em um pool)

Antes de começar

A unidade de substituição deve ter as seguintes características:

- No estado ideal

- No estado Não Atribuído
- Os mesmos atributos da unidade que está sendo substituída (tipo de mídia, tipo de interface, e assim por diante)
- A mesma capacidade FDE (recomendada, mas não obrigatória)
- A mesma capacidade de DA (recomendada, mas não obrigatória)

Passos

1. Selecione **Hardware**.
2. Se a imagem 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.

   O menu de contexto da unidade é exibido.

4. Clique em **Logically replace**.
5. **Opcional:** Selecione a caixa de seleção **Falhar unidade após a substituição** para que a unidade original falhe após ser substituída.

   Esta caixa de seleção só estará habilitada se a unidade atribuída original não estiver com falha ou ausente.

6. Na tabela **Selecionar uma unidade de substituição**, selecione a unidade de substituição que você deseja usar.

   A tabela lista apenas as unidades compatíveis com a unidade que você está substituindo. Se possível, selecione uma unidade que mantenha a proteção contra perda em prateleira e gaveta.

7. Clique em **Replace**.

   Se a unidade original estiver com falha ou ausente, os dados são reconstruídos na unidade de substituição usando as informações de paridade. Essa reconstrução começa automaticamente. Os indicadores de falha da unidade se apagam e os indicadores 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. Essa operação de cópia começa automaticamente. Após a conclusão da operação de cópia, o sistema move a unidade original para o estado Não Atribuído ou, se a caixa de seleção estiver marcada, para o estado Com Falha.

Reconstruir uma unidade manualmente no SANtricity System Manager

A reconstrução da unidade normalmente começa automaticamente após você substituir uma unidade. Se a reconstrução da unidade não começar automaticamente, você pode iniciá-la manualmente.

Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico ou pelo Recovery Guru.

Passos

1. Selecione **Hardware**.
2. Se a imagem 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 reconstruir manualmente.

   O menu de contexto da unidade é exibido.

4. Selecione **Reconstruct** e confirme que deseja realizar a operação.

Inicializar (formatar) as unidades no SANtricity System Manager

Se você mover unidades atribuídas de um array de storage para outro, você deve inicializar (formatar) as unidades antes que elas possam ser usadas no novo array de storage.

Sobre esta tarefa

A inicialização remove as informações de configuração anteriores de uma unidade e a retorna ao estado Não Atribuído. A unidade fica então disponível para ser adicionada a um novo pool ou grupo de volume no novo array de storage.

Use a operação de inicialização de unidade ao mover uma unidade única. Você não precisa inicializar as unidades se estiver movendo um grupo de volume inteiro de um array de storage para outro.

Possível perda de dados — Ao inicializar uma unidade, todos os dados na unidade serão perdidos. Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

Passos

1. Selecione **Hardware**.
2. Se a imagem 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 inicializar.

   O menu de contexto da unidade é exibido.

4. Selecione **Inicializar** e confirme que deseja realizar a operação.

Falhar manualmente uma unidade no SANtricity System Manager

Se instruído a fazê-lo, você pode falhar manualmente uma unidade.

Sobre esta tarefa

System Manager monitora as unidades no array de storage. Quando detecta que uma unidade está gerando muitos erros, o Recovery Guru notifica você de uma falha iminente da unidade. Se isso acontecer e você tiver uma unidade de substituição disponível, talvez queira forçar a falha da unidade para tomar uma ação preventiva. Se você não tiver uma unidade de substituição disponível, pode esperar que a unidade falhe por conta própria.

Possível perda de acesso aos dados — Esta operação pode resultar em perda de dados ou perda de redundância. Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico ou pelo Recovery Guru.

Passos

1. Selecione **Hardware**.
2. Se a imagem 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 que falhe.

   O menu de contexto da unidade é exibido.

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 que não sejam RAID 0.

   Antes de falhar a unidade, certifique-se de copiar o conteúdo da unidade. Dependendo da sua configuração, você pode perder todos os dados ou a redundância de dados no pool ou grupo de volume associado se não copiar o conteúdo da unidade primeiro.

   A opção de cópia permite uma recuperação de drive mais rápida do que a reconstrução e reduz a possibilidade de falha de volume caso outro drive falhe durante a operação de cópia.

6. Confirme que deseja falhar a unidade.

   Após a falha do drive, aguarde pelo menos 60 segundos antes de removê-lo.

${post_edited_translations.segment}

Você pode usar a opção Apagar para preparar uma unidade não atribuída para remoção do sistema. Esse procedimento remove os dados permanentemente, garantindo que os dados não possam ser lidos novamente.

Antes de começar

A unidade deve estar em estado Unassigned.

Sobre esta tarefa

Use a opção Erase apenas se você quiser remover permanentemente todos os dados em uma unidade. Se a unidade estiver habilitada para segurança, a opção Erase executa um apagamento criptográfico e redefine os atributos de segurança da unidade de volta para compatível com segurança.

O recurso Erase não oferece suporte a alguns modelos de drive mais antigos. Se você tentar apagar um desses modelos mais antigos, uma mensagem de erro será exibida.

Passos

1. Selecione **Hardware**.

2. Se a imagem 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 visualizar todas as unidades não atribuídas na prateleira. Na lista suspensa **Mostrar unidades que são…**, selecione **Não atribuídas**.

   ${post_edited_translations.segment}

4. Para abrir o menu de contexto da unidade, clique em uma unidade que você deseja apagar. (Se você quiser selecionar várias unidades, pode fazer isso na caixa de diálogo Apagar Unidades.)

   Possível perda de dados — A operação de apagar não pode ser desfeita. Certifique-se de selecionar as unidades corretas durante o procedimento.

5. No menu de contexto, selecione **Erase**.

   ${post_edited_translations.segment}

6. Se desejar, selecione unidades adicionais na tabela. Não é possível selecionar *todas* as unidades; certifique-se de que uma unidade permaneça desmarcada.
7. Confirme a operação digitando `erase` e depois clique em **Apagar**.

   Certifique-se de que deseja prosseguir com esta operação. Depois de clicar em Sim na próxima caixa de diálogo, a operação não poderá ser interrompida.

8. Na caixa de diálogo Tempo Estimado de Conclusão, clique em **Yes** para continuar com a operação de apagamento.

Resultados

A operação de apagamento pode levar vários minutos ou várias horas. Você pode visualizar o status em **Home › View Operations in Progress**. Quando a operação de apagamento for concluída, as unidades estarão disponíveis para uso em outro grupo de volume ou pool de discos, ou em outro array de storage.

Depois que você terminar

Se você quiser usar a unidade novamente, primeiro precisa inicializá-la. Para isso, selecione **Inicializar** no menu de contexto da unidade.

Desbloquear ou redefinir unidades NVMe ou FIPS bloqueadas no SANtricity System Manager

Se você inserir uma ou mais unidades NVMe ou FIPS bloqueadas em um array de storage, 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 realizar uma redefinição em cada unidade bloqueada inserindo seu Physical Security ID (PSID) para redefinir seus atributos de segurança e apagar os dados da unidade.

Antes de começar

- Para a opção Desbloquear, certifique-se de que o arquivo da chave de segurança (com uma extensão de `.slk`) esteja disponível no cliente de gerenciamento (o sistema com um navegador usado para acessar System Manager). Você também deve saber a frase secreta associada à chave.
- Para a opção de Reset, você deve encontrar o PSID em cada unidade que deseja resetar. Para localizar o

PSID, remova fisicamente a unidade e localize a sequência do PSID (máximo de 32 caracteres) 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 array de storage. Para situações em que a chave de segurança não está disponível, esta tarefa também descreve como realizar um reset em uma unidade bloqueada.

> Se a unidade foi bloqueada usando um servidor externo de gerenciamento de chaves, selecione **Settings › Sistema › Gerenciamento de chaves de segurança** no System Manager para configurar o gerenciamento de chaves externas e desbloquear a unidade.

Você pode acessar o recurso Desbloqueio na página Hardware ou no menu: configurações [Sistema > Gerenciamento de chaves de segurança]. A tarefa abaixo fornece instruções a partir da página Hardware.

Passos

1. Selecione **Hardware**.
2. Se a imagem 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 você deseja desbloquear ou redefinir.

   O menu de contexto da unidade é aberto.

4. Selecione **Desbloquear** para aplicar o arquivo de chave de segurança ou **Reset** se você não tiver um arquivo de chave de segurança.

   Essas opções só aparecem se você selecionar uma unidade NVMe ou FIPS bloqueada.

   > Durante uma operação de redefinição, todos os dados são apagados. Execute uma redefinição somente se você não tiver uma chave de segurança. Redefinir uma unidade bloqueada remove permanentemente todos os dados da unidade e redefine seus atributos de segurança para "secure-capable", mas não ativado. **Esta operação não é reversível.**

5. Faça uma das seguintes ações:
   a. **Desbloquear**: Na caixa de diálogo **Desbloquear unidade segura**, clique em **Procurar** e selecione o arquivo de chave de segurança correspondente à unidade que deseja desbloquear. Em seguida, digite a senha e clique em **Desbloquear**.
   b. **Redefinir**: Na caixa de diálogo **Redefinir unidade bloqueada**, insira a string PSID no campo e, em seguida, digite `RESET` para confirmar. Clique em **Redefinir**.

      Para uma operação de desbloqueio, basta realizar esta operação uma única vez para desbloquear todas as unidades NVMe ou FIPS. Para uma operação de redefinição, você deve selecionar individualmente cada unidade que deseja redefinir.

Resultados

A unidade agora está disponível para uso em outro grupo de volume ou pool de discos, ou em outro array de storage.

Gerenciar hot spares

Saiba mais sobre hot spare drives no SANtricity System Manager

Hot spares atuam como unidades de espera em grupos de volume RAID 1, RAID 5 ou RAID 6 para SANtricity System Manager.

São unidades totalmente funcionais que não contêm dados. Se uma unidade falhar no grupo de volume, o controlador reconstrói automaticamente os dados da unidade com falha para uma unidade designada como hot spare.

Os hot spares não são dedicados a grupos de volumes específicos. Eles podem ser usados para qualquer unidade com falha no array de storage, desde que o hot spare e a unidade compartilhem estes atributos:

- Capacidade igual (ou maior capacidade para o hot spare)
- Mesmo tipo de mídia (por exemplo, HDD ou SSD)
- Mesmo tipo de interface (por exemplo, SAS)

Como identificar hot spares

Você pode atribuir hot spares através do Assistente de Configuração Inicial ou na página de Hardware. Para determinar se hot spares estão atribuídos, acesse a página de Hardware e procure por baias de unidade exibidas em rosa.

Como funciona a cobertura de hot spare

A cobertura de 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.

> Hot spares não podem ser usados para pools, que possuem um método diferente de proteção de dados. Em vez de reservar uma unidade adicional, os pools reservam capacidade de reserva (chamada de *preservation capacity*) dentro de cada unidade do pool. Se uma unidade falhar em um pool, o controlador reconstrói os dados nessa capacidade de reserva.

- Se uma unidade em um grupo de volume RAID 1, RAID 5 ou RAID 6 falhar, o controlador usa automaticamente os dados de redundância para reconstruir os dados da unidade com falha. O hot spare é automaticamente substituído pela unidade com falha, sem a necessidade de uma troca física.
- Quando você substituir fisicamente a unidade com falha, uma operação de copyback ocorre da unidade hot spare para a unidade substituída. Se você tiver designado a unidade hot spare como membro permanente de um grupo de volume, a operação de copyback não será necessária.
- A disponibilidade da proteção contra perda de bandeja e da proteção contra perda de gaveta para um grupo de volume depende da localização das unidades que compõem o grupo de volume. 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 copyback.
- O volume do array de storage permanece online e acessível enquanto você substitui a unidade com falha, porque a hot spare é automaticamente substituída pela unidade com falha.

Considerações sobre a capacidade da unidade hot spare

Selecione uma unidade com capacidade igual ou superior à capacidade total da unidade que deseja 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 superior à capacidade da maior unidade no array de storage.

> Caso não haja hot spares disponíveis com a mesma capacidade física, uma unidade com capacidade inferior poderá ser usada como hot spare se a "capacidade utilizada" da unidade for igual ou menor que a capacidade da unidade hot spare.

Considerações sobre tipos de mídia e interface

A unidade usada como hot spare deve ter o mesmo tipo de mídia e interface que as unidades que ela protegerá. Por exemplo, um HDD não pode servir como hot spare para SSDs.

Considerações sobre unidades com recursos de segurança

Uma unidade com capacidade de segurança, como FDE ou FIPS, pode servir como hot spare para unidades com ou sem recursos de segurança. No entanto, uma unidade que não tem capacidade de segurança não pode servir como hot spare para unidades com recursos de segurança.

Ao selecionar uma unidade com segurança habilitada para ser usada como hot spare, System Manager solicita que você execute uma Secure Erase antes de prosseguir. A Secure Erase redefine os atributos de segurança da unidade para secure-capable, mas não secure-enabled.

> Ao ativar o recurso de Drive Security e, em seguida, criar um pool ou grupo de volume a partir de unidades com capacidade de segurança, as unidades tornam-se *secure-enabled*. O acesso de leitura e gravação fica 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 foi fisicamente removida do array de storage.

Número recomendado de hot spare

Se você utilizou o assistente de Configuração Inicial para criar automaticamente hot spares, System Manager cria uma hot spare para cada 30 unidades de um determinado tipo de mídia e interface. Caso contrário, você pode criar manualmente hot spares entre os grupos de volume no array de storage.

Atribuir hot spares no SANtricity System Manager

Você pode designar um hot spare como unidade de espera para proteção adicional de dados 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

- É necessário criar grupos de volume RAID 1, RAID 5 ou RAID 6. (Hot spares não podem ser usados para pools. Em vez disso, um pool utiliza a capacidade reserva dentro de cada unidade para sua proteção de dados.)
- Um disco rígido que atenda aos seguintes critérios deve estar disponível:
  - Não atribuído, com status Ótimo.

- Mesmo tipo de mídia que as unidades no grupo de volume (por exemplo, SSDs).
- Mesmo tipo de interface que as unidades no grupo de volume (por exemplo, SAS).
- Capacidade igual ou superior à capacidade utilizada das unidades no grupo de volume.

Sobre esta tarefa

Esta tarefa descreve como atribuir manualmente um hot spare na página de Hardware. A cobertura recomendada é de dois hot spares por conjunto de unidades.

> Hot spares também podem ser atribuídos a partir do assistente de configuração inicial. Você pode determinar se hot spares já estão atribuídos procurando por baias de unidade mostradas em rosa na página de Hardware.

Passos

1. Selecione **Hardware**.
2. Se a imagem 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 com a segurança ativada, a caixa de diálogo Secure Erase Drive? será exibida. Para usar uma unidade com segurança ativada como hot spare, você deve primeiro executar uma operação de Secure Erase para remover todos os seus dados e redefinir seus atributos de segurança.

   > **Possível perda de dados** — Certifique-se de ter selecionado a unidade correta. Após concluir a operação de Secure Erase, você não poderá recuperar nenhum dos dados.

   Se a unidade **não** estiver com o recurso de segurança ativado, a caixa de diálogo Confirm Assign Hot Spare Drive será exibida.

5. Analise o texto na caixa de diálogo e, em seguida, confirme a operação.

   A unidade é exibida em rosa na página de Hardware, o que indica que agora ela é uma hot spare.

Resultados

Se uma unidade dentro de um grupo de volume RAID 1, RAID 5 ou RAID 6 falhar, o controlador usa automaticamente os dados de redundância para reconstruir os dados da unidade com falha para a hot spare.

Desatribuir hot spares no SANtricity System Manager

Você pode alterar uma hot spare de volta para uma unidade não atribuída.

Antes de começar

O hot spare deve estar no estado Ótimo, em modo de espera.

Sobre esta tarefa

Não é possível remover a atribuição de um hot spare que esteja substituindo uma unidade com falha. Se o hot

spare não estiver em status Ótimo, siga os procedimentos do Recovery Guru para corrigir quaisquer problemas antes de tentar remover a atribuição da unidade.

Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar os controladores, clique na guia **Drives**.

   O gráfico muda para mostrar as unidades em vez dos controladores.

3. Selecione a hot spare drive (exibida em rosa) que você deseja desatribuir.

   Se houver linhas diagonais atravessando o compartimento rosa da unidade, 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 volumes afetados pela remoção deste hot spare e se outros hot spares os estão protegendo.

5. Confirme a operação de desatribuição.

Resultados

A unidade é retornada para Não Atribuído (mostrada em cinza).

Perguntas frequentes sobre compartimentos de armazenamento para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

O que é proteção contra perdas em prateleiras e proteção contra perdas em gavetas?

A proteção contra perda de compartimento e a proteção contra perda de gaveta são atributos de pools e grupos de volume que permitem manter o acesso aos dados em caso de falha de um único compartimento ou gaveta.

Proteção contra perda de compartimento

Um shelf é o gabinete que contém as unidades ou as unidades e o controlador. A proteção contra perda de shelf garante acessibilidade aos dados nos volumes de um pool ou grupo de volume caso ocorra uma perda total de comunicação com um shelf de unidades. Um exemplo de perda total de comunicação pode ser a perda de energia do shelf de unidades ou a falha de ambos os módulos de E/S (IOMs).

> A proteção contra perda de compartimento não é garantida se uma unidade já tiver falhado no pool ou grupo de volume. Nessa situação, a perda de acesso a um compartimento de unidades e, consequentemente, a outra unidade no pool ou grupo de volume causa perda de dados.

Os critérios para proteção contra perdas no compartimento de expansão dependem do método de proteção, conforme descrito na tabela a seguir:

Nível	Critérios para proteção contra perda de compartimento	Número mínimo de compartimentos necessários
Pool	O pool deve incluir unidades de pelo menos cinco compartimentos e deve haver um número igual de unidades em cada compartimento. A proteção contra perda de compartimento não se aplica a compartimentos de alta capacidade; se o seu sistema contiver compartimentos de alta capacidade, consulte Proteção contra Perda de Gaveta.	5
RAID 6	O grupo de volume contém no máximo duas unidades em um único compartimento.	3
RAID 3 ou RAID 5	Cada unidade do grupo de volume está localizada em um compartimento separado.	3
RAID 1	Cada disco rígido em um par RAID 1 deve estar localizado em um compartimento separado.	2
RAID 0	Não é possível obter proteção contra perda de compartimento.	Não aplicável

Proteção contra perda de gaveta

Uma gaveta é um dos compartimentos de uma prateleira que você puxa para acessar as unidades. Somente as prateleiras de alta capacidade possuem gavetas. A proteção contra perda de gaveta garante acessibilidade aos dados nos volumes em um pool ou grupo de volume caso ocorra uma perda total de comunicação com uma única gaveta. Um exemplo de perda total de comunicação pode ser a falta de energia na gaveta ou a 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. Nessa situação, a perda de acesso a uma gaveta (e consequentemente a outra unidade no pool ou grupo de volume) causa perda de dados.

Os critérios para proteção contra perda de gavetas dependem do método de proteção, conforme descrito na tabela a seguir:

Nível	Critérios para proteção contra perda de gaveta	Número mínimo de gavetas necessárias
Pool	Os candidatos ao pool devem incluir unidades de todas as gavetas, e deve haver um número igual de unidades em cada gaveta. O pool deve incluir unidades de pelo menos cinco gavetas e deve haver um número igual de unidades em cada gaveta. Uma prateleira de 60 discos rígidos pode atingir a Proteção contra Perda de Gavetas quando o pool contém 15, 20, 25, 30, 35, 40, 45, 50, 55 ou 60 discos rígidos. Incrementos em múltiplos de 5 podem ser adicionados ao pool após a criação inicial.	5
RAID 6	O grupo de volume contém no máximo 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 espelhado deve estar localizada em uma gaveta separada.	2
RAID 0	Não é possível alcançar a 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 medidor inteligente de bateria.

Um ciclo de aprendizagem consiste nestas fases:

- Descarga controlada da bateria
- Período de repouso
- Cobrar

As baterias são descarregadas até um limite predeterminado. Durante essa fase, o indicador de nível da bateria é calibrado.

Um ciclo de aprendizagem requer estes parâmetros:

- Baterias totalmente carregadas
- Sem baterias superaquecidas

Os ciclos de aprendizagem para sistemas de controladores duplex ocorrem simultaneamente. Para controladores com backup de energia proveniente 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, no mesmo horário e no mesmo dia da semana. O intervalo entre os ciclos é descrito em semanas.

Um ciclo de learn pode levar várias horas para ser concluído.

Perguntas frequentes sobre o controlador de storage para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

O que é auto-negociação?

A autonegociação 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 geralmente é a configuração preferida para configurar portas de gerenciamento; no entanto, se a negociação falhar, configurações incompatíveis de interface de rede podem afetar seriamente o desempenho da rede. Nos casos em que essa condição for 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.

Caso a autonegociação falhe, o controlador tenta estabelecer uma conexão em 10BASE-T, half-duplex, que é o menor denominador comum.

O que é a autoconfiguração de endereço IPv6 sem estado?

Com a autoconfiguração sem estado, os hosts não obtêm endereços e outras informações de configuração de um servidor.

A autoconfiguração sem estado no IPv6 oferece endereços locais de enlace, multicast e o protocolo Neighbor Discovery (ND). O IPv6 pode gerar o interface ID de um endereço a partir do endereço da camada de enlace de dados subjacente.

A autoconfiguração sem estado e a autoconfiguração com estado complementam-se. Por exemplo, o host pode usar a autoconfiguração sem estado para configurar seus próprios endereços, mas usar a autoconfiguração com estado para obter outras informações. A autoconfiguração com estado permite que hosts obtenham endereços e outras informações de configuração de um servidor. Internet Protocol version 6 (IPv6) também define um método pelo qual todos os endereços IP em uma rede podem ser renumerados de uma só vez. O IPv6 define um método para que dispositivos na rede configurem seu endereço IP e outros parâmetros sem a necessidade de um servidor.

Os dispositivos executam estas etapas ao usar a autoconfiguração sem estado:

1. **Gerar um endereço local de link** — O dispositivo gera um endereço local de link, que possui 10 bits, seguidos por 54 zeros e, em seguida, o ID da interface de 64 bits.
2. **Teste a unicidade de um endereço local de link** — O nó testa para garantir que o endereço local de link que ele gera não esteja em uso na rede local. O nó envia uma mensagem de solicitação de vizinho usando o protocolo ND. Em resposta, a rede local aguarda uma mensagem de anúncio de vizinho, que indica que outro dispositivo já está usando o endereço local de link. Se for o caso, um novo endereço local de link deve ser gerado ou a autoconfiguração falha, e outro método deve ser usado.
3. **Atribuir um endereço link-local** — Se o dispositivo passar no teste de unicidade, o dispositivo atribui o endereço link-local à sua interface IP. O endereço link-local pode ser usado para comunicação na rede local, mas não pela Internet.
4. **Contatar o roteador** — O nó tenta contatar um roteador local para obter mais informações sobre como continuar a configuração. Esse contato é realizado escutando mensagens de anúncio de roteador enviadas periodicamente pelos roteadores ou enviando uma mensagem de solicitação de roteador específica para pedir informações a um roteador sobre o que fazer em seguida.
5. **Fornecer instruções ao nó** — O roteador fornece instruções ao nó sobre como proceder com a autoconfiguração. Alternativamente, o roteador informa ao host como determinar o endereço global da Internet.
6. **Configurar o endereço global** — O host se configura com seu endereço de Internet globalmente único. Esse endereço geralmente é formado a partir de um prefixo de rede fornecido ao host pelo roteador.

Qual devo escolher — DHCP ou configuração manual?

O método padrão para configuração de rede é o Protocolo de Configuração Dinâmica de Hosts (DHCP). Use sempre esta opção, a menos que sua rede não possua um servidor DHCP.

O que é um servidor DHCP?

O Protocolo de Configuração Dinâmica de Hosts (DHCP) é um protocolo que automatiza a tarefa de atribuir um endereço IP.

Cada dispositivo conectado a uma rede TCP/IP deve receber um endereço IP exclusivo. Esses dispositivos incluem os controladores em seu array de storage.

Sem DHCP, um administrador de rede insere esses endereços IP manualmente. Com DHCP, quando um cliente precisa iniciar operações TCP/IP, o cliente envia uma solicitação de informações de endereço por meio de broadcast. O servidor DHCP recebe a solicitação, atribui um novo endereço por um período específico chamado de período de concessão, e envia o endereço para o cliente. Com DHCP, um dispositivo pode ter um endereço IP diferente cada vez que se conecta à rede. Em alguns sistemas, o endereço IP do dispositivo pode mudar mesmo enquanto o dispositivo ainda está conectado.

Como configuro meu servidor DHCP?

Você deve configurar um servidor Dynamic Host Configuration Protocol (DHCP) para usar endereços IP (Internet Protocol) estáticos para os controladores em seu array de storage.

Os endereços IP atribuídos pelo seu servidor DHCP geralmente são dinâmicos e podem mudar porque possuem um período de concessão que expira. Alguns dispositivos, por exemplo, servidores e roteadores, precisam usar endereços estáticos. Os controladores do seu array de storage também precisam de endereços IP estáticos.

Para obter informações sobre como atribuir endereços estáticos, consulte a documentação do seu servidor DHCP.

Por que preciso alterar a configuração de rede do controlador?

Você deve configurar a configuração de rede de cada controlador—seu endereço IP, máscara de sub-rede e gateway—ao usar gerenciamento fora da banda.

Você pode configurar a rede usando um servidor Dynamic Host Configuration Protocol (DHCP). Se você não estiver usando um servidor DHCP, deverá inserir a configuração de rede manualmente.

Onde posso obter a configuração de rede?

Você pode obter o endereço IP (Protocolo de Internet), a máscara de sub-rede (subnet mask) e as informações do gateway com o administrador de rede.

Você precisa dessas informações ao configurar as portas nos controladores.

O que são respostas ICMP PING?

O Protocolo de Mensagens de Controle da Internet (ICMP) é um dos protocolos do conjunto TCP/IP.

As `ICMP echo request` e as (`ICMP echo reply` mensagens são comumente conhecidas como `ping` mensagens. `Ping` é uma ferramenta de solução de problemas usada por administradores de sistemas para testar manualmente a conectividade entre dispositivos de rede, bem como para testar atraso de rede e perda de pacotes. O comando `ping` envia um `ICMP echo request` para um dispositivo na rede, e o dispositivo responde imediatamente com um (`ICMP echo reply`. Às vezes, a política de segurança de rede de uma empresa exige que `ping` (`ICMP echo reply` seja desativado em todos os dispositivos para dificultar sua descoberta por pessoas não autorizadas.

Quando devo atualizar a configuração da porta?

Atualize o servidor DHCP sempre que o servidor for modificado ou atualizado, e as informações de DHCP relevantes para o array de storage atual e para o array de storage que você deseja usar forem alteradas.

Especificamente, atualize a configuração da porta ou o servidor iSNS a partir do servidor DHCP quando souber que o servidor DHCP atribuirá endereços diferentes.

Atualizar a configuração de uma porta é destrutivo para todas as conexões iSCSI nessa porta.

O que devo fazer depois de configurar as portas de gerenciamento?

Se você alterou o endereço IP do array de storage, talvez queira atualizar a visualização global do array no SANtricity Unified Manager.

Para atualizar a visualização da matriz global no Unified Manager, abra a interface e acesse **Gerenciar › Descobrir**.

Se você ainda estiver usando o SANtricity Storage Manager, acesse a Enterprise Management Window (EMW), onde deverá remover e adicionar novamente o novo endereço IP.

Por que o sistema de storage está em modo não ideal?

Um sistema de storage em modo não ideal ocorre devido a um estado de Configuração de Sistema Inválida. Apesar desse estado, o acesso normal de E/S aos volumes existentes é totalmente suportado; no entanto, SANtricity System Manager proibirá algumas operações.

Um sistema de storage pode entrar em estado de Configuração de Sistema Inválida por um destes motivos:

- O controlador está fora de conformidade, possivelmente porque possui um código de identificação de submodelo (SMID) incorreto ou excedeu o limite de recursos premium.
- Está em andamento uma operação de serviço interna, como um download de firmware da unidade.
- O controlador excedeu o limite de erro de paridade e entrou em modo de bloqueio.
- Ocorreu uma condição geral de lockdown.

Perguntas frequentes sobre o protocolo iSCSI para o SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

O que acontece quando uso um servidor iSNS para registro?

Quando as informações do Internet Storage Name Service (iSNS) são utilizadas, os hosts (iniciadores) podem ser configurados para consultar o servidor iSNS para recuperar informações do alvo (controladores).

Este registro fornece ao servidor iSNS o Nome Qualificado iSCSI (IQN) e as informações de porta do controlador, permitindo consultas entre os iniciadores (iSCSI hosts) e os alvos (controladores).

Quais métodos de registro são suportados automaticamente para iSCSI?

A implementação do iSCSI suporta o método de descoberta Internet Storage Name Service (iSNS) ou o uso do comando Send Targets.

O método iSNS permite a descoberta iSNS entre os iniciadores (iSCSI hosts) e os alvos (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 iSNS, o host iSCSI pode enviar o comando Send Targets durante uma sessão de descoberta iSCSI. Em resposta, o controlador retorna as informações da porta (por exemplo, o Target IQN, endereço IP da porta, porta de escuta e Target Port Group). Esse método de descoberta não é necessário se você usar iSNS, pois o iniciador do host pode recuperar os IPs de destino do servidor iSNS.

Como interpreto as estatísticas de iSER sobre InfiniBand?

A caixa de diálogo Exibir estatísticas de iSER sobre InfiniBand exibe estatísticas do alvo local (protocolo) e estatísticas da interface iSER sobre InfiniBand (IB). Todas as estatísticas são somente leitura e não podem ser definidas.

- **Estatísticas do alvo local (protocolo)** — Fornece estatísticas para o iSER sobre InfiniBand alvo, mostrando o acesso em nível de bloco à sua mídia de armazenamento.
- **iSER over InfiniBand Interface estatísticas** — Fornece estatísticas para todas as portas iSER over InfiniBand na interface InfiniBand, incluindo estatísticas de desempenho e informações sobre erros de link associadas a cada porta do switch.

Você pode visualizar cada uma dessas estatísticas como estatísticas brutas ou como estatísticas de linha de base. Estatísticas brutas são todas as estatísticas que foram coletadas desde que os controladores foram iniciados. Estatísticas de linha de base são estatísticas de ponto no tempo que foram coletadas desde que você definiu o tempo de linha de base.

O que mais preciso fazer para configurar ou diagnosticar iSER sobre InfiniBand?

A tabela a seguir lista as funções do SANtricity System Manager que você pode usar para configurar e gerenciar iSER sobre sessões InfiniBand.

> As configurações iSER over InfiniBand estão disponíveis somente se o controlador do seu array de storage incluir uma porta de gerenciamento de host iSER over InfiniBand.

Ação	Localização
Configurar iSER em portas InfiniBand	1. Selecione **Hardware**. 2. Selecione a guia **Controladores e Componentes**. 3. Selecione um controlador. 4. Selecione **Configurar iSER em InfiniBand ports**. ou 1. Selecione o menu: configurações [Sistema]. 2. Desça até **iSER sobre configurações do InfiniBand**, e então selecione **Configurar iSER sobre portas do InfiniBand**.
Veja estatísticas de iSER sobre InfiniBand	1. Selecione o menu: configurações [Sistema]. 2. Desça até **iSER over InfiniBand configurações** e, em seguida, selecione **Exibir iSER over InfiniBand estatísticas**.

O que mais preciso fazer para configurar ou diagnosticar iSCSI?

As sessões iSCSI podem ocorrer com hosts ou arrays de storage remotos em uma relação de espelhamento assíncrono. As tabelas a seguir listam as funções do SANtricity System Manager que você pode usar para configurar e gerenciar essas sessões iSCSI.

> As configurações de iSCSI só estão disponíveis se o seu array de storage for compatível com iSCSI.

Configurar iSCSI

Ação	Localização
Gerenciar configurações iSCSI	1. Selecione o menu: configurações [Sistema]. 2. Deslize a tela para baixo até **iSCSI settings** para visualizar todas as funções de gerenciamento.
Configurar portas iSCSI	1. Selecione **Hardware**. 2. Selecione a guia **Controladores e Componentes**. 3. Selecione um controlador. 4. Selecione **Configurar portas iSCSI**.

Ação	Localização
Definir o segredo CHAP do host	1. Selecione o menu: configurações [Sistema]. 2. Role para baixo até **iSCSI settings** e, em seguida, selecione **Configurar autenticação**. ou 1. Selecione o menu: storage [Hosts]. 2. Selecione um membro host. 3. Clique no menu: Exibir/Editar configurações [Host Ports] tab.

Diagnosticar iSCSI

Ação	Localização
Visualizar ou encerrar sessões iSCSI	1. Selecione o menu: configurações [Sistema]. 2. Role para baixo até **configurações iSCSI** e, em seguida, selecione **Exibir/Encerrar sessões iSCSI**. ou 1. Selecione menu: guia Suporte [Support Center > Diagnostics]. 2. Selecione **Visualizar/Encerrar sessões iSCSI**.
Visualizar estatísticas iSCSI	1. Selecione o menu: configurações [Sistema]. 2. Role para baixo até **configurações iSCSI** e, em seguida, selecione **Exibir pacotes de estatísticas iSCSI**. ou 1. Selecione menu: guia Suporte [Support Center > Diagnostics]. 2. Selecione **Exibir pacotes de estatísticas iSCSI**.

Perguntas frequentes do protocolo NVMe para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

Como interpreto estatísticas NVMe over Fabrics?

A caixa de diálogo Exibir estatísticas do NVMe sobre Fabrics exibe estatísticas para o subsistema NVMe e a interface RDMA. Todas as estatísticas são somente leitura e não podem ser definidas.

- **Estatísticas do subsistema NVMe** — Exibe estatísticas do controlador NVMe e sua fila. O controlador NVMe fornece um caminho de acesso entre um host e os namespaces no array de storage. Você pode revisar as estatísticas do subsistema NVMe para itens como falhas de conexão, reinicializações e desligamentos. Para obter mais informações sobre essas estatísticas, clique em **Exibir legenda para cabeçalhos da tabela**.
- **Estatísticas da interface RDMA** — Fornece estatísticas para todas as portas NVMe over Fabrics na interface RDMA, incluindo estatísticas de desempenho e informações sobre erros de link associados a cada porta do switch. Esta guia só aparece quando as portas NVMe over Fabrics estão disponíveis. Para mais informações sobre as estatísticas, clique em **Exibir legenda para cabeçalhos da tabela**.

Você pode visualizar cada uma dessas estatísticas como estatísticas brutas ou como estatísticas de linha de base. Estatísticas brutas são todas as estatísticas que foram coletadas desde que os controladores foram iniciados. Estatísticas de linha de base são estatísticas de ponto no tempo que foram coletadas desde que você definiu o tempo de linha de base.

O que mais preciso fazer para configurar ou diagnosticar NVMe over InfiniBand?

A tabela a seguir lista as funções do SANtricity System Manager que você pode usar para configurar e gerenciar sessões NVMe sobre InfiniBand.

> As configurações de NVMe over InfiniBand estão disponíveis somente se o controlador do seu array de storage incluir uma porta NVMe over InfiniBand.

Ação	Localização
Configurar NVMe em portas InfiniBand	1. Selecione **Hardware**. 2. Selecione a guia **Controladores e Componentes**. 3. Selecione um controlador. 4. Selecione **Configurar NVMe sobre InfiniBand ports**. ou 1. Selecione o menu: configurações [Sistema]. 2. Desça até **NVMe sobre InfiniBand configurações** e, em seguida, selecione **Configurar NVMe sobre InfiniBand portas**.
Visualizar estatísticas de NVMe over InfiniBand	1. Selecione o menu: configurações [Sistema]. 2. Desça até **NVMe over InfiniBand configurações** e, em seguida, selecione **Exibir estatísticas NVMe over Fabrics**.

O que mais preciso fazer para configurar ou diagnosticar NVMe over RoCE?

Você pode configurar e gerenciar NVMe over RoCE nas páginas Hardware e Configurações.

> As configurações de NVMe sobre RoCE estão disponíveis somente se o controlador do seu array de storage incluir uma porta NVMe sobre RoCE.

Ação	Localização
Configurar NVMe sobre portas RoCE	1. Selecione **Hardware**. 2. Selecione a guia **Controladores e Componentes**. 3. Selecione um controlador. 4. Selecione **Configurar NVMe over RoCE ports**. ou 1. Selecione o menu: configurações [Sistema]. 2. Desça até **Configurações de NVMe sobre RoCE** e selecione **Configurar portas NVMe sobre RoCE**.
Veja estatísticas NVMe over Fabrics	1. Selecione o menu: configurações [Sistema]. 2. Desça até **Configurações de NVMe sobre RoCE** e, em seguida, selecione **Exibir estatísticas de NVMe sobre Fabrics**.

Por que existem dois endereços IP para uma porta física?

O array de storage EF600 pode incluir dois HICs — um externo e um interno.

Nessa configuração, o HIC externo está conectado a um HIC interno auxiliar. Cada porta física que você pode acessar a partir do HIC externo tem uma porta virtual associada do HIC interno.

Para atingir o desempenho máximo de 200Gb, você deve atribuir um endereço IP exclusivo tanto para as portas físicas quanto para as virtuais, para que o host possa estabelecer conexões com cada uma delas. Se você não atribuir um endereço IP à porta virtual, o HIC funcionará com aproximadamente metade de sua velocidade máxima.

Por que existem dois conjuntos de parâmetros para uma porta física?

O array de storage EF600 pode incluir dois HICs — um externo e um interno.

Nessa configuração, o HIC externo está conectado a um HIC interno auxiliar. Cada porta física que você pode acessar a partir do HIC externo tem uma porta virtual associada do HIC interno.

Para atingir o desempenho máximo de 200Gb, você deve atribuir parâmetros tanto para as portas físicas quanto para as virtuais, para que o host possa estabelecer conexões com cada uma delas. Se você não atribuir parâmetros à porta virtual, o HIC funcionará com aproximadamente metade de sua velocidade máxima.

Perguntas frequentes sobre storage drives para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

O que é um hot spare?

Hot spares atuam como unidades de espera em grupos de volume RAID 1, RAID 5 ou RAID 6. São unidades totalmente funcionais que não contêm dados. Se uma unidade falhar no grupo de volume, o controlador

reconstrói automaticamente os dados da unidade com falha para um hot spare.

Se uma unidade falhar no array de storage, a hot spare é automaticamente substituída pela unidade com falha, sem a necessidade de troca física. Se a hot spare estiver disponível quando uma unidade falhar, o controlador usa os dados de redundância para reconstruir os dados da unidade com falha na hot spare.

Um hot spare não é dedicado a um grupo de volume específico. Em vez disso, você pode usar um hot spare para qualquer unidade com falha no array de storage com a mesma capacidade ou capacidade menor. Um 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 utilizam a capacidade de preservação dentro de cada unidade que compõe o pool.

O que é capacidade de preservação?

A capacidade de preservação é a quantidade de capacidade (número de drives) reservada em um pool para suportar possíveis falhas de drives.

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 utilizam capacidade de preservação durante a reconstrução, enquanto os grupos de volumes utilizam hot spare para a mesma finalidade. O método de capacidade de preservação representa uma melhoria em relação ao hot spare, pois permite que a reconstrução ocorra mais rapidamente. A capacidade de preservação é distribuída por várias unidades no pool, em vez de estar concentrada em uma única unidade, como no caso de um hot spare, portanto, você não fica limitado pela velocidade ou disponibilidade de uma única unidade.

Por que eu substituiria logicamente uma unidade?

Se uma unidade falhar ou se você quiser substituí-la por qualquer outro motivo, e houver uma unidade não atribuída em seu array de storage, você pode substituir logicamente a unidade com falha pela unidade não atribuída. Se você não tiver uma unidade não atribuída, poderá substituir fisicamente a unidade.

Os dados da unidade original são copiados ou reconstruídos na unidade de substituição.

Onde posso visualizar o status de uma unidade em processo de reconstrução?

Você pode visualizar o status da reconstrução da unidade no painel Operations in Progress.

Na página inicial, clique no link **Ver operações em andamento** no canto superior direito.

Dependendo da unidade, a reconstrução completa pode levar um tempo considerável. Se a propriedade de um volume tiver sido alterada, uma reconstrução completa pode ocorrer em vez da reconstrução rápida.

Alertas

Saiba mais sobre alertas no SANtricity System Manager

Você pode configurar SANtricity System Manager para enviar alertas do array de storage por e-mail, traps SNMP e mensagens syslog.

O que são alertas?

Alerts notificam os administradores sobre eventos importantes que ocorrem no array de storage. Os eventos podem incluir problemas como falha de bateria, um componente passando de Optimal para Offline ou erros de redundância no controlador. Todos os eventos Critical são considerados "alertáveis", juntamente com alguns eventos Warning e Informational.

Saiba mais:

- "Como funcionam os alertas"
- "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 um trap SNMP para um servidor SNMP ou como uma mensagem para um servidor syslog. A configuração de alertas está disponível em **Configurações › Alertas**.

Saiba mais:

- "Configurar o servidor de e-mail e os destinatários para alertas"
- "Configurar servidor syslog para alertas"
- "Configurar alertas SNMP"

Informações relacionadas

Saiba mais sobre conceitos relacionados a alertas:

- "Visão geral do log de eventos"
- "Registros de data e hora inconsistentes"

Conceitos

Como funcionam os alertas no SANtricity System Manager

Os alertas notificam os administradores sobre eventos importantes que ocorrem no array de storage. Os alertas podem ser enviados por e-mail, SNMP traps 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 email.
   - **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 array de storage detecta um problema, ele registra informações sobre esse problema no log de eventos (disponível em **Support › Event Log**). Por exemplo, os problemas podem incluir eventos como falha de bateria, um componente passando de Optimal para Offline ou erros de redundância no controlador.
3. Se o monitor de eventos determinar que o evento é "passível de alerta", ele então enviará uma notificação usando os métodos de alerta configurados (email, SNMP e/ou syslog). Todos os eventos críticos são

considerados "passíveis de alerta", juntamente com alguns eventos de aviso e informativos.

Configuração de alertas

Você pode configurar alertas no assistente de Configuração Inicial (somente para alertas por e-mail) ou na página Alertas. Para verificar a configuração atual, acesse **Configurações › Alertas**.

O bloco Alerts exibe a configuração de alertas, que pode ser uma das seguintes:

- Não configurado.
- Configurado; pelo menos um método de alerta está definido. Para determinar quais métodos de alerta estão configurados, posicione o cursor sobre o bloco.

Informações de alertas

Os alertas podem incluir os seguintes tipos de informação:

- Nome do array de storage.
- Tipo de erro de evento relacionado a uma entrada do log de eventos.
- Data e hora em que o evento ocorreu.
- Breve descrição do evento.

Os alertas do syslog seguem o padrão de mensagens RFC 5424.

Aprenda sobre a terminologia de alertas no software SANtricity

Saiba como os termos de alertas se aplicam ao seu array de storage.

Componente	Descrição
Monitor de eventos	O monitor de eventos reside no array de storage e é executado como uma tarefa em segundo plano. Quando o monitor de eventos detecta anomalias no array de storage, ele registra informações sobre os problemas no log de eventos. Os problemas podem incluir eventos como falha de bateria, um componente passando de Ideal para Offline ou erros de redundância no controlador. Se o monitor de eventos determinar que o evento é "alertável", ele então enviará uma notificação usando os métodos de alerta configurados (email, SNMP e/ou syslog). Todos os eventos Críticos são considerados "alertáveis", juntamente com alguns eventos de Aviso e Informativos.
Servidor de e-mail	O servidor de e-mail é usado para enviar e receber alertas por e-mail. O servidor utiliza Simple Mail Transfer Protocol (SMTP).
SNMP	Simple Network Management Protocol (SNMP) é um protocolo padrão da Internet usado para gerenciar e compartilhar informações entre dispositivos em redes IP.
Trap SNMP	Um SNMP trap é uma notificação enviada a um servidor SNMP. O trap contém informações sobre problemas significativos com o array de storage.

Componente	Descrição
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	O nome de comunidade é uma sequência de caracteres que funciona como uma senha para o(s) servidor(es) de rede em um ambiente SNMP.
Arquivo MIB	O arquivo MIB (Management Information Base) define os dados que estão sendo monitorados e gerenciados no array de storage. Ele deve ser copiado e compilado no servidor com o aplicativo de serviço SNMP. Este arquivo MIB está disponível com o System Manager no site de suporte.
Variáveis MIB	As variáveis da Base de Informações de Gerenciamento (MIB) podem retornar valores como o nome do array de storage, a localização do array e uma pessoa de contato em resposta ao SNMP GetRequests.
Syslog	Syslog é um protocolo usado por dispositivos de rede para enviar mensagens de eventos a um servidor de log.
UDP	O Protocolo de Datagrama do Usuário (UDP) é um protocolo da camada de transporte que especifica um número de porta de origem e um número de porta de destino nos cabeçalhos dos pacotes.

Gerenciar alertas de email

Configurar o servidor de e-mail e os destinatários de alertas no SANtricity System Manager

Para configurar alertas por e-mail, você deve especificar o endereço do servidor de e-mail e os endereços de e-mail dos destinatários dos alertas. Até 20 endereços de e-mail são permitidos.

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 precisa configurar um servidor DNS em ambos os controladores. Você pode configurar um servidor DNS na página Hardware.

- O endereço de e-mail a ser usado como remetente do alerta deve estar disponível. Este é o endereço que aparece no campo "De" da mensagem de alerta. Um endereço de remetente é obrigatório no protocolo SMTP; sem ele, ocorre um erro.
- Os endereços de e-mail dos destinatários do alerta devem estar disponíveis. O destinatário normalmente é um endereço para um administrador de rede ou administrador de storage. Você pode inserir até 20 endereços de e-mail.

Sobre esta tarefa

Esta tarefa descreve como configurar o servidor de e-mail, inserir endereços de e-mail para o remetente e os

destinatários e testar todos os endereços de e-mail inseridos na página de Alerts.

Os alertas por e-mail também podem ser configurados no assistente de configuração inicial.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **Email**.

   Se um servidor de e-mail ainda não estiver configurado, a guia E-mail exibirá "Configurar Mail Server."

3. Selecione **Configurar Mail Server**.

   A caixa de diálogo Configurar Servidor de Correio é aberta.

4. Insira as informações do servidor de e-mail e, em seguida, clique em **Salvar**.
   - **Endereço do servidor de e-mail** — Insira um domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6 do servidor de e-mail.

     Para usar um nome de domínio totalmente qualificado, você precisa configurar um servidor DNS em ambos os controladores. Você pode configurar um servidor DNS na página Hardware.

   - **Endereço do remetente do e-mail** — insira um endereço de e-mail válido para ser usado como remetente do e-mail. Este endereço aparece no campo "De" da mensagem de e-mail.
   - **Criptografia** — Se desejar criptografar as mensagens, selecione **SMTPS** ou **STARTTLS** para o tipo de criptografia e, em seguida, selecione o número da porta para as mensagens criptografadas. Caso contrário, selecione **None**.
   - **Nome de usuário e senha** — Se necessário, insira um nome de usuário e uma senha para autenticação com o remetente de saída e o servidor de e-mail.
   - **Incluir informações de contato no email** — Para incluir as informações de contato do remetente na mensagem de alerta, selecione esta opção e insira um nome e um número de telefone.

     Após clicar em **Salvar**, os endereços de e-mail aparecem na guia E-mail da página de Alertas.

5. Selecione **Add Emails**.

   A caixa de diálogo Adicionar Emails é aberta.

6. Insira um ou mais endereços de e-mail para os destinatários do alerta e clique em **Add**.

   Os endereços de e-mail aparecem na página Alerts.

7. Se quiser garantir que os endereços de e-mail são válidos, clique em **Test All Emails** para enviar mensagens de teste aos destinatários.

Resultados

Após configurar os alertas por e-mail, o monitor de eventos envia mensagens de e-mail aos destinatários especificados sempre que ocorre um evento passível de alerta.

Editar endereços de e-mail para alertas no SANtricity System Manager

Você pode alterar os endereços de e-mail dos destinatários que recebem alertas por e-mail.

Antes de começar

O endereço de e-mail que você pretende editar deve ser definido na guia Email da página de Alertas.

Passos

1. Selecione o menu: configurações [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. Digite um novo endereço e clique no ícone **Salvar** (marca de seleção).

   Se você quiser cancelar as alterações, selecione o ícone **Cancel** (X).

Resultados

A guia Email da página de Alertas exibe os endereços de email atualizados.

Adicionar endereços de e-mail para alertas no SANtricity System Manager

Você pode adicionar até 20 destinatários para alertas por e-mail.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **Email**.
3. Selecione **Add Emails**.

   A caixa de diálogo Adicionar Emails é aberta.

4. No campo vazio, insira um novo endereço de e-mail. Se desejar adicionar mais de um endereço, selecione **Adicionar outro e-mail** para abrir outro campo.
5. Clique em **Add**.

Resultados

A guia Email da página de Alertas exibe os novos endereços de email.

Excluir o servidor de e-mail ou os endereços de e-mail para alertas no SANtricity System Manager

Você pode remover o servidor de e-mail previamente definido para que os alertas não sejam mais enviados para os endereços de e-mail, ou pode remover endereços de e-mail individualmente.

Passos

1. Selecione o menu: configurações [Alertas].

2. Selecione a guia **Email**.
3. Na tabela, faça uma das seguintes ações:
   - Para remover um servidor de e-mail para que 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 **Excluir** no canto superior direito da tabela ficará disponível para seleção.
4. Clique em **Excluir** e confirme a operação.

Editar servidor de e-mail para alertas no SANtricity System Manager

Você pode alterar o endereço do servidor de e-mail e o endereço do remetente de e-mail usados para alertas por e-mail.

Antes de começar

O endereço do servidor de e-mail que você está alterando precisa 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 precisa configurar um servidor DNS em ambos os controladores. Você pode configurar um servidor DNS na página Hardware.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **Email**.
3. Selecione **Configurar Mail Server**.

   A caixa de diálogo Configurar Servidor de Correio é aberta.

4. Edite o endereço do servidor de e-mail, as informações do remetente e as informações de contato.
   - **Endereço do servidor de e-mail** — Edite o domínio totalmente qualificado, o endereço IPv4 ou o endereço IPv6 do servidor de e-mail.

     > Para usar um nome de domínio totalmente qualificado, você precisa configurar um servidor DNS em ambos os controladores. Você pode configurar um servidor DNS na página Hardware.

   - **Endereço do remetente do e-mail** — Edite o endereço de e-mail que será usado como remetente do e-mail. Este endereço aparece no campo "De" da mensagem de e-mail.
   - **Incluir informações de contato no email** — Para editar as informações de contato do remetente, selecione esta opção e, em seguida, edite o nome e o número de telefone.
5. Clique em **Salvar**.

Gerenciar alertas SNMP

Configurar alertas SNMP no SANtricity System Manager

Para configurar alertas do Protocolo Simples de Gerenciamento de Rede (SNMP), você deve identificar pelo menos um servidor para o qual o monitor de eventos do array de

storage possa enviar traps SNMP. A configuração requer um nome de comunidade ou nome de usuário e um endereço IP para o servidor.

Antes de começar

- É necessário configurar um servidor de rede com um aplicativo de serviço SNMP. Você precisa do endereço de rede desse servidor (um endereço IPv4 ou IPv6), para que o monitor de eventos possa enviar mensagens de trap para esse endereço. É possível usar mais de um servidor (até 10 servidores são permitidos).
- O arquivo de management information base (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.

  Caso não possua o arquivo MIB, você pode obtê-lo no site de suporte da NetApp:

  - Vá para "Suporte da NetApp".
  - Clique na guia **Downloads** e, em seguida, selecione **Downloads**.
  - Clique em **E-Series SANtricity OS Controller Software**.
  - Selecione **Download Latest Release**.
  - Faça login.
  - Aceite a declaração de cautela e o contrato de licença.
  - Role a página para baixo até ver o arquivo MIB para o seu tipo de controlador e, em seguida, clique no link para baixar o arquivo.

Sobre esta tarefa

Esta tarefa descreve como identificar o servidor SNMP para destinos de trap e, em seguida, testar sua configuração.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Na configuração inicial, a guia SNMP exibe "Configure Communities/Users."

3. Selecione **Configurar comunidades/usuários**.

   A caixa de diálogo Selecionar versão SNMP é aberta.

4. Selecione a versão SNMP para os alertas, **SNMPv2c** ou **SNMPv3**.

   Dependendo da sua seleção, a caixa de diálogo Configurar Comunidades ou a caixa de diálogo Configurar Usuários SNMPv3 é 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 string que identifica um conjunto conhecido de estações de gerenciamento e geralmente é criada por um administrador de rede. Consiste apenas em caracteres ASCII imprimíveis. Você pode adicionar até 256 comunidades. Quando terminar, clique em **Salvar**.
   - **SNMPv3 (usuários)** — Na caixa de diálogo Configurar SNMPv3 Users, clique em **Add** e insira as seguintes informações:

- **Nome de usuário** — Digite um nome para identificar o usuário, que pode ter até 31 caracteres.
- **ID do mecanismo** — Selecione o ID do mecanismo, 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 **Personalizado**; outro campo aparecerá onde você deverá inserir o ID do mecanismo autorizado como uma string hexadecimal, com um número par de caracteres entre 10 e 32 caracteres.
- **Credenciais de autenticação** — Selecione um protocolo de autenticação, que garante a identidade dos usuários. Em seguida, insira uma senha de autenticação, que é necessária quando o protocolo de autenticação é definido ou alterado. A senha deve ter entre 8 e 128 caracteres.
- **Credenciais de privacidade** — Selecione um protocolo de privacidade, que é usado para criptografar o conteúdo das mensagens. Em seguida, insira uma senha de privacidade, que é necessária quando o protocolo de privacidade é definido ou alterado. A senha deve ter entre 8 e 128 caracteres. Quando terminar, clique em **Adicionar** e depois em **Fechar**.

6. Na página de Alertas, com a aba SNMP selecionada, clique em **Add Trap Destinations**.

   A caixa de diálogo Adicionar Destinos de Trap é aberta.

7. Insira um ou mais destinos de trap, selecione os nomes de comunidade ou nomes de usuário associados e clique em **Adicionar**.
   - **Destino da armadilha** — Insira um endereço IPv4 ou IPv6 do servidor que executa um serviço SNMP.
   - **Nome da comunidade ou nome de usuário** — No menu suspenso, selecione o nome da comunidade (SNMPv2c) ou o nome de usuário (SNMPv3) para este destino de trap. (Se você definiu apenas um, o nome já aparece neste campo.)
   - **Enviar Trap de Falha de Autenticação** — selecione esta opção (a caixa de seleção) se desejar alertar o destino do trap sempre que uma solicitação SNMP for rejeitada devido a um nome de comunidade ou nome de usuário não reconhecido. Após clicar em **Adicionar**, os destinos do trap e os nomes associados aparecem na guia **SNMP** da página **Alertas**.
8. Para garantir que um trap seja válido, selecione um destino de trap na tabela e clique em **Testar Destino do Trap** para enviar um trap de teste para o endereço configurado.

Resultados

O monitor de eventos envia traps SNMP para o(s) servidor(es) sempre que ocorre um evento alertável.

Adicionar destinos de trap para alertas SNMP no SANtricity System Manager

Você pode adicionar até 10 servidores para enviar traps SNMP.

Antes de começar

- O servidor de rede que você deseja adicionar deve estar configurado com um aplicativo de serviço SNMP. Você precisa do endereço de rede desse servidor (um endereço IPv4 ou IPv6), para que o monitor de eventos possa enviar mensagens de trap para esse endereço. Você pode usar mais de um servidor (até 10 servidores são permitidos).
- O arquivo de management information base (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.

  Caso não possua o arquivo MIB, você pode obtê-lo no site de suporte da NetApp:

  - Vá para "Suporte da NetApp".

- Clique em **Downloads** e depois selecione **Downloads**.
- Clique em **E-Series SANtricity OS Controller Software**.
- Selecione **Download Latest Release**.
- Faça login.
- Aceite a declaração de cautela e o contrato de licença.
- Role a página para baixo até ver o arquivo MIB para o seu tipo de controlador e, em seguida, clique no link para baixar o arquivo.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os destinos de trap atualmente definidos aparecem na tabela.

3. Selecione **Add Trap Desinations**.

   A caixa de diálogo Adicionar Destinos de Trap é aberta.

4. Insira um ou mais destinos de trap, selecione os nomes de comunidade ou nomes de usuário associados e clique em **Adicionar**.
   - **Destino da armadilha** — Insira um endereço IPv4 ou IPv6 do servidor que executa um serviço SNMP.
   - **Nome da comunidade ou nome de usuário** — No menu suspenso, selecione o nome da comunidade (SNMPv2c) ou o nome de usuário (SNMPv3) para este destino de trap. (Se você definiu apenas um, o nome já aparece neste campo.)
   - **Enviar Trap de Falha de Autenticação** — Selecione esta opção (a caixa de seleção) se desejar alertar o destino do trap sempre que uma solicitação SNMP for rejeitada devido a um nome de comunidade ou nome de usuário não reconhecido. Depois de clicar em **Adicionar**, os destinos do trap e os nomes de comunidade ou nomes de usuário associados aparecem na tabela.
5. Para garantir que um trap seja válido, selecione um destino de trap na tabela e clique em **Testar Destino do Trap** para enviar um trap de teste para o endereço configurado.

Resultados

O monitor de eventos envia traps SNMP para o(s) servidor(es) sempre que ocorre um evento alertável.

Configurar variáveis MIB do SNMP no SANtricity System Manager

Para alertas SNMP, você pode opcionalmente configurar variáveis da Base de Informações de Gerenciamento (MIB) que aparecem nos traps SNMP. Essas variáveis podem retornar o nome do array de storage, a localização 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 você não tiver um arquivo MIB, poderá obtê-lo da seguinte forma:

- Vá para "Suporte da NetApp".
- Clique em **Downloads** e depois selecione **Downloads**.

- Clique em **E-Series SANtricity OS Controller Software**.
- Selecione **Download Latest Release**.
- Faça login.
- Aceite a declaração de cautela e o contrato de licença.
- Role a página para baixo até ver o arquivo MIB para o seu tipo de controlador e, em seguida, clique no link para baixar o 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 para o array de storage)
- `sysLocation` (localização do array de storage)
- `sysContact` (nome de um administrador)

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.
3. Selecione **Configurar variáveis MIB SNMP**.

   A caixa de diálogo Configurar variáveis MIB SNMP é aberta.

4. Insira um ou mais dos seguintes valores e clique em **Save**.
   - **Nome** — O valor para a variável MIB `sysName`. Por exemplo, insira um nome para o array de storage.
   - **Localização** — O valor da variável MIB `sysLocation`. Por exemplo, insira a localização do array de storage.
   - **Contato** — O valor para a variável MIB `sysContact`. Por exemplo, insira um administrador responsável pelo array de storage.

Resultados

Esses valores aparecem em mensagens de trap SNMP para alertas de array de storage.

Editar comunidades para traps SNMPv2c em SANtricity System Manager

Você pode editar nomes de comunidades para traps SNMPv2c.

Antes de começar

Um nome de comunidade deve ser criado.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os destinos das armadilhas e os nomes das comunidades aparecem na tabela.

3. Selecione **Configurar Communities**.

4. Digite o novo nome da comunidade e clique em **Save**. Os nomes das comunidades podem conter apenas caracteres ASCII imprimíveis.

Resultados

A guia SNMP da página de Alertas exibe o nome da comunidade atualizado.

${post_edited_translations.segment}

${post_edited_translations.segment}

Antes de começar

${post_edited_translations.segment}

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os destinos das armadilhas e os nomes de usuário aparecem na tabela.

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - **ID do mecanismo** — Selecione o ID do mecanismo, 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 **Personalizado**; outro campo aparecerá onde você deverá inserir o ID do mecanismo autorizado como uma string hexadecimal, com um número par de caracteres entre 10 e 32 caracteres.
   - **Credenciais de autenticação** — Selecione um protocolo de autenticação, que garante a identidade dos usuários. Em seguida, insira uma senha de autenticação, que é necessária quando o protocolo de autenticação é definido ou alterado. A senha deve ter entre 8 e 128 caracteres.
   - **Credenciais de privacidade** — Selecione um protocolo de privacidade, que é usado para criptografar o conteúdo das mensagens. Em seguida, insira uma senha de privacidade, que é necessária quando o protocolo de privacidade é definido ou alterado. A senha deve ter entre 8 e 128 caracteres.

Resultados

${post_edited_translations.segment}

Adicionar comunidades para traps SNMPv2c no SANtricity System Manager

Você pode adicionar até 256 nomes de comunidade para traps SNMPv2c.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os destinos das armadilhas e os nomes das comunidades aparecem na tabela.

3. Selecione **Configurar Communities**.

A caixa de diálogo Configurar Comunidades é aberta.

4. Selecione **Add another community**.
5. Digite o novo nome da comunidade e clique em **Save**.

Resultados

O novo nome da comunidade aparece na guia SNMP da página de Alertas.

Adicionar usuários para traps SNMPv3 no SANtricity System Manager

Você pode adicionar até 256 usuários para SNMPv3 traps.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os destinos das armadilhas e os nomes de usuário aparecem na tabela.

3. Selecione **Configurar Users**.

   A caixa de diálogo Configurar usuários SNMPv3 é aberta.

4. Selecione **Add**.
5. Insira as seguintes informações e clique em **Add**.
   - **Nome de usuário** — Digite um nome para identificar o usuário, que pode ter até 31 caracteres.
   - **ID do mecanismo** — Selecione o ID do mecanismo, 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 **Personalizado**; outro campo aparecerá onde você deverá inserir o ID do mecanismo autorizado como uma string hexadecimal, com um número par de caracteres entre 10 e 32 caracteres.
   - **Credenciais de autenticação** — Selecione um protocolo de autenticação, que garante a identidade dos usuários. Em seguida, insira uma senha de autenticação, que é necessária quando o protocolo de autenticação é definido ou alterado. A senha deve ter entre 8 e 128 caracteres.
   - **Credenciais de privacidade** — Selecione um protocolo de privacidade, que é usado para criptografar o conteúdo das mensagens. Em seguida, insira uma senha de privacidade, que é necessária quando o protocolo de privacidade é definido ou alterado. A senha deve ter entre 8 e 128 caracteres.

Remova comunidades para traps SNMPv2c no SANtricity System Manager

Você pode remover um nome de comunidade para traps SNMPv2c.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os destinos das armadilhas e os nomes das comunidades aparecem na página **Alerts**.

3. Selecione **Configurar Communities**.

   A caixa de diálogo Configurar Comunidades é aberta.

4. Selecione o nome da comunidade que deseja excluir e clique no ícone **Remover** (X) no canto direito.

   Se destinos de captura estiverem associados a esse nome de comunidade, a caixa de diálogo Confirmar Remoção da Comunidade exibirá os endereços de destino de captura afetados.

5. Confirme a operação e, em seguida, clique em **Remover**.

Resultados

O nome da comunidade e seu destino de trap associado foram removidos da página de Alertas.

Remover usuários para traps SNMPv3 em SANtricity System Manager

Você pode remover um usuário para traps SNMPv3.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os destinos das armadilhas e os nomes de usuário aparecem na página de Alerts.

3. Selecione **Configurar Users**.

   A caixa de diálogo Configurar usuários SNMPv3 é aberta.

4. Selecione o nome de usuário que deseja excluir e clique em **Delete**.
5. Confirme a operação e, em seguida, clique em **Excluir**.

Resultados

O nome de usuário e o destino de trap associados são removidos da página de Alertas.

Excluir destinos de trap no SANtricity System Manager

Você pode excluir um endereço de destino de trap para que o monitor de eventos do array de storage não envie mais traps SNMP para esse endereço.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os endereços de destino das armadilhas aparecem na tabela.

3. Selecione um destino de trap e clique em **Excluir** no canto superior direito da página.
4. Confirme a operação e, em seguida, clique em **Excluir**.

   O endereço de destino não aparece mais na página de Alertas.

Resultados

O destino de trap excluído não recebe mais traps SNMP do monitor de eventos do array de storage.

Gerenciar alertas do syslog

Configurar o servidor syslog para alertas no SANtricity System Manager

Para configurar alertas do syslog, você deve inserir o endereço de um servidor syslog e uma porta UDP. Até cinco servidores syslog são permitidos.

Antes de começar

- O endereço do servidor syslog deve estar disponível. Esse endereço pode ser um domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- O número da porta UDP do servidor syslog deve estar disponível. Essa porta normalmente é 514.

Sobre esta tarefa

Esta tarefa descreve como inserir o endereço e a porta do servidor syslog e, em seguida, testar o endereço inserido.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **Syslog**.

   Se um servidor syslog ainda não estiver definido, a página de Alertas exibirá "Adicionar servidores syslog".

3. Clique em **Adicionar Syslog Servers**.

   A caixa de diálogo Adicionar Servidor syslog é aberta.

4. Insira as informações de um ou mais servidores syslog (máximo de cinco) e clique em **Adicionar**.
   - **Endereço do servidor** — Insira um 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 para os endereços do servidor, selecione **Test All Syslog Servers**.

Resultados

O monitor de eventos envia alertas para o servidor syslog sempre que ocorre um evento que exige alerta. Para configurar ainda mais as definições do syslog para logs de auditoria, consulte "Configurar servidor syslog para logs de auditoria".

> Se vários servidores syslog estiverem configurados, todos os servidores syslog configurados receberão um log de auditoria.

Edite os servidores syslog para alertas no SANtricity System Manager

Você pode editar o endereço do servidor usado para receber alertas do syslog.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **Syslog**.
3. Na tabela, selecione um endereço de servidor syslog e clique no ícone **Editar** (lápis) no canto direito.

A linha se torna um campo editável.

4. Edite o endereço do servidor e o número da porta UDP e, em seguida, clique no ícone **Save** (marca de seleção).

Resultados

O endereço do servidor atualizado aparece na tabela.

Adicione servidores syslog para alertas no SANtricity System Manager

Você pode adicionar no máximo cinco servidores para alertas do syslog.

Antes de começar

- O endereço do servidor syslog deve estar disponível. Esse endereço pode ser um domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- O número da porta UDP do servidor syslog deve estar disponível. Essa porta normalmente é 514.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **Syslog**.
3. Selecione **Add Syslog Servers**.

   A caixa de diálogo Adicionar Servidor syslog é aberta.

4. Selecione **Adicionar outro servidor syslog**.
5. Insira as informações para o servidor syslog e clique em **Adicionar**.
   - **Endereço do servidor Syslog** — Insira um 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.

Excluir servidores syslog para alertas no SANtricity System Manager

Você pode excluir um servidor syslog para que ele não receba mais alertas.

Passos

1. Selecione o menu: configurações [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 exclusão do servidor syslog é aberta.

4. Confirme a operação e, em seguida, clique em **Excluir**.

Resultados

O servidor que você removeu não recebe mais alertas do monitor de eventos.

Perguntas frequentes sobre alertas do storage system para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

E se os alertas estiverem desativados?

Se você deseja que os administradores recebam notificações sobre eventos importantes que ocorrem no array de storage, é necessário configurar um método de alerta.

Para arrays de storage gerenciados com SANtricity System Manager, você configura alertas na página de Alertas. As notificações de alerta podem ser enviadas por e-mail, traps SNMP ou mensagens syslog. Além disso, alertas por e-mail podem ser configurados no 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 do Simple Network Management Protocol (SNMP) ou por mensagens de syslog.

Para configurar alertas SNMP ou syslog, acesse **Configurações › Alertas**.

Por que os registros de data e hora são inconsistentes entre o array de storage e os alertas?

Quando o array de storage envia alertas, ele não corrige o fuso horário do servidor ou host de destino que recebe os alertas. Em vez disso, o array de storage usa a hora local (GMT) para criar o registro de data e hora usado para o registro do alerta. Como resultado, você pode observar inconsistências entre os registros de data e hora do array de storage e do servidor ou host que recebe um alerta.

Como o array de storage não corrige o fuso horário ao enviar alertas, o registro de data e hora nos alertas é relativo ao GMT, que tem um deslocamento de fuso horário zero. Para calcular um registro de data e hora apropriado para o seu fuso horário local, você deve determinar o seu deslocamento de hora em relação ao GMT e então adicionar ou subtrair esse valor dos registros de data e hora.

Configurações do array

Saiba mais sobre a visão geral das configurações no SANtricity System Manager

Você pode configurar SANtricity System Manager para algumas configurações gerais do array e recursos complementares.

Quais configurações posso configurar?

As configurações do array incluem:

- "Configurações de cache e desempenho"
- "Balanceamento de carga automático"
- "Recursos adicionais"

- "Segurança de unidade"

Tarefas relacionadas

Saiba mais sobre tarefas relacionadas às System Settings:

- "Baixe a interface de linha de comando (CLI)"
- "Criar chave de segurança interna"
- "Criar chave de segurança externa"
- "Configurar portas iSCSI"
- "Configurar portas NVMe sobre IB"
- "Configurar NVMe sobre portas RoCE"

Conceitos

Saiba mais sobre configurações de cache e desempenho no software SANtricity

A memória cache é uma área de armazenamento temporário volátil no controlador que possui um tempo de acesso mais rápido do que a mídia de armazenamento.

Com o armazenamento em cache, o desempenho geral de E/S pode ser aumentado da seguinte forma:

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

As configurações de cache padrão atendem aos requisitos da maioria dos ambientes, mas você pode alterá-las se quiser.

Configurações de cache do array de storage

Para todos os volumes no array de storage, você pode especificar os seguintes valores na página System:

- **Valor inicial para limpeza** — a porcentagem de dados não gravados no cache que aciona uma limpeza do cache (gravação em disco). Quando o cache atinge a porcentagem inicial especificada de dados não gravados, uma limpeza é acionada. Por padrão, o controlador inicia a limpeza do cache quando o cache atinge 80 por cento de sua capacidade.
- **Tamanho do bloco de cache** — o tamanho máximo de cada bloco de cache, que é uma unidade organizacional para o 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 seus aplicativos. Sistemas de arquivos ou aplicativos de banco de dados geralmente usam tamanhos menores, enquanto um tamanho maior é bom para aplicativos que exigem grande transferência de dados ou E/S sequencial.

Configurações de cache de volume

Para volumes individuais em um array de storage, você pode especificar os seguintes valores na página Volumes (**Storage › Volumes**):

- **Armazenamento em cache de leitura** — 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 serem liberados.
  - **Pré-busca dinâmica de leitura em cache** — A pré-busca dinâmica de leitura em cache permite que o controlador copie blocos de dados sequenciais adicionais para o cache enquanto lê blocos de dados de uma unidade para o cache. Esse armazenamento em cache aumenta a chance de que solicitações futuras de dados possam ser atendidas pelo cache. A pré-busca dinâmica de leitura em cache é importante para aplicativos multimídia que usam E/S sequencial. A taxa e a quantidade de dados pré-buscados para o cache se ajustam automaticamente com base na taxa e no tamanho da solicitação de leitura do host. O acesso aleatório não faz com que dados sejam pré-buscados para o cache. Esse recurso não se aplica quando o armazenamento em cache 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 serem gravados nas unidades. Write caching pode aumentar o desempenho de E/S.

> **Possível perda de dados** — Se você ativar a opção **Gravar em cache sem baterias** e não tiver uma fonte de alimentação universal para proteção, poderá perder dados. Além disso, você poderá perder dados se não tiver baterias do controlador e ativar a opção **Gravar em cache sem baterias**.

  - **Armazenamento em cache de gravação sem baterias** — A configuração de armazenamento em cache de gravação sem baterias permite que o armazenamento em cache continue mesmo quando as baterias estão ausentes, com defeito, completamente descarregadas ou não totalmente carregadas. Escolher armazenamento em cache de gravação sem baterias geralmente não é recomendado, pois os dados podem ser perdidos se houver uma queda de energia. Normalmente, o armazenamento em cache de gravação é desativado temporariamente pelo controlador até que as baterias sejam carregadas ou uma bateria com defeito seja substituída.
  - **Armazenamento em cache com espelhamento** — armazenamento em cache com espelhamento ocorre quando os dados gravados na memória cache de um controlador também são gravados na memória 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 está disponível somente se o armazenamento em cache de gravação estiver habilitado e houver dois controladores. O armazenamento em cache com espelhamento é a configuração padrão na criação do volume.

Saiba mais sobre o balanceamento de carga automático no software SANtricity

O balanceamento automático de carga proporciona gerenciamento de recursos de I/O aprimorado, reagindo dinamicamente às mudanças 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 são transferidas entre os controladores.

A carga de trabalho de cada controlador é monitorada continuamente e, com a cooperação dos multipath drivers instalados nos hosts, pode ser automaticamente reequilibrada sempre que necessário. Quando a carga de trabalho é reequilibrada automaticamente entre os controladores, o administrador de storage fica livre da tarefa de ajustar manualmente a propriedade dos controladores de volume para acomodar as mudanças de carga no array de storage.

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 I/O entre os hosts e o array de storage.

Ativando e desativando o balanceamento de carga automático

O balanceamento de carga automático está ativado por padrão em todos os arrays de storage.

Você pode querer desativar o Balanceamento de Carga Automático em seu array de storage pelos seguintes motivos:

- Você não deseja alterar automaticamente a propriedade do controlador de um determinado volume para equilibrar a carga de trabalho.
- Você está operando em um ambiente altamente otimizado, onde a distribuição de carga é configurada propositalmente para alcançar uma distribuição específica entre os controladores.

Tipos de hosts que suportam o recurso de Automatic Load Balancing

Embora o balanceamento de carga automático esteja habilitado no array de storage, o tipo de host que você seleciona para um host ou cluster de hosts influencia diretamente como o recurso opera.

Ao equilibrar a carga de trabalho do array de storage entre os controladores, o recurso de Balanceamento Automático de Carga tenta mover volumes que sejam acessíveis por ambos os controladores e que estejam mapeados apenas para um host ou cluster de hosts capaz de suportar o recurso de Balanceamento Automático de Carga.

Esse comportamento impede que um host perca o acesso a um volume devido ao processo de distribuição de carga; no entanto, a presença de volumes mapeados para hosts que não suportam o Balanceamento Automático de Carga afeta a capacidade do array de storage de equilibrar a carga de trabalho. Para que o Balanceamento Automático de Carga possa equilibrar a carga de trabalho, o driver multipath deve suportar TPGS e o tipo de host deve estar incluído na tabela a seguir.

> Para que um cluster de hosts seja considerado capaz de realizar Automatic Load Balancing, todos os hosts desse grupo devem ser capazes de suportar Automatic Load Balancing.

Tipo de host compatível com distribuição automática de carga	Com este multipath driver
Windows ou Windows Clustered	MPIO com NetApp E-Series DSM
Linux DM-MP (Kernel 3.10 ou posterior)	DM-MP com `scsi_dh_alua` device handler
VMware	Plug-in de multipathing nativo (NMP) com `VMW_SATP_ALUA Storage Array Type` plug-in

> Com pequenas exceções, os tipos de host que não suportam balanceamento de carga automático continuam a operar normalmente, independentemente de o recurso estar ativado. Uma exceção é que, se um sistema tiver um failover, os arrays de storage movem volumes não mapeados ou não atribuídos de volta para o controlador proprietário quando o caminho de dados retorna. Quaisquer volumes que estejam mapeados ou atribuídos a hosts sem balanceamento de carga automático não são movidos.

Consulte a "Ferramenta de Matriz de Interoperabilidade" para obter informações de compatibilidade para driver multipath específico, nível do sistema operacional e suporte à bandeja de controlador/unidade.

Verificando a compatibilidade do sistema operacional com o recurso Automatic Load Balancing

Verifique a compatibilidade do sistema operacional com o recurso Automatic Load Balancing antes de configurar um novo sistema (ou migrar um sistema existente).

1. Acesse o "Ferramenta de Matriz de Interoperabilidade" para encontrar sua solução e verificar o suporte.

   Se o seu sistema estiver executando 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 tanto `retain_attached_device_handler` quanto `detect_prio` estejam definidos como `yes` para o fornecedor e produto aplicáveis, ou utilize as configurações padrão.

Configurar configurações do array

Editar o nome do array de storage no SANtricity System Manager

Você pode alterar o nome do array de storage que aparece na barra de título do SANtricity System Manager.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Geral**, procure o campo **Name:**.

   Se um array de storage não tiver um nome definido, este campo exibirá "Desconhecido".

3. Clique no ícone **Editar** (lápis) ao lado do nome do array de storage.

   O campo torna-se editável.

4. Digite um novo nome.

   Um nome pode conter letras, números e os caracteres especiais sublinhado (_), hífen (-) e cerquilha (#). Um nome não pode conter espaços. Um nome pode ter um comprimento máximo de 30 caracteres. O nome deve ser único.

5. Clique no ícone **Save** (marca de seleção).

   Se você quiser fechar o campo editável sem fazer alterações, clique no ícone **Cancel** (X).

Resultados

O novo nome aparece na barra de título do SANtricity System Manager.

Ative as luzes localizadoras do array de storage no SANtricity System Manager

Para localizar fisicamente um array de storage em um gabinete, você pode acender suas luzes localizadoras (LED).

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Geral**, clique em **Ativar luzes indicadoras do array de storage**.

   A caixa de diálogo Ativar luzes indicadoras do array de storage é aberta e as luzes indicadoras do array de storage correspondente são acesas.

3. Após localizar fisicamente o array de storage, retorne à caixa de diálogo e selecione **Desligar**.

Resultados

As luzes indicadoras se apagam e a caixa de diálogo se fecha.

Sincronize os relógios do array de storage no SANtricity System Manager

Se o Network Time Protocol (NTP) não estiver ativado, você pode configurar manualmente os relógios dos controladores para que sejam sincronizados com o cliente (o sistema usado para executar o navegador que acessa SANtricity System Manager).

Sobre esta tarefa

A sincronização garante que os registros de data e hora dos eventos no log de eventos correspondam aos registros de data e hora gravados nos arquivos de log do host. 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 os 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, os agendamentos são afetados (ASUP, snapshots, etc.) e os registros de data e hora nos dados de log ficam distorcidos. Usar NTP evita esse problema.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Geral**, clique em **Sincronizar relógios do array de storage**.

   A caixa de diálogo Sincronizar Relógios do Array de Storage é aberta. Ela exibe a data e a hora atuais do(s) controlador(es) e do computador usado como cliente de gerenciamento.

   > Para arrays de storage simplex, apenas um controlador é mostrado.

3. Se os horários exibidos na caixa de diálogo não coincidirem, clique em **Synchronize**.

Resultados

Após a sincronização ser bem-sucedida, os registros de data e hora dos eventos são os mesmos no log de eventos e nos logs do host.

Salvar a configuração do array de storage no SANtricity System Manager

Você pode salvar as informações de configuração de um array de storage em um arquivo de script para economizar tempo na configuração de arrays de storage adicionais com a

mesma configuração.

Antes de começar

O array de storage não deve estar passando por nenhuma operação que altere suas configurações lógicas. Exemplos dessas operações incluem criar ou excluir volumes, fazer download do firmware do controlador, atribuir ou modificar unidades hot spare ou adicionar capacidade (unidades) a um grupo de volume.

Sobre esta tarefa

Salvar a configuração do array de storage gera um script de interface de linha de comando (CLI) que contém as configurações do array de storage, configuração de volume, configuração de host ou atribuições de host para volume para um array de storage. Você pode usar esse script CLI gerado para replicar uma configuração para outro array de storage com exatamente a mesma configuração de hardware.

No entanto, você não deve usar este 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 do Auto-Support mais recente.

Esta operação *não* salva estas configurações:

- A vida útil da bateria
- A hora do dia do controlador
- As configurações da memória estática não volátil de acesso aleatório (NVSRAM)
- Quaisquer recursos premium
- A senha do array de storage
- O status operacional e os estados dos componentes de hardware
- O status operacional (exceto Optimal) e os estados dos grupos de volume
- Serviços de cópia, como espelhamento e cópia de volume

Risco de erros de aplicação — Não utilize esta opção se o array de storage estiver passando por uma operação que altere qualquer configuração lógica. Exemplos dessas operações incluem criar ou excluir volumes, fazer download de firmware, atribuir ou modificar unidades hot spare ou adicionar capacidade (unidades) a um grupo de volume.

Passos

1. Selecione o menu: configurações [Sistema].
2. Selecione **Save Storage Array Configuration**.
3. Selecione os itens da configuração que deseja salvar:
    - Configurações do array de storage
    - Configuração de volume
    - Configuração do host
    - Atribuições de host para volume

Se você selecionar o item **Atribuições de host para volume**, os itens **Configuração de volume** e **Configuração de host** também serão selecionados por padrão. Não é possível salvar "Atribuições de host para volume" sem também salvar "Configuração de volume" e "Configuração de host".

4. Clique em **Salvar**.

   O arquivo é salvo na pasta Downloads do seu navegador com o nome `storage-array-configuration.cfg`.

Depois que você terminar

Para carregar a configuração do array de storage salva em outro array de storage, use a interface de linha de comando SANtricity (SMcli) com a opção `-f` para aplicar o arquivo `.cfg`.

> Você também pode carregar uma configuração de array de storage para outros arrays de storage usando a interface Unified Manager (selecione **Manage › Import Settings**).

Limpar configuração do array de storage no SANtricity System Manager

Use a operação Clear Configuration quando desejar excluir todos os pools, grupos de volumes, volumes, definições de host e atribuições de host do array de storage.

Antes de começar

Antes de limpar a configuração do array de storage, faça backup dos dados.

Sobre esta tarefa

Existem duas opções de Clear Storage Array Configuration:

- **Volume** — Normalmente, você pode usar a opção Volume para reconfigurar um array de storage de teste como um array de storage de produção. Por exemplo, você pode configurar um array de storage para testes e, ao concluir os testes, remover a configuração de teste e configurar o array de storage para um ambiente de produção.
- **Storage Array** — Normalmente, você usaria a opção Storage Array para mover um array de storage para outro departamento ou grupo. Por exemplo, você pode estar usando um array de storage na Engineering, e agora Engineering está recebendo um novo array de storage, então você deseja mover o array de storage para Administration, onde ele será reconfigurado.

  A opção Storage Array exclui algumas configurações adicionais.

	Volume	Array de storage
Desativa ARVM	X	X
Exclui pools e grupos de volumes	X	X
Exclui volumes	X	X
Exclui hosts e clusters de hosts	X	X
Exclui atribuições de host	X	X
Exclui nome do array de storage		X

	Volume	Array de storage
Redefine as configurações de cache do array de storage para o padrão		X

Risco de perda de dados — Esta operação apaga todos os dados do seu array de storage. (Não realiza uma exclusão segura.) Você não poderá cancelar esta operação após o início. Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

Passos

1. Selecione o menu: configurações [Sistema].
2. Selecione **Clear Storage Array Configuration**.
3. Na lista suspensa, selecione **Volume** ou **Storage Array**.
4. **Opcional:** Se desejar salvar a configuração (não os dados), utilize os links na caixa de diálogo.
5. Confirme que você deseja realizar a operação.

Resultados

- A configuração atual é excluída, destruindo todos os dados existentes no array de storage.
- Todas as unidades estão não atribuídas.

O array de storage será iniciado no modo de recuperação. Você deve limpar o modo de recuperação antes de usar o array de storage. Consulte "Limpar modo de recuperação" para mais informações.

Alterar as configurações de cache do array de storage no SANtricity System Manager

Para todos os volumes no array de storage, você pode ajustar as configurações de memória cache para liberação e tamanho do bloco.

Sobre esta tarefa

A memória cache é uma área de armazenamento temporário volátil no controlador, que possui um tempo de acesso mais rápido do que a mídia da unidade. Para otimizar o desempenho da memória cache, você pode ajustar as seguintes configurações:

Configuração de armazenamento em cache	Descrição
Iniciar limpeza do cache de demanda	Start demand cache flushing especifica a porcentagem de dados não gravados no cache que aciona uma limpeza do cache (gravação em disco). Por padrão, a limpeza do cache começa quando os dados não gravados atingem 80% da capacidade. Uma porcentagem maior é uma boa escolha para ambientes com operações predominantemente de gravação, assim novas solicitações de gravação podem ser processadas pelo cache sem precisar acessar o disco. Configurações menores são melhores em ambientes onde a E/S é irregular (com rajadas de dados), para que o sistema limpe o cache frequentemente entre essas rajadas. No entanto, uma porcentagem inicial menor que 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 o gerenciamento de cache. Por padrão, o tamanho do bloco é 32 KiB. O sistema permite que o tamanho do bloco de cache seja 4, 8, 16 ou 32 KiBs. Os aplicativos usam tamanhos de bloco diferentes, o que impacta o desempenho do armazenamento. Um tamanho menor é uma boa escolha para sistemas de arquivos ou aplicativos de banco de dados. Um tamanho maior é ideal para aplicativos que geram E/S sequencial, como multimídia.

Passos

1. Selecione o menu: configurações [Sistema].
2. Desça até **Configurações adicionais** e, em seguida, clique em **Alterar configurações de cache**.

   A caixa de diálogo Alterar configurações de cache é aberta.

3. Ajuste os seguintes valores:
   - **Iniciar a limpeza do cache sob demanda** — Escolha uma porcentagem adequada para a E/S usada em seu ambiente. Se você escolher um valor inferior a 80%, poderá notar diminuição no desempenho.
   - **Tamanho do bloco de cache —** Escolha um tamanho adequado para suas aplicações.
4. Clique em **Salvar**.

Defina o balanceamento de carga automático no SANtricity System Manager

O recurso de balanceamento de carga automático garante que o tráfego de E/S proveniente dos hosts seja gerenciado e balanceado dinamicamente entre ambos os controladores. Esse recurso está habilitado por padrão, mas você pode desabilitá-lo no SANtricity 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 I/O entre os hosts e o array de storage.

Você pode querer desativar o Balanceamento de Carga Automático em seu array de storage pelos seguintes motivos:

- Você não deseja alterar automaticamente a propriedade do controlador de um determinado volume para equilibrar a carga de trabalho.
- Você está operando em um ambiente altamente otimizado, onde a distribuição de carga é configurada propositalmente para alcançar uma distribuição específica entre os controladores.

Passos

1. Selecione o menu: configurações [Sistema].
2. Desça até **Configurações adicionais** e, em seguida, clique em **Ativar/Desativar balanceamento de carga automático**.

   O texto abaixo desta opção indica se o recurso está atualmente ativado ou desativado.

   Uma caixa de diálogo de confirmação é aberta.

3. Confirme clicando em **Yes** para continuar.

   Ao selecionar esta opção, você alterna o recurso entre ativado/desativado.

   Se esse recurso for alterado de desativado para ativado, o recurso de Relatório de Conectividade de Host também será ativado automaticamente.

${post_edited_translations.segment}

${post_edited_translations.segment}

Sobre esta tarefa

Por padrão, a interface de gerenciamento legada está ativada. Se você desabilitá-la, o array de storage 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 ela for desabilitada.

${post_edited_translations.segment}

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- **Desativado** — Configuração necessária para impor a confidencialidade nas comunicações entre o array de storage e o cliente de gerenciamento, e para acessar ferramentas externas. Configuração recomendada ao configurar um Directory Server (LDAP).

Passos

1. Selecione o menu: configurações [Sistema].
2. Desça até **Configurações adicionais** e clique em **Alterar interface de gerenciamento**.
3. Na caixa de diálogo, clique em **Yes** para continuar.

Configurar recursos adicionais

Como funcionam os recursos adicionais no SANtricity System Manager

Os complementos são funcionalidades que não estão incluídas na configuração padrão do SANtricity System Manager e podem exigir uma chave para serem ativados. Um complemento pode ser tanto um recurso premium individual quanto um pacote de recursos.

Os passos a seguir fornecem uma visão geral para ativar um recurso premium ou pacote de recursos:

1. Obtenha as seguintes informações:
   - O número de série do chassi e o Identificador de Habilitação do Recurso, que identificam o array de storage 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 do recurso para ativação.
3. Usando o System Manager, habilite o recurso premium ou o pacote de recursos usando o arquivo de chave de recurso.

Aprenda sobre a terminologia de recursos adicionais no software SANtricity

Saiba como os termos dos recursos adicionais se aplicam ao seu array de storage.

Termo	Descrição
Identificador de ativação de recurso	Um Identificador de Habilitação de Recurso é uma sequência de caracteres exclusiva que identifica o array de storage. Esse identificador garante que, ao obter o recurso premium, ele seja associado somente a esse array de storage. Essa sequência de caracteres é exibida em Complementos na página Sistema.
Arquivo de chave de feature	Um arquivo de chave de recurso é um arquivo que você recebe para desbloquear e ativar um recurso premium ou pacote de recursos.
Pacote de recursos	Um pacote de recursos é um pacote que altera os atributos do array de storage (por exemplo, alterando o protocolo de Fibre Channel para iSCSI). Pacotes de recursos exigem uma chave especial para habilitá-los.
Recurso premium	Um recurso premium é uma opção extra que requer uma chave para ser ativado. Ele não está incluído na configuração padrão do System Manager.

Obtenha um arquivo de chave de recurso no SANtricity System Manager

Para habilitar um recurso premium ou um pacote de recursos em seu array de storage, você deve primeiro obter um arquivo de chave de recurso. Uma chave está associada a apenas um array de storage.

Sobre esta tarefa

Esta tarefa descreve como coletar as informações necessárias para o recurso e, em seguida, enviar uma solicitação para um arquivo de chave do recurso. As informações necessárias incluem:

- Número de série do chassi
- Identificador de ativação de recurso
- Código de ativação do recurso

Passos

1. No System Manager, localize e anote o número de série do chassi. Você pode visualizar esse número de série passando o cursor do mouse sobre o bloco da Central de Suporte.
2. No System Manager, localize o Identificador de Habilitação de Recursos. Vá para **Configurações › Sistema** e role para baixo até **Complementos**. Procure pelo **Identificador de Habilitação de Recursos**. Anote o número do Identificador de Habilitação de Recursos.
3. Localize e anote o código de ativação do recurso. Para pacotes de recursos, esse código é fornecido nas instruções apropriadas para realizar a conversão.

   Para recursos premium, você pode acessar o código de ativação no site de suporte, da seguinte forma:

   a. Faça login em "Suporte da NetApp".
   b. Vá para **Licenças de Software** do seu produto.
   c. Insira o número de série do chassi do array de storage e clique em **Ir**.
   d. Procure os códigos de ativação de recursos na coluna **License Key**.
   e. Anote o código de ativação do recurso que você deseja.
4. Solicite um arquivo de chave de recurso enviando um e-mail ou um documento de texto para seu fornecedor de storage com as seguintes informações: número de série do chassi, o identificador de habilitação e o código para ativação do recurso.

   Você também pode acessar "NetApp License Activation: ativação do recurso premium do array de storage" e inserir as informações necessárias para obter o recurso ou pacote de recursos. (As instruções neste site são para recursos premium, não para pacotes de recursos.)

Depois que você terminar

Quando você possui um arquivo de chave de recurso, pode ativar o recurso premium ou o pacote de recursos.

Habilite um recurso premium no SANtricity System Manager

Um recurso premium é uma opção extra que requer uma chave para habilitar.

Antes de começar

- Você obteve uma chave de recurso. Se necessário, entre em contato com o suporte técnico para uma chave.
- Você carregou o arquivo de chave no cliente de gerenciamento (o sistema com um navegador para acessar System Manager).

Sobre esta tarefa

Esta tarefa descreve como usar System Manager para habilitar um recurso premium.

> Se você deseja desativar um recurso premium, deve usar o comando Disable Storage Array Feature (`disable storageArray) (featurePack | feature=featureAttributeList`) na interface de linha de comando (CLI).

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Complementos**, selecione **Enable Premium Feature**.

   A caixa de diálogo Ativar um recurso premium é aberta.

3. Clique em **Procurar** e, em seguida, selecione o arquivo de chave.

   O nome do arquivo é exibido na caixa de diálogo.

4. Clique em **Enable**.

Ativar o pacote de recursos no SANtricity System Manager

Um feature pack é um pacote que altera os atributos do array de storage (por exemplo, alterando o protocolo de Fibre Channel para iSCSI). Feature packs exigem uma chave especial para capacitação.

Antes de começar

- Você seguiu as instruções apropriadas que descrevem a conversão e a preparação para os novos atributos do array de storage. Para instruções sobre a conversão do protocolo do host, consulte o guia de manutenção de hardware para o seu modelo de controlador.
- O array de storage está offline, portanto nenhum host ou aplicação está acessando-o.
- Todos os dados estão em backup.
- Você obteve um arquivo de feature pack.

  O arquivo do pacote de recursos é carregado no cliente de gerenciamento (o sistema com um navegador para acessar System Manager).

> Você deve agendar uma janela de manutenção de inatividade e interromper todas as operações de E/S entre o host e os controladores. Além disso, esteja ciente de que não será possível acessar os dados no array de storage até que a conversão seja concluída com sucesso.

Sobre esta tarefa

Esta tarefa descreve como usar System Manager para habilitar um pacote de recursos. Quando terminar, você deve reinicializar o array de storage.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Complementos**, selecione **Change Feature Pack**.
3. Clique em **Procurar** e, em seguida, selecione o arquivo de chave.

   O nome do arquivo é exibido na caixa de diálogo.

4. Digite `change` no campo.
5. Clique em **Change**.

   A migração do pacote de recursos é iniciada e os controladores reinicializam. Os dados de cache não gravados são excluídos, o que garante que não haja atividade de E/S. Ambos os controladores

reinicializam automaticamente para que o novo pacote de recursos entre em vigor. O array de storage retorna a um estado responsivo após a conclusão da reinicialização.

Baixe a interface de linha de comando (CLI) do SANtricity

No SANtricity System Manager, você pode baixar o pacote da interface de linha de comando (CLI).

A CLI fornece um método baseado em texto para configurar e monitorar arrays de storage. Ela se comunica via https e usa a mesma sintaxe da CLI disponível no pacote de software de gerenciamento instalado externamente. Nenhuma chave é necessária para baixar a CLI.

Antes de começar

Um Java Runtime Environment (JRE), versão 8 ou superior, deve estar disponível no sistema de gerenciamento onde você planeja executar os comandos da CLI.

Passos

1. Selecione o menu: configurações [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 da interface de linha de comando para o array de storage e, em seguida, extraia o arquivo.

   Agora você pode executar comandos da CLI a partir de um prompt do sistema operacional, como o prompt C: do DOS. Uma referência de comandos da CLI está disponível no menu Ajuda, no canto superior direito da interface de usuário do System Manager.

Perguntas frequentes sobre as configurações do array de storage para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

O que é balanceamento automático de carga?

O recurso de balanceamento automático de carga proporciona balanceamento automático de I/O e garante que o tráfego de I/O proveniente dos hosts seja gerenciado e balanceado dinamicamente entre ambos os controladores.

O recurso de balanceamento automático de carga proporciona um gerenciamento de recursos de I/O aprimorado, reagindo dinamicamente às mudanças 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 são transferidas entre os controladores.

A carga de trabalho de cada controlador é monitorada continuamente e, com a cooperação dos multipath drivers instalados nos hosts, pode ser automaticamente reequilibrada sempre que necessário. Quando a carga de trabalho é reequilibrada automaticamente entre os controladores, o administrador de storage fica livre da tarefa de ajustar manualmente a propriedade dos controladores de volume para acomodar as mudanças de carga no array de storage.

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 I/O entre os hosts e o array de storage.

Qualquer volume atribuído ao uso do SSD Cache de um controlador não é elegível para transferência automática de load balance.

O que é cache do controlador?

O cache do controlador é um espaço de memória física que otimiza dois tipos de operações de E/S (entrada/saída): entre os controladores e hosts, e entre os controladores e discos.

Para transferências de dados de leitura e gravação, os hosts e controladores comunicam-se por meio de conexões de alta velocidade. No entanto, a comunicação do back-end do controlador para os discos é mais lenta, pois os discos são dispositivos relativamente lentos.

Quando o cache do controlador recebe dados, o controlador confirma aos aplicativos do host que agora está mantendo os dados. Dessa forma, os aplicativos do host não precisam esperar que a E/S seja gravada em disco. Em vez disso, os aplicativos podem continuar as operações. Os dados em cache também ficam prontamente acessíveis pelos aplicativos do servidor, eliminando a necessidade de leituras adicionais de disco para acessar os dados.

O cache do controlador afeta o desempenho geral do array de storage de várias maneiras:

- O cache funciona como um buffer, assim as transferências de dados entre o host e o disco não precisam 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 armazenamento em cache de gravação for utilizado, o host pode enviar comandos de gravação subsequentes antes que os dados de uma operação de gravação anterior sejam gravados em disco.
- Se o pré-carregamento de cache estiver ativado, o acesso de leitura sequencial é otimizado. O pré-carregamento de cache torna mais provável que uma operação de leitura encontre seus dados no cache, em vez de ler os dados do disco.

Possível perda de dados — Se você ativar a opção **Gravar em cache sem baterias** e não tiver uma fonte de alimentação universal para proteção, poderá perder dados. Além disso, você poderá perder dados se não tiver baterias do controlador e ativar a opção **Gravar em cache sem baterias**.

O que é cache flushing?

Quando a quantidade de dados não gravados no cache atinge um determinado nível, o controlador grava periodicamente os dados em cache em uma unidade. Esse processo de gravação é chamado de "flushing".

O controlador utiliza dois algoritmos para limpar o cache: baseado em demanda e baseado em idade. O controlador utiliza um algoritmo baseado em demanda até que a quantidade de dados em cache caia abaixo do limite de limpeza do cache. Por padrão, uma limpeza é iniciada quando 80 por cento do cache está em uso.

No System Manager, você pode definir o limite de “Start demand cache flushing” para melhor suportar o tipo

de E/S usado em seu ambiente. Em um ambiente com operações predominantemente de gravação, você deve definir a porcentagem de “Start demand cache flushing” como alta para aumentar a probabilidade de que novas solicitações de gravação possam ser processadas pelo cache sem precisar acessar o disco. Uma porcentagem alta limita o número de limpezas de cache, de modo que mais dados permaneçam no cache, o que aumenta a chance de mais acertos de cache.

Em um ambiente onde a E/S é errática (com picos de dados), você pode usar uma limpeza de cache baixa para que o sistema limpe o cache frequentemente entre os 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 por cento como um bom meio-termo. Esteja ciente de que, se você escolher uma porcentagem inicial inferior a 80 por cento, poderá observar uma queda no desempenho porque os dados necessários para uma leitura do host podem não estar disponíveis. Escolher uma porcentagem menor também aumenta o número de gravações em 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 estarem aptos a serem liberados para os discos. Os controladores usam o algoritmo baseado em idade até que o limite de liberação do cache seja atingido. O padrão é 10 segundos, mas esse período é contado apenas durante períodos de inatividade. Você não pode modificar o tempo de liberação no System Manager; em vez disso, deve usar o comando **Set Storage Array** na interface de linha de comando (CLI).

Possível perda de dados — Se você ativar a opção **Gravar em cache sem baterias** e não tiver uma fonte de alimentação universal para proteção, poderá perder dados. Além disso, você poderá perder dados se não tiver baterias do controlador e ativar a opção **Gravar em cache sem baterias**.

O que é o tamanho do bloco de cache?

O controlador do array de storage organiza seu cache em "blocos", que são partes da memória que podem ter 8, 16 ou 32 KiB de tamanho. Todos os volumes no sistema de storage compartilham o mesmo espaço de cache; portanto, os volumes podem ter apenas um tamanho de bloco de cache.

Os aplicativos usam diferentes tamanhos de bloco, que podem ter um impacto no desempenho do storage. Por padrão, o tamanho do bloco no System Manager é 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 transferência de dados grandes, E/S sequencial ou alta largura de banda, como multimídia.

Quando devo sincronizar os relógios do array de storage?

Você deve sincronizar manualmente os relógios do controlador no array de storage se notar que os registros de data e hora exibidos no SANtricity System Manager não estão alinhados com os registros de data e hora exibidos no seu cliente (o computador que está acessando SANtricity System Manager pelo navegador). Essa tarefa só é necessária se o NTP (Network Time Protocol) não estiver habilitado no SANtricity System Manager.

Recomendamos vivamente que utilize um servidor NTP em vez de sincronizar os relógios manualmente. O 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 do Array de Storage, disponível na página System. Se os horários exibidos na caixa de diálogo não coincidirem, execute uma sincronização. Você pode visualizar periodicamente esta caixa de diálogo, que indica se os horários exibidos

pelos relógios do controlador se desalinharem e não estiverem mais sincronizados.

Segurança de unidade

Saiba mais sobre segurança de unidades em SANtricity System Manager

Você pode configurar Drive Security e o gerenciamento de chaves na página Security Key Management.

O que é Drive Security?

Drive Security é um recurso que impede o acesso não autorizado a dados em drives com segurança habilitada quando removidos do array de storage. Esses drives podem ser Full Disk Encryption (FDE) drives ou Federal Information Processing Standard (FIPS) drives. Quando drives FDE ou FIPS são fisicamente removidos do array, eles não podem operar até serem instalados em outro array, momento em que os drives ficarão em um estado de Security Locked até que a security key correta seja fornecida. Uma *security key* é uma sequência de caracteres compartilhada entre esses tipos de drives e os controladores em um array de storage.

Saiba mais:

- "Como funciona o recurso Drive Security"
- "Como funciona o gerenciamento de chaves de segurança"
- "Terminologia de segurança de drive"

Como faço para configurar o gerenciamento de chaves?

Para implementar Drive Security, você deve ter unidades FDE ou FIPS instaladas no array. Para configurar o gerenciamento de chaves para essas unidades, acesse **Settings › Sistema › Security key management**, onde você pode criar uma chave interna a partir da memória persistente do controlador ou uma chave externa a partir de um servidor de gerenciamento de chaves. Por fim, habilite Drive Security para pools e grupos de volumes selecionando "secure-capable" nas configurações do volume.

Saiba mais:

- "Criar chave de segurança interna"
- "Criar chave de segurança externa"
- "Criar pool manualmente"
- "Criar grupos de volumes"

Como faço para desbloquear unidades?

Se você configurou o gerenciamento de chaves e, posteriormente, move unidades com segurança habilitada de um array de storage para outro, você deve reatribuir a chave de segurança ao novo array de storage para obter acesso aos dados criptografados nas unidades.

Saiba mais:

- "Desbloqueie unidades ao usar o gerenciamento interno de chaves"
- "Desbloqueie unidades ao usar o gerenciamento de chaves externas"

Informações relacionadas

Saiba mais sobre tarefas relacionadas à gestão de chaves:

- "Use certificados assinados por CA para autenticação com um servidor de gerenciamento de chaves"
- "Fazer backup da chave de segurança"

Conceitos

Como funciona o recurso Drive Security no SANtricity System Manager

Drive Security é um recurso do array de storage que fornece uma camada extra de segurança com unidades Full Disk Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS).

Quando esses discos são usados com o recurso Drive Security, eles exigem uma chave de segurança para acesso aos seus dados. Quando os discos são fisicamente removidos do array, eles não podem operar até serem instalados em outro array, momento em que ficarão em estado de Security Locked até que a chave de segurança correta seja fornecida.

Como implementar Drive Security

Para implementar a Segurança do Drive, execute as seguintes etapas.

1. Equipe seu array de storage com unidades compatíveis com segurança, sejam elas FDE drives ou FIPS drives. (Para volumes que exigem suporte a FIPS, use somente FIPS drives. Misturar FIPS drives e FDE drives em um grupo de volume ou pool fará com que todas as unidades sejam tratadas como FDE drives. Além disso, um FDE drive não pode ser adicionado ou usado como reserva em um grupo de volume ou pool composto apenas por FIPS drives.)
2. Crie uma chave de segurança, que é uma sequência de caracteres compartilhada pelo controlador e pelas unidades para acesso de leitura/gravação. Você pode criar uma chave interna a partir da memória persistente do controlador ou uma chave externa a partir 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 de unidade para pools e grupos de volume:
   - Crie um pool ou grupo de volume (procure por **Sim** na coluna **Secure-capable** na tabela Candidates).
   - Selecione um pool ou grupo de volume ao criar um novo volume (procure por **Sim** ao lado de **Compatível com segurança** na tabela de candidatos a pool e grupo de volume).

Como o Drive Security funciona no nível da unidade

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

O recurso Drive Security oferece uma camada extra de proteção para unidades com capacidade de segurança. Quando grupos de volumes ou pools nessas unidades são selecionados para 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 do array de storage

Com o recurso Drive Security, você cria uma chave de segurança que é compartilhada entre as unidades habilitadas para segurança e os controladores em um array de storage. Sempre que a energia das unidades for desligada e ligada, as unidades habilitadas para segurança mudam para o estado Security Locked até que o controlador aplique a chave de segurança.

Se uma unidade com segurança habilitada for removida do array de storage e reinstalada em um array de storage diferente, ela ficará em estado de Segurança Bloqueada. A unidade realocada procura a chave de segurança antes de tornar os dados acessíveis novamente. Para desbloquear os dados, você aplica a chave de segurança do array de storage de origem. Após um processo de desbloqueio bem-sucedido, a unidade realocada passará a usar a chave de segurança já armazenada no array de storage de destino, e o arquivo de chave de segurança importado não será mais necessário.

Para gerenciamento interno de chaves, a chave de segurança propriamente dita é armazenada no controlador em um local inacessível. Ela não está em formato legível por humanos, nem é acessível ao usuário.

Como o Drive Security funciona no nível de volume

Ao criar um pool ou grupo de volume a partir de unidades com recursos de segurança, você também pode habilitar Drive Security para esses pools ou grupos de volume. A opção Drive Security torna as unidades e os grupos de volume e pools associados secure-*enabled*.

Tenha em mente as seguintes diretrizes antes de criar grupos de volume e pools com segurança habilitada:

- Os grupos de volumes e pools devem ser compostos inteiramente por drives com capacidade de segurança. (Para volumes que exigem suporte a FIPS, use apenas drives FIPS. Misturar drives FIPS e FDE em um grupo de volume ou pool fará com que todos os drives sejam tratados como drives FDE. Além disso, um drive FDE não pode ser adicionado ou usado como reserva em um grupo de volume ou pool totalmente FIPS.)
- Os grupos de volume e os pools devem estar em um estado ideal.

Como funciona o gerenciamento de chaves de segurança no SANtricity System Manager

Ao implementar o recurso de Drive Security, as unidades com segurança habilitada (FIPS ou FDE) exigem uma chave de segurança para acesso aos dados. Uma chave de segurança é uma sequência de caracteres compartilhada entre esses tipos de unidades e os controladores em um array de storage.

Sempre que a alimentação das unidades é desligada e ligada, as unidades com segurança habilitada entram no estado Bloqueado por Segurança até que o controlador aplique a chave de segurança. Se uma unidade com segurança habilitada for removida do array de storage, os dados da unidade são bloqueados. Quando a unidade é reinstalada em um array de storage diferente, ela procura a chave de segurança antes de tornar os dados acessíveis novamente. Para desbloquear os dados, você deve aplicar a chave de segurança original.

Você pode criar e gerenciar chaves de segurança usando um dos seguintes métodos:

- Gerenciamento interno de chaves na memória persistente do controlador.
- Gerenciamento de chaves externas em um servidor de gerenciamento de chaves externo.

Gerenciamento interno de chaves

As chaves internas são mantidas e "ocultas" em um local inacessível na memória persistente do controlador. Para implementar o gerenciamento de chaves internas, execute as seguintes etapas:

1. Instale unidades com recursos de segurança no array de storage. Essas unidades podem ser unidades com criptografia de disco completa (FDE) ou unidades Federal Information Processing Standard (FIPS).
2. Certifique-se de que o recurso de Drive Security esteja ativado. Se necessário, entre em contato com seu fornecedor de storage para obter instruções sobre como ativar o recurso de Drive Security.
3. Crie uma chave de segurança interna, o que envolve definir um identificador e uma frase secreta. O identificador é uma sequência de caracteres associada à chave de segurança e é armazenado no controlador e em todas as unidades associadas à chave. A frase secreta é usada para criptografar a chave de segurança para fins de backup. Para criar uma chave interna, vá para **Settings › Sistema › Security key management › Create Internal Key**.

A chave de segurança é armazenada no controlador em um local oculto e inacessível. Você pode então criar grupos de volume ou pools com segurança habilitada, ou pode habilitar a segurança em grupos de volume existentes e pools existentes.

Gerenciamento de chaves externas

As chaves externas são mantidas em um servidor de gerenciamento de chaves separado, usando um Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP). Para implementar o gerenciamento de chaves externas, execute as seguintes etapas:

1. Instale unidades com recursos de segurança no array de storage. Essas unidades podem ser unidades com criptografia de disco completa (FDE) ou unidades Federal Information Processing Standard (FIPS).
2. Certifique-se de que o recurso de Drive Security esteja ativado. Se necessário, entre em contato com seu fornecedor de storage para obter instruções sobre como ativar o recurso de Drive Security.
3. Obtenha um arquivo de certificado de cliente assinado. Um certificado de cliente valida os controladores do array de storage, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP.
   a. Primeiro, você preenche e faz o download de uma Solicitação de Assinatura de Certificado (CSR) do cliente. Vá para **Settings › Certificates › Key Management › Complete CSR**.
   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.)
   c. Depois de obter um arquivo de certificado de cliente, copie esse arquivo para o host onde você está acessando System Manager.
   d. Alternativamente, você pode gerar uma solicitação de assinatura de certificado externamente usando um par de chaves privada e pública.
4. Recupere um arquivo de certificado do servidor de gerenciamento de chaves e copie esse arquivo para o host onde você está acessando System Manager. Um certificado de servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, para que o array de storage possa confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.
5. Crie uma chave externa, o que envolve definir o endereço IP do servidor de gerenciamento de chaves e o número da porta usado para comunicações KMIP. Durante esse processo, você também carrega arquivos de certificado. Para criar uma chave externa, acesse **Settings › Sistema › Security key management › Create External Key**.

O sistema se conecta ao servidor de gerenciamento de chaves com as credenciais que você inseriu. Você pode então criar grupos de volume ou pools com segurança habilitada, ou pode habilitar a segurança em grupos de volume e pools existentes.

Aprenda sobre a terminologia de segurança de unidades no software SANtricity

Saiba como os termos de segurança da unidade se aplicam ao seu array de storage.

Termo	Descrição
Recurso de segurança da unidade	Drive Security é um recurso do array de storage que fornece uma camada extra de segurança com unidades Full Disk Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS). Quando essas unidades são usadas com o recurso Drive Security, elas exigem uma chave de segurança para acesso aos seus dados. Quando as unidades são fisicamente removidas do array, elas não podem operar até serem instaladas em outro array; nesse momento, elas estarão em um estado Security Locked até que a chave de segurança correta seja fornecida.
Unidades FDE	Unidades com criptografia de disco completa (FDE) realizam criptografia na unidade de disco no nível do hardware. O disco rígido contém um chip ASIC que criptografa os dados durante as gravações e os descriptografa durante as leituras.
Unidades FIPS	Unidades FIPS utilizam o Federal Information Processing Standards (FIPS) 140-2 nível 2. Essencialmente, são unidades FDE que seguem os padrões do governo dos Estados Unidos para garantir algoritmos e métodos de criptografia robustos. Unidades FIPS possuem padrões de segurança mais elevados do que unidades FDE.
Cliente de gerenciamento	Um sistema local (computador, tablet, etc.) que inclui um navegador para acessar System Manager.
Frase secreta	A frase secreta é usada para criptografar a chave de segurança para fins de backup. A mesma frase secreta 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 cabeçote. Uma frase secreta pode ter entre 8 e 32 caracteres. A senha para Segurança da Unidade é independente da senha de Administrador do array de storage.
Unidades com capacidade de segurança	Unidades com capacidade de segurança podem ser unidades Full Disk Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS), que criptografam os dados durante as gravações e descriptografam os dados durante as leituras. Essas unidades são consideradas secure-*capable* porque podem ser usadas para segurança adicional usando o recurso Drive Security. Se o recurso Drive Security estiver habilitado para grupos de volume e pools usados com essas unidades, as unidades se tornam secure-*enabled*.

Termo	Descrição
Unidades com segurança ativada	Unidades com segurança habilitada são usadas com o recurso Drive Security. Quando você habilita o recurso Drive Security e, em seguida, aplica Drive Security a um pool ou grupo de volume em unidades secure-capable, as unidades passam a ser secure-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 foi fisicamente removida do array de storage.
Chave de segurança	Uma chave de segurança é uma sequência de caracteres compartilhada entre as unidades e controladores com segurança habilitada em um array de storage. Sempre que a energia das unidades é desligada e ligada, as unidades com segurança habilitada entram no estado Security Locked até que o controlador aplique a chave de segurança. Se uma unidade com segurança habilitada for removida do array de storage, os dados da unidade serão bloqueados. Quando a unidade for reinstalada em um array de storage diferente, ela buscará a chave de segurança antes de tornar os dados acessíveis novamente. Para desbloquear os dados, você deve aplicar a chave de segurança original. Você pode criar e gerenciar chaves de segurança usando um dos seguintes métodos: • Gerenciamento de chaves internas — criar e manter chaves de segurança na memória persistente do controlador. • Gerenciamento de chaves externas — criar e manter chaves de segurança em um servidor de gerenciamento de chaves externo.
Identificador da chave de segurança	O identificador da chave de segurança é uma sequência de caracteres 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

Crie uma chave de segurança interna no SANtricity System Manager

Para usar o recurso de Segurança de Unidade, você pode criar uma chave de segurança interna que é compartilhada pelos controladores e unidades com capacidade de segurança no array de storage. As chaves internas são mantidas na memória persistente do controlador.

Antes de começar

- Unidades com capacidade de segurança devem ser instaladas no array de storage. Essas unidades podem ser unidades com criptografia de disco completa (FDE) ou unidades com o padrão Federal Information Processing Standard (FIPS).
- O recurso Drive Security deve estar ativado. Caso contrário, uma caixa de diálogo Cannot Create Security Key será exibida durante esta tarefa. Se necessário, entre em contato com o fornecedor do seu array de storage para obter instruções sobre como ativar o recurso Drive Security.

Se ambas as unidades FDE e FIPS estiverem instaladas no array de storage, todas compartilharão a mesma chave de segurança.

Sobre esta tarefa

Nesta tarefa, você define um identificador e uma frase secreta para associar à chave de segurança interna.

> A senha para Segurança da Unidade é independente da senha de Administrador do array de storage.

Passos

1. Selecione o menu: configurações [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 é aberta.

3. Insira informações nos seguintes campos:

   - **Defina um identificador de chave de segurança** — Você pode aceitar o valor padrão (nome do array de storage e carimbo de data/hora, que é gerado pelo firmware do controlador) ou inserir seu próprio valor. Você pode inserir até 189 caracteres alfanuméricos, sem espaços, pontuação ou símbolos.

     > Caracteres adicionais são gerados automaticamente, anexados às duas extremidades da sequência que você inserir. Os caracteres gerados garantem que o identificador seja único.

   - **Definir uma frase secreta/Digitar novamente a frase secreta** — Digite e confirme uma frase secreta. O valor pode ter entre 8 e 32 caracteres e deve incluir cada um dos seguintes:
     - Uma letra maiúscula (ou mais). Lembre-se de que a senha diferencia maiúsculas de minúsculas.
     - Um número (um ou mais).
     - Um caractere não alfanumérico, como !, *, @ (um ou mais).

   > **Certifique-se de registrar suas anotações para uso posterior**. Se precisar mover uma unidade com segurança habilitada do array de storage, você deve saber o identificador e a pass phrase para desbloquear os dados da unidade.

4. Clique em **Create**.

   A chave de segurança é armazenada no controlador em um local inacessível. Junto com a chave real, há um arquivo de chave criptografado que é baixado do seu navegador.

   > O caminho para o arquivo baixado pode depender do local de download padrão do seu navegador.

5. Anote o identificador da chave, a frase secreta e o local do arquivo de chave baixado e, em seguida, clique em **Fechar**.

Resultados

Agora você pode criar grupos ou pools de volumes com segurança habilitada, ou pode habilitar a segurança em grupos de volumes e pools de volumes existentes.

Sempre que a alimentação das unidades é desligada e ligada novamente, todas as unidades com segurança habilitada passam para o estado Security Locked. Nesse 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 Security Locked impede o acesso não autorizado aos seus dados.

Depois que você terminar

Você deve validar a chave de segurança para garantir que o arquivo de chave não esteja corrompido.

Crie uma chave de segurança externa no SANtricity System Manager

Para usar o recurso de segurança de unidade com um servidor de gerenciamento de chaves, você deve criar uma chave externa que é compartilhada pelo servidor de gerenciamento de chaves e pelas unidades com capacidade de segurança no array de storage.

Antes de começar

- Unidades de armazenamento com capacidade de segurança devem ser instaladas no array. Essas unidades podem ser unidades com criptografia de disco completa (FDE) ou unidades Federal Information Processing Standard (FIPS).

  Se ambas as unidades FDE e FIPS estiverem instaladas no array de storage, todas compartilharão a mesma chave de segurança.

- O recurso Drive Security deve estar ativado. Caso contrário, uma caixa de diálogo Cannot Create Security Key será exibida durante esta tarefa. Se necessário, entre em contato com o fornecedor do seu array de storage para obter instruções sobre como ativar o recurso Drive Security.
- Você possui um arquivo de certificado de cliente assinado para os controladores do array de storage e copiou esse arquivo para o host onde está acessando System Manager. Um certificado de cliente valida os controladores do array de storage, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações do Key Management Interoperability Protocol (KMIP).
- Você deve obter um arquivo de certificado do servidor de gerenciamento de chaves e, em seguida, copiar esse arquivo para o host onde você está acessando System Manager. Um certificado de servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, então o array de storage pode confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.

  Para obter mais informações sobre o certificado do servidor, consulte a documentação do seu key management server.

Sobre esta tarefa

Nesta tarefa, você define o endereço IP do servidor de gerenciamento de chaves e o número da porta que ele utiliza e, em seguida, carrega certificados para o gerenciamento externo de chaves.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Criar chave externa**.

Se o gerenciamento de chaves interno estiver atualmente configurado, uma caixa de diálogo será aberta e solicitará que você confirme que deseja mudar para o gerenciamento de chaves externo.

A caixa de diálogo Criar chave de segurança externa é aberta.

3. Em **Conectar ao Key Server**, insira informações nos seguintes campos.
   - **Endereço do servidor de gerenciamento de chaves** — Insira o 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** — Insira o número da porta usado para comunicações KMIP. O número de porta mais comum usado para comunicações com o 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 primário não puder ser acessado. Certifique-se de que cada servidor de chaves tenha acesso ao mesmo banco de dados de chaves; caso contrário, o array exibirá erros e não poderá usar o servidor de backup.

     Apenas um servidor de chaves é usado por vez. Se o array de storage não conseguir alcançar o servidor de chaves primário, o array entrará em contato com o servidor de chaves de backup. Esteja ciente de que você deve manter a paridade entre ambos os servidores; a falha em fazê-lo pode resultar em erros.

   - **Selecionar certificado do cliente** — Clique no primeiro botão **Procurar** para selecionar o arquivo de certificado para os controladores do array de storage.
   - **Selecionar arquivo de chave privada** — Se necessário, clique no segundo botão **Procurar** para selecionar um arquivo de chave privada para os controladores do array de storage.
   - **Selecione o certificado do servidor de gerenciamento de chaves** — Clique no terceiro botão **Procurar** para selecionar o arquivo de certificado do servidor de gerenciamento de chaves. Você pode escolher um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.
4. Clique em **Next**.
5. Em **Criar/Fazer Backup da Chave**, você pode criar uma chave de backup para fins de segurança.
   - (Recomendado) Para criar uma chave de backup, mantenha a caixa de seleção marcada e, em seguida, insira e confirme uma senha. O valor pode ter entre 8 e 32 caracteres e deve incluir cada um dos seguintes:
     - Uma letra maiúscula (ou mais). Lembre-se de que a senha diferencia maiúsculas de minúsculas.
     - Um número (um ou mais).
     - Um caractere não alfanumérico, como !, *, @ (um ou mais).

     Certifique-se de anotar suas entradas para uso posterior. Se precisar mover uma unidade com segurança habilitada do array de storage, você precisa saber a senha para desbloquear os dados da unidade.

   +
   - Se não quiser criar uma chave de backup, desmarque a caixa de seleção.

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 caso elas sejam migradas para outro array de storage. Esta opção é o único método para criar uma chave de backup no System Manager.

6. Clique em **Concluir**.

   O sistema se conecta ao servidor de gerenciamento de chaves com as credenciais que você inseriu. Uma cópia da chave de segurança é então armazenada em seu sistema local.

   O caminho para o arquivo baixado pode depender do local de download padrão do seu navegador.

7. Anote sua frase secreta e o local do arquivo de chave baixado e, em seguida, clique em **Fechar**.

   A página exibe a seguinte mensagem com links adicionais para gerenciamento externo de chaves:

   ```
   Current key management method: External
   ```

8. Teste a conexão entre o array de storage e o servidor de gerenciamento de chaves selecionando **Test Communication**.

   Os resultados dos testes são exibidos na caixa de diálogo.

Resultados

Quando o gerenciamento de chaves externas está ativado, você pode criar grupos ou pools de volumes com segurança habilitada, ou pode habilitar a segurança em grupos e pools de volumes existentes.

Sempre que a alimentação das unidades é desligada e ligada novamente, todas as unidades com segurança habilitada passam para o estado Security Locked. Nesse 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 Security Locked impede o acesso não autorizado aos seus dados.

Depois que você terminar

Você deve validar a chave de segurança para garantir que o arquivo de chave não esteja corrompido.

Gerenciar chaves de segurança

Alterar uma chave de segurança no SANtricity System Manager

A qualquer momento, você pode substituir uma chave de segurança por uma nova. Você pode precisar trocar uma chave de segurança em casos de potencial violação de segurança na sua empresa e deseja garantir que pessoas não autorizadas não possam acessar os dados das unidades.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Alterar chave**.

A caixa de diálogo Alterar chave de segurança é aberta.

3. Insira informações nos campos a seguir.
   - **Defina um identificador de chave de segurança** — (Apenas para chaves de segurança internas.) Aceite o valor padrão (nome do array de storage e carimbo de data/hora, que é gerado pelo firmware do controlador) ou insira seu próprio valor. Você pode inserir até 189 caracteres alfanuméricos, sem espaços, pontuação ou símbolos.

     Caracteres adicionais são gerados automaticamente e anexados às duas extremidades da sequência de caracteres que você inserir. Os caracteres gerados ajudam a garantir que o identificador seja único.

   - **Definir uma frase secreta/Inserir frase secreta novamente** — Em cada um destes campos, insira sua frase secreta. O valor pode ter entre 8 e 32 caracteres e deve incluir cada um dos seguintes:
     - Uma letra maiúscula (ou mais). Lembre-se de que a senha diferencia maiúsculas de minúsculas.
     - Um número (um ou mais).
     - Um caractere não alfanumérico, como !, *, @ (um ou mais).
4. Para chaves de segurança externas, se você quiser excluir a chave de segurança antiga quando a nova for criada, selecione a caixa de seleção "Excluir chave de segurança atual…" na parte inferior da caixa de diálogo.

   Certifique-se de registrar suas entradas para uso posterior — Se você precisar mover uma unidade com segurança habilitada do array de storage, você deve saber o identificador e a frase secreta para desbloquear os dados da unidade.

5. Clique em **Change**.

   A nova chave de segurança sobrescreve 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. Anote o identificador da chave, a frase secreta e o local do arquivo de chave baixado e, em seguida, clique em **Fechar**.

Depois que você terminar

Você deve validar a chave de segurança para garantir que o arquivo de chave não esteja corrompido.

Altere do gerenciamento de chaves externas para internas no SANtricity System Manager

Você pode alterar o método de gerenciamento da Segurança da Unidade de um servidor de chaves externo para o método interno usado pelo array de storage. A chave de segurança previamente definida para o gerenciamento de chaves externas passa a ser usada para o gerenciamento de chaves internas.

Sobre esta tarefa

Nesta tarefa, você desativa o gerenciamento de chaves externas e baixa uma nova cópia de backup para o seu host local. A chave existente ainda é usada para Drive Security, mas será gerenciada internamente no array de storage.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Desativar External Key Management**.

   A caixa de diálogo Desativar gerenciamento de chaves externas é aberta.

3. Em **Definir uma frase secreta/Reinserir frase secreta**, insira e confirme uma frase secreta para o backup da chave. O valor pode ter entre 8 e 32 caracteres e deve incluir cada um dos seguintes:
   - Uma letra maiúscula (ou mais). Lembre-se de que a senha diferencia maiúsculas de minúsculas.
   - Um número (um ou mais).
   - Um caractere não alfanumérico, como !, *, @ (um ou mais).

   Certifique-se de registrar suas anotações para uso posterior. Se precisar mover uma unidade com segurança habilitada do array de storage, você deverá saber o identificador e a frase secreta para desbloquear os dados da unidade.

4. Clique em **Desativar**.

   A chave de backup é baixada para o seu host local.

5. Anote o identificador da chave, a frase secreta e o local do arquivo de chave baixado e, em seguida, clique em **Fechar**.

Resultados

A segurança da unidade agora é gerenciada internamente pelo array de storage.

Depois que você terminar

Você deve validar a chave de segurança para garantir que o arquivo de chave não esteja corrompido.

Editar as configurações do servidor de gerenciamento de chaves no SANtricity System Manager

Se você configurou o gerenciamento de chaves externo, pode visualizar e editar as configurações do servidor de gerenciamento de chaves a qualquer momento.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Visualizar/Editar configurações do servidor de gerenciamento de chaves**.
3. Edite as informações nos seguintes campos:
   - **Endereço do servidor de gerenciamento de chaves** — Insira o 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** — Insira o número da porta usado para as comunicações do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP).

     Opcional: você pode incluir outro servidor de chaves clicando em **Add Key Server**.

4. Clique em **Salvar**.

Faça backup das chaves de segurança no SANtricity System Manager

Após 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 que você criou anteriormente. Durante este procedimento, você cria uma nova frase secreta para o backup. Essa frase secreta não precisa ser igual à frase secreta usada quando a chave original foi criada ou alterada pela última vez. A frase secreta se aplica somente ao backup que você está criando.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Back Up Key**.

   A caixa de diálogo Back Up Security Key é aberta.

3. Nos campos **Definir uma frase secreta/Redigitar frase secreta**, insira e confirme uma frase secreta para este backup.

   O valor pode ter entre 8 e 32 caracteres e deve incluir cada um dos seguintes:

   - Uma letra maiúscula (uma ou mais)
   - Um número (um ou mais)
   - Um caractere não alfanumérico, como !, *, @ (um ou mais)

   > **Anote sua entrada para uso posterior**. Você precisa da senha para acessar o backup desta chave de segurança.

4. Clique em **Back Up**.

   Um backup da chave de segurança é baixado para o seu host local e, em seguida, a caixa de diálogo **Confirmar/Registrar Backup da Chave de Segurança** é aberta.

   > O caminho para o arquivo de chave de segurança baixado pode depender do local de download padrão do seu navegador.

5. Anote sua frase secreta em um local seguro e clique em **Fechar**.

Depois que você terminar

Você deve validar a chave de segurança de backup.

Validar chave de segurança no SANtricity System Manager

Você pode validar a chave de segurança para garantir que ela não foi corrompida e para verificar se você possui uma frase secreta correta.

Sobre esta tarefa

Esta tarefa descreve como validar a chave de segurança que você criou anteriormente. Este é um passo importante para garantir que o arquivo da chave não esteja corrompido e que a senha esteja correta, o que assegura que você poderá acessar os dados da unidade posteriormente, caso mova uma unidade com

segurança habilitada de um array de storage para outro.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Validar chave**.

   A caixa de diálogo Validate Security Key é aberta.

3. Clique em **Procurar**, e selecione o arquivo de chave (por exemplo, `drivesecurity.slk`).
4. Digite a frase secreta associada à chave que você selecionou.

   Ao selecionar um arquivo de chave válido e uma senha válida, o botão **Validar** ficará disponível.

5. Clique em **Validar**.

   Os resultados da validação são exibidos na caixa de diálogo.

6. Se os resultados mostrarem "A chave de segurança foi validada com sucesso", clique em **Fechar**. Se uma mensagem de erro for exibida, siga as instruções sugeridas na caixa de diálogo.

Desbloquear unidades ao usar o gerenciamento de chaves internas no SANtricity System Manager

Se você configurou o gerenciamento de chaves internas e, posteriormente, moveu unidades com segurança habilitada de um array de storage para outro, você deve reatribuir a chave de segurança ao novo array de storage para obter acesso aos dados criptografados nas unidades.

Antes de começar

- No array de origem (o array onde você está removendo as unidades), você exportou os grupos de volumes e removeu as unidades. No array de destino, você reinstalou 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 volume para um array de storage diferente.

  Instruções detalhadas para migrar um grupo de volume são fornecidas no "Base 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 Drive Security deve estar ativado. Caso contrário, uma caixa de diálogo Cannot Create Security Key será exibida durante esta tarefa. Se necessário, entre em contato com o fornecedor do seu array de storage para obter instruções sobre como ativar o recurso Drive Security.
- Você deve saber a chave de segurança associada às unidades que deseja desbloquear.
- O arquivo de chave de segurança está disponível no cliente de gerenciamento (o sistema com navegador usado para acessar o System Manager). Se você estiver movendo as unidades para um array de storage gerenciado por um sistema diferente, será necessário mover o arquivo de chave de segurança para esse cliente de gerenciamento.

Sobre esta tarefa

Ao usar o gerenciamento de chaves internas, a chave de segurança é armazenada localmente no array de storage. Uma chave de segurança é uma sequência de caracteres compartilhada pelo controlador e pelas

unidades para acesso de leitura/gravação. Quando as unidades são fisicamente removidas do array e instaladas em outro, 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 a partir de um servidor de gerenciamento de chaves. Este tópico descreve o desbloqueio de dados quando o gerenciamento de chaves *interno* é utilizado. Se você utilizou o gerenciamento de chaves *externo*, consulte "Desbloqueie unidades ao usar o gerenciamento de chaves externas". Se você estiver realizando uma atualização do controlador e substituindo todos os controladores pelo hardware mais recente, você deve seguir etapas diferentes, conforme descrito no centro de documentação E-Series e SANtricity, em "Desbloquear unidades".

Após reinstalar unidades com segurança habilitada em outro array, esse array detecta as unidades e exibe a condição "Requer Atenção", juntamente com o status "Chave de Segurança Necessária". Para desbloquear os dados da unidade, você seleciona o arquivo da chave de segurança e insere a frase secreta da chave. (Essa frase secreta não é a mesma que a senha de administrador do array de storage.)

Se outras unidades com recursos de segurança habilitados estiverem instaladas no novo array de storage, elas poderão usar uma chave de segurança diferente daquela 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 for concluído com sucesso, as unidades recém-instaladas serão reassociadas à chave de segurança do array de storage de destino.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Desbloquear unidades seguras**.

   A caixa de diálogo Desbloquear unidades seguras é aberta. Todas as unidades que exigem uma chave de segurança são exibidas na tabela.

3. **Opcional:** passe o cursor do mouse sobre o número da unidade para ver a localização da unidade (número da prateleira e número da baia).
4. Clique em **Procurar** e, em seguida, selecione o arquivo de chave de segurança que corresponde à unidade que você deseja desbloquear.

   O arquivo de chave que você selecionou aparece na caixa de diálogo.

5. Digite a frase secreta associada a este arquivo de chave.

   Os caracteres que você inserir são mascarados.

6. Clique em **Unlock**.

   Se a operação de desbloqueio for bem-sucedida, a caixa de diálogo exibirá: "As unidades seguras associadas foram desbloqueadas."

Resultados

Quando todas as unidades são bloqueadas e depois desbloqueadas, cada controlador no array de storage será reinicializado. No entanto, se já houver algumas unidades desbloqueadas no array de storage de destino, os controladores não serão reinicializados.

Depois que você 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 volume para um array de storage diferente.

Instruções detalhadas para migrar um grupo de volume são fornecidas em "Base de Conhecimento da NetApp".

Desbloquear unidades ao usar o gerenciamento de chaves externas no SANtricity System Manager

Se você configurou o gerenciamento de chaves externas e, posteriormente, moveu unidades com segurança habilitada de um array de storage para outro, você deve reatribuir a chave de segurança ao novo array de storage para obter acesso aos dados criptografados nas unidades.

Antes de começar

- No array de origem (o array onde você está removendo as unidades), você exportou os grupos de volumes e removeu as unidades. No array de destino, você reinstalou 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 volume para um array de storage diferente.

  Instruções detalhadas para migrar um grupo de volume são fornecidas no "Base 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 Drive Security deve estar ativado. Caso contrário, uma caixa de diálogo Cannot Create Security Key será exibida durante esta tarefa. Se necessário, entre em contato com o fornecedor do seu array de storage para obter instruções sobre como ativar o recurso Drive Security.
- Você deve saber o endereço IP e o número da porta do servidor de gerenciamento de chaves.
- Você possui um arquivo de certificado de cliente assinado para os controladores do array de storage e copiou esse arquivo para o host onde está acessando System Manager. Um certificado de cliente valida os controladores do array de storage, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações do Key Management Interoperability Protocol (KMIP).
- Você deve obter um arquivo de certificado do servidor de gerenciamento de chaves e, em seguida, copiar esse arquivo para o host onde você está acessando System Manager. Um certificado de servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, então o array de storage pode confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.

  Para obter mais informações sobre o certificado do servidor, consulte a documentação do seu key management server.

Sobre esta tarefa

Ao usar 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 sequência de caracteres compartilhada pelo controlador e pelas unidades para acesso de leitura/gravação. Quando as unidades são fisicamente removidas do array e instaladas em outro, 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 a partir de um servidor de gerenciamento de chaves. Este tópico descreve o desbloqueio de dados quando o gerenciamento de chaves *externo* é utilizado. Se você utilizou o gerenciamento de chaves *interno*, consulte "Desbloqueie unidades ao usar o gerenciamento interno de chaves". Se você estiver realizando uma atualização do controlador e substituindo todos os controladores pelo hardware mais recente, deve seguir etapas diferentes, conforme descrito na E-Series e na Central de Documentação do SANtricity, em "Desbloquear unidades".

Após reinstalar unidades com segurança habilitada em outro array, esse array detecta as unidades e exibe uma condição "Requer Atenção" juntamente com um status de "Chave de Segurança Necessária". Para desbloquear os dados da unidade, você importa o arquivo da chave de segurança e insere a frase secreta da chave. (Essa frase secreta não é a mesma que a senha de administrador do array de storage.) Durante esse processo, você configura o array de storage para usar um servidor externo de gerenciamento de chaves e então a chave de segurança ficará acessível. Você é obrigado a fornecer as informações de contato do servidor para que o array de storage possa se conectar e recuperar a chave de segurança.

Se outras unidades com recursos de segurança habilitados estiverem instaladas no novo array de storage, elas poderão usar uma chave de segurança diferente daquela 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 for concluído com sucesso, as unidades recém-instaladas serão reassociadas à chave de segurança do array de storage de destino.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Criar chave externa**.
3. Conclua o assistente com as informações de conexão pré-requisito e certificados.
4. Clique em **Test Communication** para garantir o acesso ao servidor externo de gerenciamento de chaves.
5. Selecione **Unlock Secure Drives**.

   A caixa de diálogo Desbloquear unidades seguras é aberta. Todas as unidades que exigem uma chave de segurança são exibidas na tabela.

6. **Opcional:** passe o cursor do mouse sobre o número da unidade para ver a localização da unidade (número da prateleira e número da baia).
7. Clique em **Procurar** e, em seguida, selecione o arquivo de chave de segurança que corresponde à unidade que você deseja desbloquear.

   O arquivo de chave que você selecionou aparece na caixa de diálogo.

8. Digite a frase secreta associada a este arquivo de chave.

   Os caracteres que você inserir são mascarados.

9. Clique em **Unlock**.

   Se a operação de desbloqueio for bem-sucedida, a caixa de diálogo exibirá: "As unidades seguras associadas foram desbloqueadas."

Resultados

Quando todas as unidades são bloqueadas e depois desbloqueadas, cada controlador no array de storage será reinicializado. No entanto, se já houver algumas unidades desbloqueadas no array de storage de destino,

os controladores não serão reinicializados.

Depois que você 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 volume para um array de storage diferente.

Instruções detalhadas para migrar um grupo de volume são fornecidas em "Base de Conhecimento da NetApp".

Perguntas frequentes sobre segurança de storage drive para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

O que preciso saber antes de criar uma chave de segurança?

Uma chave de segurança é compartilhada entre controladores e unidades com segurança habilitada dentro de um array de storage. Se uma unidade com segurança habilitada for removida do array de storage, a chave de segurança protege os dados contra acesso não autorizado.

Você pode criar e gerenciar chaves de segurança usando um dos seguintes métodos:

- Gerenciamento interno de chaves na memória persistente do controlador.
- Gerenciamento de chaves externas em um servidor de gerenciamento de chaves externo.

Gerenciamento interno de chaves

As chaves internas são mantidas e “hidden” em um local inacessível na memória persistente do controlador. Antes de criar uma chave de segurança interna, você deve fazer o seguinte:

1. Instale unidades com recursos de segurança no array de storage. Essas unidades podem ser unidades com criptografia de disco completa (FDE) ou unidades Federal Information Processing Standard (FIPS).
2. Certifique-se de que o recurso de Drive Security esteja ativado. Se necessário, entre em contato com seu fornecedor de storage para obter instruções sobre como ativar o recurso de Drive Security.

Em seguida, você pode criar uma chave de segurança interna, o que envolve definir um identificador e uma frase secreta. O identificador é uma string que está associada à chave de segurança e é armazenado no controlador e em todas as unidades associadas à chave. A frase secreta é usada para criptografar a chave de segurança para fins de backup. Quando você termina, a chave de segurança é armazenada no controlador em um local inacessível. Você pode então criar grupos de volumes ou pools com segurança habilitada, ou pode 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 Key Management Interoperability Protocol (KMIP). Antes de criar uma chave de segurança externa, você deve fazer o seguinte:

1. Instale unidades com recursos de segurança no array de storage. Essas unidades podem ser unidades com criptografia de disco completa (FDE) ou unidades Federal Information Processing Standard (FIPS).
2. Certifique-se de que o recurso de Drive Security esteja ativado. Se necessário, entre em contato com seu fornecedor de storage para obter instruções sobre como ativar o recurso de Drive Security.
3. Obtenha um arquivo de certificado de cliente assinado. Um certificado de cliente valida os controladores do array de storage, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP.
   a. Primeiro, você preenche e faz o download de uma Solicitação de Assinatura de Certificado (CSR) do cliente. Vá para **Settings › Certificates › Key Management › Complete CSR**.
   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 obter um arquivo de certificado de cliente, copie esse arquivo para o host onde você está acessando 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 System Manager. Um certificado de servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, para que o array de storage possa confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.

Em seguida, você pode criar uma chave externa, o que envolve definir o endereço IP do servidor de gerenciamento de chaves e o número da porta usado para as comunicações KMIP. Durante esse processo, você também carrega os arquivos de certificado. Ao concluir, o sistema se conecta ao servidor de gerenciamento de chaves com as credenciais inseridas. Você pode então criar grupos de volumes ou pools com segurança habilitada, ou pode habilitar a segurança em grupos de volumes e pools existentes.

Por que preciso definir uma frase secreta?

A senha é usada para criptografar e descriptografar o arquivo de chave de segurança armazenado no cliente de gerenciamento local. Sem a senha, a chave de segurança não pode ser descriptografada e usada para desbloquear dados de uma unidade com segurança habilitada, caso ela seja reinstalada em outro array de storage.

Por que é importante registrar as informações da chave de segurança?

Se você perder as informações da chave de segurança e não tiver um backup, poderá perder dados ao realocar unidades com segurança habilitada ou ao atualizar um controlador. Você precisa da chave de segurança para desbloquear dados nas unidades.

Certifique-se de registrar o identificador da chave de segurança, a frase secreta associada e o local no host local onde o arquivo da chave de segurança foi salvo.

O que preciso saber antes de fazer backup de uma chave de segurança?

Se a sua chave de segurança original for corrompida e você não tiver um backup, você perderá o acesso aos dados nas unidades caso elas sejam migradas de um array de storage para outro.

Antes de fazer backup de uma chave de segurança, tenha em mente estas diretrizes:

- Certifique-se de conhecer o identificador da chave de segurança e a frase secreta do arquivo de chave original.

Somente as chaves internas usam identificadores. Ao criar o identificador, caracteres adicionais foram gerados automaticamente e anexados às duas extremidades da string do identificador. Os caracteres gerados garantem que o identificador seja único.

- Você cria uma nova frase secreta para o backup. Essa frase secreta não precisa ser igual à frase secreta usada quando a chave original foi criada ou alterada pela última vez. A frase secreta se aplica somente ao backup que você está criando.

A frase secreta para Drive Security não deve ser confundida com a senha de administrador do array de storage. A frase secreta para Drive Security protege os backups de uma chave de segurança. A senha de administrador protege todo o array de storage 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 registrar onde as informações da sua chave de segurança estão armazenadas.

O que preciso saber antes de desbloquear unidades seguras?

Para desbloquear os dados de uma unidade com segurança ativada, você deve importar sua chave de segurança.

Antes de desbloquear unidades com segurança ativada, tenha em mente as seguintes diretrizes:

- O array de storage já deve possuir uma chave de segurança. As unidades migradas serão reconfiguradas com uma nova chave para o array de storage de destino.
- Para as unidades que você está migrando, você deve saber o identificador da chave de segurança e a frase secreta que corresponde ao arquivo da chave de segurança.
- O arquivo de chave de segurança deve estar disponível no cliente de gerenciamento (o sistema com navegador usado para acessar System Manager).
- Se você estiver redefinindo uma unidade NVMe bloqueada, precisará inserir o ID de segurança da unidade. Para localizar o ID de segurança, você deve remover fisicamente a unidade e encontrar a sequência PSID (máximo de 32 caracteres) na etiqueta da unidade. Certifique-se de que a unidade esteja reinstalada antes de iniciar a operação.

O que é acessibilidade de leitura/gravação?

A janela Configurações da unidade inclui informações sobre os atributos de segurança da unidade. "Leitura/gravação acessível" é um dos atributos que indica se os dados de uma unidade foram bloqueados.

Para visualizar os atributos de segurança da unidade, acesse a página Hardware. Selecione uma unidade, clique em **Exibir configurações** e, em seguida, clique em **Mostrar mais configurações**. Na parte inferior da página, o valor do atributo Leitura/Gravação acessível é **Sim** quando a unidade está desbloqueada. O valor do atributo Leitura/Gravação acessível é **Não, chave de segurança inválida** quando a unidade está bloqueada. Você pode desbloquear uma unidade segura importando uma chave de segurança (vá para **Configurações › Sistema › Desbloquear unidades seguras**).

O que preciso saber sobre validar a chave de segurança?

Após criar uma chave de segurança, você deve validar o arquivo da chave para garantir que não esteja corrompido.

Se a validação falhar, faça o seguinte:

- Se o identificador da chave de segurança não corresponder ao identificador no controlador, localize o arquivo de chave de segurança correto e tente a validação novamente.
- Se o controlador não conseguir descriptografar a chave de segurança para validação, você pode ter digitado a frase secreta incorretamente. Verifique a frase secreta, digite-a novamente se necessário e tente a validação novamente. Se a mensagem de erro aparecer novamente, selecione um backup do arquivo de chave (se disponível) e tente a validação novamente.
- 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 chave de segurança interna e gerenciamento externo de chave de segurança?

Ao implementar o recurso de Segurança de Unidade, você pode usar uma chave de segurança interna ou externa para bloquear os dados quando uma unidade com segurança habilitada for removida do array de storage.

Uma chave de segurança é uma sequência de caracteres, que é compartilhada entre as unidades com segurança habilitada e os controladores em um array de storage. 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 Key Management Interoperability Protocol (KMIP).

Gerenciamento de acesso

Saiba mais sobre controle de acesso no SANtricity System Manager

O Access Management é um método para estabelecer autenticação de usuário no SANtricity System Manager.

Quais métodos de autenticação estão disponíveis?

Os métodos de autenticação incluem RBAC (controle de acesso baseado em funções), Serviços de Diretório e Security Assertion Markup Language (SAML):

- **RBAC/Funções de usuário locais** — A autenticação é gerenciada por meio de recursos RBAC implementados no array de storage. Funções de usuário locais 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 Directory Services, como o Active Directory da Microsoft.
- **SAML** — A autenticação é gerenciada por meio de um Identity Provider (IdP) usando SAML 2.0.

Saiba mais:

- "Como funciona o gerenciamento de acessos"
- "Terminologia de gerenciamento de acesso"
- "Permissões para funções mapeadas"
- "Funções de usuário local"
- "Serviços de diretório"
- "SAML"

Como faço para configurar autenticação?

O array de storage está pré-configurado para usar funções de usuário locais, que são uma implementação dos recursos RBAC. Se você quiser configurar um método diferente, acesse o menu: configurações [Gerenciamento de acesso].

Saiba mais:

- "Adicionar um servidor de diretório LDAP"
- "Configurar SAML"

Informações relacionadas

Saiba mais sobre tarefas relacionadas ao controle de acesso:

- "Alterar senhas"
- "Visualizar atividade do log de auditoria"
- "Configurar servidor syslog para logs de auditoria"

Conceitos

Como o controle de acesso funciona no SANtricity System Manager

O Access Management é um método para estabelecer autenticação de usuário no SANtricity System Manager.

A configuração e autenticação do usuário funcionam da seguinte maneira:

1. Um administrador faz login no System Manager com um perfil de usuário que inclui permissões de Security Admin.

   > No primeiro acesso, o nome de usuário `admin` é exibido automaticamente e não pode ser alterado. O `admin` usuário tem acesso total a todas as funções do sistema.

2. O administrador navega até Gerenciamento de Acesso na interface de usuário. O array de storage está pré-configurado para usar funções de usuário locais, que são uma implementação das capacidades de controle de acesso baseado em funções (RBAC).
3. O administrador configura um ou mais dos seguintes métodos de autenticação:
   - **Funções de usuário locais** — A autenticação é gerenciada por meio de recursos RBAC implementados no array de storage. As funções de usuário locais incluem perfis de usuário predefinidos e funções com permissões de acesso específicas. Os administradores podem usar essas funções de usuário locais como o único método de autenticação ou usá-las em combinação com um serviço de diretório. Nenhuma configuração é necessária, além da definição de senhas para os usuários.
   - **Serviços de diretório** — A autenticação é gerenciada por meio de um servidor LDAP (Lightweight Directory Access Protocol) e um serviço de diretório, como o Active Directory da Microsoft. Um administrador se conecta ao servidor LDAP e, em seguida, mapeia os usuários LDAP para as funções de usuário locais incorporadas no array de storage.
   - **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 comunicação entre o sistema

IdP e o array de storage e, em seguida, mapeia os usuários do IdP para as funções de usuário locais incorporadas no array de storage.

4. O administrador fornece aos usuários as credenciais de login para System Manager.
5. Os usuários fazem login no sistema inserindo suas credenciais.

> Se a autenticação for gerenciada com SAML e um SSO (single sign-on), o sistema poderá ignorar a caixa de diálogo de login do System Manager.

Durante o login, o sistema executa as seguintes tarefas em segundo plano:

- Autentica o nome de usuário e a senha na conta do usuário.
- Determina as permissões do usuário com base nas funções atribuídas.
- Fornece ao usuário acesso a tarefas na interface de usuário.
- Exibe o nome de usuário no canto superior direito da interface.

Tarefas disponíveis no System Manager

O acesso às tarefas depende das funções atribuídas ao usuário, que incluem o seguinte:

- **Administrador de armazenamento** — acesso completo de leitura/gravação aos objetos de armazenamento (por exemplo, volumes e conjuntos de discos), mas sem acesso à configuração de segurança.
- **Administrador de segurança** — Acesso à configuração de segurança no Gerenciamento de Acesso, gerenciamento de certificados, gerenciamento do log de auditoria e a capacidade de ativar ou desativar a interface de gerenciamento legada (SYMbol).
- **Administrador de suporte** — Acesso a todos os recursos de hardware no array de storage, dados de falhas, 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 storage, mas sem acesso à configuração de segurança.

Uma tarefa indisponível aparece acinzentada ou não é exibida na interface de usuário. Por exemplo, um usuário com a função Monitor pode visualizar todas as informações sobre volumes, mas não pode acessar funções para modificar esse volume. As guias para recursos como **Copy Services** e **Add to Workload** ficarão acinzentadas; somente **View/Edit Settings** estará disponível.

Limitações no Unified Manager e Storage Manager

Se o SAML estiver configurado para um array de storage, os usuários não poderão descobrir ou gerenciar storage desse array a partir do Unified Manager ou das interfaces legadas do Storage Manager.

Quando as funções de usuário local e os serviços de diretório estão configurados, os usuários devem inserir credenciais antes de executar qualquer uma das seguintes funções:

- Renomeando o array de storage
- Atualizando firmware do controlador
- Carregando uma configuração de array de storage
- Executando um script
- Tentativa de executar uma operação ativa quando uma sessão não utilizada expirou

Aprenda sobre a terminologia de gerenciamento de acesso no software SANtricity

Saiba como os termos de Access Management se aplicam ao seu array de storage.

Termo	Descrição
Token de acesso	Os tokens de acesso são usados para autenticar com a API REST ou interface de linha de comando (CLI) em vez 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.
Active Directory	Active Directory (AD) é um serviço de diretório da Microsoft que utiliza LDAP para redes de domínio Windows.
Vinculação	As operações de bind são usadas para autenticar clientes no servidor de diretório. Bind geralmente requer credenciais de conta e senha, mas alguns servidores permitem operações de bind anônimas.
CA	Uma autoridade certificadora (CA) é uma entidade confiável que emite documentos eletrônicos, chamados certificados digitais, para segurança na Internet. Esses certificados identificam os proprietários de sites, permitindo conexões seguras entre clientes e servidores.
Certificado	Um certificado identifica o proprietário de um site para fins de segurança, o que impede que invasores se façam passar pelo 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 determinar se esse usuário foi autenticado com sucesso. O IdP pode ser configurado para fornecer autenticação multifator e usar qualquer banco de dados de usuários, como Active Directory. Sua equipe de segurança é responsável por manter o IdP.
LDAP	O Lightweight Directory Access Protocol (LDAP) é um protocolo de aplicação para acessar e manter serviços de informações de diretório distribuídos. Este protocolo permite que diversas aplicações e serviços se conectem ao servidor LDAP para validar usuários.
RBAC	Controle de acesso baseado em funções (RBAC) é um método de regular o acesso a recursos de rede ou computador com base nas funções de usuários individuais. Os controles RBAC são aplicados no array de storage e incluem funções predefinidas.
SAML	A Security Assertion Markup Language (SAML) é um padrão baseado em XML para autenticação e autorização entre duas entidades. O SAML permite autenticação multifator, na qual os usuários devem fornecer dois ou mais itens para comprovar sua identidade (por exemplo, uma senha e impressão digital). O recurso SAML incorporado ao array de storage é compatível com SAML2.0 para asserção de identidade, autenticação e autorização.

Termo	Descrição
SP	Um Service Provider (SP) é um sistema que controla a autenticação e o acesso do usuário. Quando o Access Management é configurado com SAML, o array de storage atua como o Service Provider para solicitar autenticação do Identity Provider.
SSO	Single sign-on (SSO) é um serviço de autenticação que permite que um único conjunto de credenciais de login acesse vários aplicativos.

Saiba sobre permissões para funções mapeadas no SANtricity System Manager

Os recursos de RBAC (controle de acesso baseado em funções) aplicados no array de storage incluem perfis de usuário predefinidos com uma ou mais funções atribuídas. Cada função inclui permissões para acessar tarefas no SANtricity System Manager.

Os perfis de usuário e as funções mapeadas podem ser acessados no menu:Configurações [Gerenciamento de acesso > Funções de usuário local] na interface de usuário de qualquer System Manager.

As funções conferem ao usuário acesso às tarefas, conforme a seguir:

- **Administrador de armazenamento** — acesso completo de leitura/gravação aos objetos de armazenamento (por exemplo, volumes e conjuntos de discos), mas sem acesso à configuração de segurança.
- **Administrador de segurança** — Acesso à configuração de segurança no Gerenciamento de Acesso, gerenciamento de certificados, gerenciamento do log de auditoria e a capacidade de ativar ou desativar a interface de gerenciamento legada (SYMbol).
- **Administrador de suporte** — Acesso a todos os recursos de hardware no array de storage, dados de falhas, 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 storage, mas sem acesso à configuração de segurança.

Se um usuário não tiver permissões para uma determinada tarefa, essa tarefa ficará acinzentada ou não será exibida na interface de usuário.

Configurar o controle de acesso com funções de usuário locais no SANtricity System Manager

Para o gerenciamento de acesso, os administradores podem usar os recursos de RBAC (controle de acesso baseado em funções) aplicados no array de storage. Esses recursos são chamados de "funções de usuário locais".

Fluxo de trabalho de configuração

As funções de usuário locais são pré-configuradas para o array de storage. Para usar funções de usuário locais 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 Security Admin.

O `admin` usuário 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 acessam o sistema com as credenciais que lhes foram atribuídas.

Gerenciamento

Ao usar apenas funções de usuário locais 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 senha.

Configurar o controle de acesso com serviços de diretório no SANtricity System Manager

Para o gerenciamento de acesso, os administradores podem usar um servidor LDAP (Lightweight Directory Access Protocol) e um serviço de diretório, como o Active Directory da Microsoft.

Fluxo de trabalho de configuração

Se um servidor LDAP e um serviço de diretório forem 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 Security Admin.

   O `admin` usuário tem acesso total a todas as funções do sistema.

2. O administrador insere as configurações do servidor LDAP. As configurações incluem o nome de domínio, a URL e as informações da conta Bind.
3. Se o servidor LDAP usar um protocolo seguro (LDAPS), o administrador carrega uma cadeia de certificados da Autoridade Certificadora (CA) para autenticação entre o servidor LDAP e o array de storage.
4. Após a conexão com o servidor ser estabelecida, o administrador mapeia os grupos de usuários para as funções do array de storage. Essas funções são predefinidas e não podem ser modificadas.
5. O administrador testa a conexão entre o servidor LDAP e o array de storage.
6. Os usuários acessam o 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:

- Adicionar um servidor de diretório.
- Editar configurações do servidor de diretório.

- Mapear usuários LDAP para funções de usuário locais.
- Remova um servidor de diretório.

Configurar o controle de acesso com SAML no SANtricity System Manager

Para o gerenciamento de acesso, os administradores podem usar os recursos do 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 Security Admin.

   O `admin` usuário tem acesso total a todas as funções no System Manager.

2. O administrador vai para a guia **SAML** em Gerenciamento de Acesso.
3. Um administrador configura a comunicação com o Identity Provider (IdP). Um IdP é um sistema externo usado para solicitar credenciais de um usuário e determinar se o usuário foi autenticado com sucesso. Para configurar a comunicação com o array de storage, o administrador baixa o arquivo de metadados do IdP do sistema IdP e, em seguida, usa o System Manager para carregar o arquivo no array de storage.
4. Um administrador estabelece uma relação de confiança entre o Service Provider e o IdP. Um Service Provider controla a autorização do usuário; neste caso, o controlador no array de storage atua como o Service Provider. Para configurar as comunicações, o administrador usa System Manager para exportar um arquivo de metadados do Service Provider para cada controlador. A partir do sistema IdP, o administrador então importa esses arquivos de metadados para o IdP.

   Os administradores também devem garantir que o IdP suporte a capacidade de retornar um Name ID na autenticação.

5. O administrador mapeia as funções do array de storage para os atributos de usuário definidos no IdP. Para isso, o administrador usa System Manager para criar os mapeamentos.
6. O administrador testa o login SSO no URL do IdP. Este teste garante que o array de storage e o IdP possam se comunicar.

   Uma vez que o SAML esteja ativado, você *não* pode desativá-lo através da interface de usuário, nem editar as configurações do IdP. Se precisar desativar ou editar a configuração do SAML, entre em contato com o Technical Support para obter assistência.

7. A partir do System Manager, o administrador habilita o SAML para o array de storage.
8. Os usuários acessam o sistema com suas credenciais de SSO.

Gerenciamento

Ao usar SAML para autenticação, os administradores podem executar as seguintes tarefas de gerenciamento:

- Modificar ou criar novo mapeamento de funções
- Exportar arquivos do provedor de serviços

Restrições de acesso

Quando o SAML está ativado, os usuários não podem descobrir ou gerenciar o armazenamento desse array a partir do Unified Manager ou da interface Storage Manager legada.

Além disso, os seguintes clientes não podem acessar os serviços e recursos do array de storage:

- Janela de gerenciamento empresarial (EMW)
- Clientes de Software Developer Kits (SDK)
- Clientes in-band
- Faça login usando o endpoint padrão da API REST

Conectividade limitada com SAML ativado

Os seguintes recursos do array de storage têm conectividade limitada com autenticação JSON Web Token sempre que o SAML está ativado.

- Interface de linha de comando (CLI)
- Clientes de API REST com autenticação básica HTTP

Saiba mais sobre tokens de acesso e o software SANtricity

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 SAML e JSON web token

Por padrão, um sistema com SAML habilitado não permite acesso às ferramentas tradicionais de linha de comando. A API REST e a CLI tornam-se efetivamente inoperáveis porque o fluxo de trabalho de MFA exige um redirecionamento para um servidor de Identity Provider para autenticação. Portanto, você deve gerar tokens no System Manager, o que exige que um usuário seja autenticado via MFA.

> Não é necessário ter SAML ativado para usar tokens da web, mas SAML é recomendado para o mais alto nível de segurança.

Fluxo de trabalho para criação e uso de 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 para um arquivo e então 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>`
   - **Secure CLI**: Para usar um token na CLI, adicione o valor do token na linha de comando ou use o caminho para um arquivo que contenha o valor do token. Por exemplo:
     - Valor do token na linha de comando: `-t access-token-value`

- Caminho para um arquivo que contém o valor do token: `-T access-token-file`

Saiba mais:

- "Criar tokens de acesso"
- "Editar tokens de acesso"
- "Revogar tokens de acesso"

Use funções de usuário locais

Visualizar funções de usuário locais no SANtricity System Manager

Na guia Funções de Usuário Local, você pode visualizar os mapeamentos dos perfis de usuário para as funções padrão. Esses mapeamentos fazem parte do RBAC (controles de acesso baseado em funções) aplicados no array de storage.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.

Sobre esta tarefa

Os perfis de usuário e seus mapeamentos não podem ser alterados. Somente as senhas podem ser modificadas.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **Funções de usuário local**.

   Os perfis dos usuários são mostrados na tabela:

   - **Administrador raiz** (admin) — Superadministrador que tem acesso a todas as funções do sistema. Este perfil de usuário inclui todas as funções.
   - **Administrador de armazenamento** (storage) — O administrador responsável por todo provisionamento de storage. Este perfil de usuário inclui as seguintes funções: Storage Admin, Support Admin e Monitor.
   - **Administrador de segurança** (segurança) — O usuário responsável pela configuração de segurança, incluindo gerenciamento de acesso, gerenciamento de certificados e funções de unidade com segurança habilitada. Este perfil de usuário inclui as seguintes funções: administrador de segurança e monitor.
   - **Administrador de suporte** (suporte) — O usuário responsável pelos recursos de hardware, dados de falhas e upgrades de firmware. Este perfil de usuário inclui as seguintes funções: Administrador 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 no SANtricity System Manager

Você pode alterar as senhas de usuário para cada perfil de usuário no Access Management.

Antes de começar

- Você deve estar conectado como administrador local, o que inclui permissões de Root admin.
- Você deve saber a senha do administrador local.

Sobre esta tarefa

Mantenha estas diretrizes em mente ao escolher uma senha:

- Quaisquer novas senhas de usuários locais devem atender ou exceder a configuração atual para senha mínima (em Exibir/Editar Configurações).
- As senhas diferenciam maiúsculas de minúsculas.
- Os espaços em branco no final das senhas não são removidos durante a sua criação. Tenha cuidado para incluir os espaços caso eles estejam presentes na senha.
- Para maior segurança, use pelo menos 15 caracteres 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, alterações de senha causam o encerramento da sessão ativa do usuário.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **Funções de usuário local**.
3. Selecione um usuário da tabela.

   O botão Alterar Senha se torna disponível.

4. Selecione **Change Password**.

   A caixa de diálogo Alterar Senha é aberta.

5. Se não houver um comprimento mínimo de senha definido para senhas de usuários locais, você pode marcar a caixa para exigir que o usuário selecionado insira uma senha para acessar o array de storage e, em seguida, você pode digitar a nova senha para o usuário selecionado.
6. Digite a senha do administrador local e, em seguida, clique em **Alterar**.

Resultados

Se o usuário estiver conectado no momento, a alteração da senha faz com que a sessão ativa do usuário seja encerrada.

Alterar as configurações de senha do usuário local em SANtricity System Manager

Você pode definir o comprimento mínimo exigido para todas as senhas de usuários locais novas ou atualizadas no array de storage. Você também pode permitir que usuários locais acessem o array de storage sem inserir uma senha.

Antes de começar

Você deve estar conectado como administrador local, o que inclui permissões de Root admin.

Sobre esta tarefa

Mantenha estas diretrizes em mente ao definir o comprimento mínimo para senhas de usuários locais:

- As alterações de configuração não afetarão as senhas de usuários locais existentes.
- A configuração de comprimento mínimo exigido para senhas de usuários locais deve estar entre 0 e 30 caracteres.
- Quaisquer novas senhas de usuários locais devem atender ou exceder a configuração atual de comprimento mínimo.
- Não defina um comprimento mínimo para a senha se desejar que os usuários locais acessem o array de storage sem digitar uma senha.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **Funções de usuário local**.
3. Selecione o botão **View/Edit Settings**.

   A caixa de diálogo Configurações de senha do usuário local é aberta.

4. Faça uma das seguintes ações:
   - Para permitir que os usuários locais acessem o array de storage *sem* inserir uma senha, desmarque a caixa de seleção "Exigir que todas as senhas de usuários locais tenham pelo menos".
   - Para definir um comprimento mínimo de senha para todas as senhas de usuários locais, marque a caixa de seleção "Exigir que todas as senhas de usuários locais tenham pelo menos" e então use o seletor para definir o comprimento mínimo exigido para todas as senhas de usuários locais.

     Quaisquer novas senhas de usuários locais devem atender ou exceder a configuração atual.

5. Clique em **Salvar**.

Use os serviços de diretório

Adicionar um servidor de diretório LDAP no SANtricity System Manager

Para configurar autenticação para o Access Management, você pode estabelecer comunicações entre o array de storage e um servidor LDAP e, em seguida, mapear os grupos de usuários LDAP para as funções predefinidas do array.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- Os grupos de usuários devem ser definidos no 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 de vinculação.
- Para servidores LDAPS que utilizam um protocolo seguro, a cadeia de certificados do servidor LDAP deve estar instalada em 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 a URL. Se o seu servidor usa 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 você tiver credenciais para uma conta de bind, também pode inserir o nome de usuário e a senha da sua conta. Em seguida, você

mapeia os grupos de usuários do servidor LDAP para as funções predefinidas do array de storage.

> Durante o procedimento para adicionar um servidor LDAP, a interface de gerenciamento legada será desativada. A interface de gerenciamento legada (SYMbol) é um método de comunicação entre o array de storage e o cliente de gerenciamento. Quando desativada, o array de storage e o cliente de gerenciamento usam um método de comunicação mais seguro (API REST sobre https).

Passos

1. Selecione o menu: Configurações [Access Management].
2. Na guia Directory Services, selecione **Add Directory Server**.

   A caixa de diálogo Adicionar Servidor de Diretório é aberta.

3. Na guia Configurações do servidor, insira as credenciais para o servidor LDAP.

Detalhes do campo

Configuração	Descrição
Configurações de configuração	Domínio(s)
Insira o nome de domínio do servidor LDAP. Para vários domínios, insira os nomes de domínio em uma lista separada por vírgulas. O nome de domínio é usado no login (*username* @*domain*) para especificar em qual servidor de diretório autenticar.	URL do servidor
Insira a URL para acessar o servidor LDAP no formato `ldap[s]://**host:***port*`.	Fazer upload do certificado (opcional)
Este campo aparece somente se um protocolo LDAPS for especificado no campo Server URL acima. Clique em **Procurar** e selecione um certificado de CA para carregar. Este é o certificado confiável ou cadeia de certificados usado para autenticação do servidor LDAP.	Vincular conta (opcional)

Configuração	Descrição
Insira uma conta de usuário somente leitura para consultas de pesquisa no servidor LDAP e para pesquisas dentro dos grupos. Insira o nome da conta em um formato do tipo LDAP. Por exemplo, se o bind user for chamado "bindacct", você pode inserir um valor como "CN=bindacct,CN=Users,DC=cpoc,DC=local."	Senha de bind (opcional)
Este campo aparece quando você insere uma conta de bind acima. Digite a senha para a conta de bind.	Testar a conexão do servidor antes de adicionar

Configuração	Descrição
Selecione esta caixa de seleção se desejar garantir que o array de storage possa se comunicar com a configuração do servidor LDAP que você inseriu. O teste ocorre após você clicar em **Adicionar** na parte inferior da caixa de diálogo. Se esta caixa de seleção estiver marcada 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 privilégios**
DN base de pesquisa	Insira o contexto LDAP para pesquisar usuários, normalmente no formato de `CN=Users, DC=cpoc, DC=local`.
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 do usuário, que é usada para o mapeamento de grupo para função. Por exemplo: `memberOf, managedObjects`.

4. Clique na guia **Mapeamento de Funções**.
5. Atribua grupos LDAP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

Detalhes do campo

Configuração	Descrição
Mapeamentos	Nome diferenciado do grupo
Especifique o nome diferenciado (DN) do grupo para o grupo de usuários LDAP a ser mapeado. Expressões regulares são suportadas. Esses caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular: \.[]{}()<>*+-=!?^$	
Funções	Clique no campo e selecione uma das funções do array de storage a ser mapeada para o nome diferenciado do grupo. Você deve selecionar individualmente cada função que deseja incluir para este grupo. A função Monitor é necessária em combinação com as outras funções para fazer login no SANtricity System Manager. As funções mapeadas incluem as seguintes permissões: • **Administrador de armazenamento** — acesso completo de leitura/gravação aos objetos de armazenamento (por exemplo, volumes e conjuntos de discos), mas sem acesso à configuração de segurança. • **Administrador de segurança** — Acesso à configuração de segurança no Gerenciamento de Acesso, gerenciamento de certificados, gerenciamento do log de auditoria e a capacidade de ativar ou desativar a interface de gerenciamento legada (SYMbol). • **Administrador de suporte** — Acesso a todos os recursos de hardware no array de storage, dados de falhas, 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 storage, mas sem acesso à configuração de segurança.

A função de Monitor é obrigatória para todos os usuários, incluindo o administrador. System Manager não funcionará corretamente para nenhum usuário sem a função de 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 **Adicionar**.

   O sistema realiza uma validação, garantindo que o array de storage e o servidor LDAP possam se comunicar. Se uma mensagem de erro aparecer, verifique as credenciais inseridas na caixa de diálogo e insira as informações novamente, se necessário.

Editar as configurações do servidor de diretório e os mapeamentos de funções no SANtricity System Manager

Se você já configurou um servidor de diretório no Access Management, pode 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 precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- É necessário definir um servidor de diretório.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **Directory Services**.
3. Se mais de um servidor estiver definido, selecione o servidor que você deseja editar na tabela.
4. Selecione **Visualizar/Editar Settings**.

   A caixa de diálogo Configurações do Servidor de Diretório é aberta.

5. Na guia Configurações do Servidor, altere as configurações desejadas.

Detalhes do campo

Configuração	Descrição
Configurações de configuração	Domínio(s)
O(s) nome(s) de domínio do(s) servidor(es) LDAP. Para múltiplos 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 autenticar.	URL do servidor
A URL para acessar o servidor LDAP no formato de `ldap[s]://host:port`.	Vincular conta (opcional)
A conta de usuário somente leitura para consultas de pesquisa contra o servidor LDAP e para pesquisas dentro dos grupos.	Senha de bind (opcional)
A senha da conta de bind. (Este campo aparece quando uma conta de bind é inserida.)	Teste a conexão com o servidor antes de salvar

Configuração	Descrição
Verifica se o array de storage consegue se comunicar com a configuração do servidor LDAP. O teste ocorre após você clicar em **Salvar** na parte inferior da caixa de diálogo. Se esta caixa de seleção estiver marcada 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 editar a configuração novamente.	**Configurações de privilégios**
DN base de pesquisa	O contexto LDAP para pesquisar usuários, normalmente no formato de `CN=Users, DC=cpoc, DC=local`.
Atributo de nome de usuário	O atributo que está vinculado ao ID do usuário para autenticação. Por exemplo: `sAMAccountName`.
Atributo(s) do grupo	Uma lista de atributos de grupo do usuário, usada para mapeamento de grupo para função. Por exemplo: `memberOf, managedObjects`.

6. Na guia Mapeamento de Funções, altere o mapeamento desejado.

Detalhes do campo

Configuração	Descrição
Mapeamentos	Nome diferenciado do grupo
O nome de domínio para o grupo de usuários LDAP a ser mapeado. Expressões regulares são suportadas. Esses caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular: \.[]{}()<>*+-=!?^$	
Funções	As funções do array de storage a serem mapeadas para o DN do grupo. Você deve selecionar individualmente cada função que deseja incluir neste grupo. A função Monitor é necessária em combinação com as outras funções para fazer login no SANtricity System Manager. As funções do array de storage incluem o seguinte: • **Administrador de armazenamento** — acesso completo de leitura/gravação aos objetos de armazenamento (por exemplo, volumes e conjuntos de discos), mas sem acesso à configuração de segurança. • **Administrador de segurança** — Acesso à configuração de segurança no Gerenciamento de Acesso, gerenciamento de certificados, gerenciamento do log de auditoria e a capacidade de ativar ou desativar a interface de gerenciamento legada (SYMbol). • **Administrador de suporte** — Acesso a todos os recursos de hardware no array de storage, dados de falhas, 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 storage, mas sem acesso à configuração de segurança.

A função de Monitor é obrigatória para todos os usuários, incluindo o administrador. System Manager não funcionará corretamente para nenhum usuário sem a função de Monitor presente.

7. Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.

8. Clique em **Salvar**.

Resultados

Após concluir esta tarefa, todas as sessões de usuário ativas são encerradas. Apenas a sua sessão de usuário atual é mantida.

Remover servidor de diretório em SANtricity System Manager

Para interromper a conexão entre um servidor de diretório e o array de storage, você pode remover as informações do servidor na página de Access Management. Você pode querer realizar essa tarefa se você configurou um novo servidor e depois quiser remover o antigo.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.

Sobre esta tarefa

Após concluir esta tarefa, todas as sessões de usuário ativas são encerradas. Apenas a sua sessão de usuário atual é mantida.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **Directory Services**.
3. Na lista, selecione o servidor de diretório que você deseja excluir.
4. Clique em **Remover**.

   A caixa de diálogo Remove Directory Server é aberta.

5. Digite `remove` no campo e clique em **Remover**.

   As configurações do servidor de diretório, as configurações de privilégios e os mapeamentos de funções são removidos. Os usuários não podem mais fazer login com credenciais deste servidor.

Usar SAML

Configurar SAML no SANtricity System Manager

Para configurar autenticação para o Gerenciamento de Acesso, você pode usar os recursos da Security Assertion Markup Language (SAML) incorporados no array de storage. Essa configuração estabelece uma conexão entre um Identity Provider e o Storage Provider.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- Você deve saber o endereço IP ou nome de domínio de cada controlador no array de storage.
- Um administrador de IdP configurou um sistema IdP.

- Um administrador do IdP garantiu que o IdP suporta a capacidade de retornar um Name ID na autenticação.
- Um administrador assegurou que os relógios do servidor IdP e do controlador estão sincronizados (seja por meio de um servidor NTP ou ajustando as configurações do relógio do controlador).
- Um arquivo de metadados do IdP é baixado do sistema IdP e fica disponível no sistema local usado para acessar System Manager.

Sobre esta tarefa

Um Provedor de Identidade (IdP) é um sistema externo usado para solicitar credenciais de um usuário e determinar se esse usuário foi autenticado com sucesso. O IdP pode ser configurado para fornecer autenticação multifator e usar qualquer banco de dados de usuários, como Active 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 Access Management é configurado com SAML, o array de storage atua como o Service Provider para solicitar autenticação do Identity Provider. Para estabelecer uma conexão entre o IdP e o array de storage, você compartilha arquivos de metadados entre essas duas entidades. Em seguida, você mapeia as entidades de usuário do IdP para as funções do array de storage. E, finalmente, você testa a conexão e os logins SSO antes de habilitar o SAML.

SAML e Serviços de Diretório. Se você habilitar SAML quando Serviços de Diretório estiver configurado como método de autenticação, SAML substituirá Serviços de Diretório no System Manager. Se você desabilitar SAML depois, a configuração de Serviços de Diretório retornará à configuração anterior.

Edição e Desativação. Depois de ativar o SAML, você *não* pode desativá-lo pela interface de usuário, nem editar as configurações do IdP. Se precisar desativar ou editar a configuração do SAML, entre em contato com o Suporte Técnico para obter assistência.

Configurar a autenticação SAML é um procedimento que envolve várias etapas.

Etapa 1: Carregar o arquivo de metadados do IdP

Para fornecer ao array de storage as informações de conexão do IdP, você importa os metadados do IdP no System Manager. O sistema IdP precisa desses metadados para redirecionar as solicitações de autenticação para a URL correta e para validar as respostas recebidas. Você só precisa carregar um arquivo de metadados para o array de storage, mesmo que haja dois controladores.

Passos

1. Selecione o menu: Configurações [Access Management].
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 Import Identity Provider File é aberta.

4. Clique em **Procurar** para selecionar e carregar o arquivo de metadados do IdP que você copiou para o seu sistema local.

   Após selecionar o arquivo, o IdP Entity ID é exibido.

5. Clique em **Importar**.

Etapa 2: exportar arquivos do provedor de serviços

Para estabelecer uma relação de confiança entre o IdP e o array de storage, você importa os metadados do Service Provider para o IdP. O IdP precisa desses metadados para estabelecer uma relação de confiança com os controladores e para 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 Service Providers.

Passos

1. Clique no link **Export Service Provider files**.

   A caixa de diálogo Export Service Provider Files é aberta.

2. Insira o endereço IP do controlador ou o nome DNS no campo **Controlador A** e, em seguida, clique em **Exportar** para salvar o arquivo de metadados no seu sistema local. Se o array de storage incluir dois controladores, repita esta etapa para o segundo controlador no campo **Controlador B**.

   Após clicar em **Export**, os metadados do Service Provider são baixados para o seu sistema local. Anote onde o arquivo foi armazenado.

3. No sistema local, localize o(s) arquivo(s) de metadados do provedor de serviços que você exportou.

   Existe um arquivo formatado em XML para cada controlador.

4. A partir do servidor IdP, importe o(s) arquivo(s) de metadados do Service Provider para estabelecer a relação de confiança. Você pode importar os arquivos diretamente ou inserir manualmente as informações do controlador a partir dos arquivos.

Etapa 3: mapear funções

Para fornecer aos usuários autorização e acesso ao System Manager, você deve mapear os atributos de usuário e as associações de grupo do IdP para as funções predefinidas do array de storage.

Antes de começar

- Um administrador do IdP configurou os atributos do usuário e a associação a grupos no sistema IdP.
- O arquivo de metadados do IdP é importado para System Manager.
- Um arquivo de metadados do provedor de serviços para cada controlador é importado no sistema IdP para a relação de confiança.

Passos

1. Clique no link para **mapeamento System Manager** de funções.

   A caixa de diálogo Mapeamento de Funções é aberta.

2. Atribua atributos de usuário e grupos do IdP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

Detalhes do campo

Configuração	Descrição
Mapeamentos	Atributo do usuário
Especifique o atributo (por exemplo, "member of") 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 caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular: \.[]{}()<>*+-=!?^$	
Funções	Clique no campo e selecione uma das funções do array de storage a ser mapeada para o atributo. Você deve selecionar individualmente cada função que deseja incluir. A função Monitor é necessária em combinação com as outras funções para fazer login no System Manager. A função Security Admin também é necessária para pelo menos um grupo. As funções mapeadas incluem as seguintes permissões: • **Administrador de armazenamento** — acesso completo de leitura/gravação aos objetos de armazenamento (por exemplo, volumes e conjuntos de discos), mas sem acesso à configuração de segurança. • **Administrador de segurança** — Acesso à configuração de segurança no Gerenciamento de Acesso, gerenciamento de certificados, gerenciamento do log de auditoria e a capacidade de ativar ou desativar a interface de gerenciamento legada (SYMbol). • **Administrador de suporte** — Acesso a todos os recursos de hardware no array de storage, dados de falhas, 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 storage, mas sem acesso à configuração de segurança.

A função de Monitor é obrigatória para todos os usuários, incluindo o administrador. System Manager não funcionará corretamente para nenhum usuário sem a função de Monitor presente.

3. Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.

Os mapeamentos de funções podem ser modificados após o SAML ser ativado.

4. Quando terminar com os mapeamentos, clique em **Salvar**.

Etapa 4: teste o login SSO

Para garantir que o sistema IdP e o array de storage possam se comunicar, você pode, opcionalmente, testar um login SSO. Esse teste também é realizado durante a etapa final para habilitar o SAML.

Antes de começar

- O arquivo de metadados do IdP é importado para System Manager.
- Um arquivo de metadados do provedor de serviços para cada controlador é importado no sistema IdP para a relação de confiança.

Passos

1. Selecione o link **Test SSO Login**.

   Uma caixa de diálogo é aberta para inserir as credenciais de SSO.

2. Insira as credenciais de login de um usuário com permissões de Security Admin e de Monitor.

   Uma caixa de diálogo é aberta enquanto o sistema testa o login.

3. Procure uma mensagem de Teste bem-sucedido. Se o teste for concluído com sucesso, vá para a próxima etapa para habilitar o SAML.

   Se o teste não for concluído com êxito, uma mensagem de erro será exibida com mais informações. Certifique-se de que:

   - O usuário pertence a um grupo com permissões de Security Admin e Monitor.
   - Os metadados que você carregou para o servidor IdP estão corretos.
   - Os endereços dos controladores nos arquivos de metadados do SP estão corretos.

Etapa 5: habilitar SAML

O último passo 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 de login SSO é descrito na etapa anterior.

Antes de começar

- O arquivo de metadados do IdP é importado para System Manager.
- Um arquivo de metadados do provedor de serviços para cada controlador é importado no sistema IdP para a relação de confiança.
- Pelo menos um mapeamento de função de Monitor e um de Security Admin está configurado.

Edição e Desativação. Depois de ativar o SAML, você *não* pode desativá-lo pela interface de usuário, nem editar as configurações do IdP. Se precisar desativar ou editar a configuração do SAML, entre em contato com o Suporte Técnico para obter assistência.

Passos

1. Na aba **SAML**, selecione o link **Enable SAML**.

   A caixa de diálogo Confirm Enable SAML é aberta.

2. Digite `enable`, e clique em **Ativar**.
3. Insira as credenciais do usuário para um teste de login SSO.

Resultados

Após o sistema habilitar SAML, ele encerra todas as sessões ativas e começa a autenticar os usuários por meio de SAML.

Alterar mapeamentos de funções SAML no SANtricity System Manager

Se você já configurou o SAML para gerenciamento de acesso, pode alterar os mapeamentos de funções entre os grupos do IdP e as funções predefinidas do array de storage.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- Um administrador do IdP configurou os atributos do usuário e a associação a grupos no sistema IdP.
- SAML está configurado e ativado.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **SAML**.
3. Selecione **Role Mapping**.

   A caixa de diálogo Mapeamento de Funções é aberta.

4. Atribua atributos de usuário e grupos do 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 System Manager.

Detalhes do campo

Configuração	Descrição
Mapeamentos	Atributo do usuário
Especifique o atributo (por exemplo, "member of") para o grupo SAML a ser mapeado.	Valor do atributo
Especifique o valor do atributo para o grupo a ser mapeado.	Funções

A função de Monitor é obrigatória para todos os usuários, incluindo o administrador. System Manager não funcionará corretamente para nenhum usuário sem a função de Monitor presente.

5. Opcionalmente, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.
6. Clique em **Salvar**.

Resultados

Após concluir esta tarefa, todas as sessões de usuário ativas são encerradas. Apenas a sua sessão de usuário atual é mantida.

Exportar arquivos do provedor de serviços SAML no SANtricity System Manager

Caso necessário, você pode exportar os metadados do Provedor de Serviço para o array de storage e reimportar o(s) arquivo(s) no sistema do Provedor de Identidade (IdP).

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- SAML está configurado e ativado.

Sobre esta tarefa

Nesta 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 para 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 o menu: Configurações [Access Management].
2. Selecione a guia **SAML**.
3. Selecione **Export**.

A caixa de diálogo Export Service Provider Files é aberta.

4. Para cada controlador, clique em **Exportar** para salvar o arquivo de metadados em seu sistema local.

   Os campos de nome de domínio para cada controlador são somente leitura.

   Anote onde o arquivo está armazenado.

5. No sistema local, localize o(s) arquivo(s) de metadados do provedor de serviços que você exportou.

   Existe um arquivo formatado em XML para cada controlador.

6. A partir do servidor IdP, importe o(s) arquivo(s) de metadados do Service Provider. Você pode importar os arquivos diretamente ou inserir manualmente as informações do controlador a partir deles.
7. Clique em **Close**.

Use tokens de acesso

Criar tokens de acesso no SANtricity System Manager

Você pode criar um token de acesso para autenticar-se com a API REST ou interface de linha de comando (CLI) em vez de um nome de usuário e senha.

Tokens não possuem senhas, portanto, você deve gerenciá-los com cuidado.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **Access Tokens**.
3. Selecione **Exibir/Editar configurações de token de acesso**. Na caixa de diálogo, certifique-se de que a caixa de seleção **Habilitar tokens de acesso** esteja marcada. Clique em **Salvar** para fechar a caixa de diálogo.
4. Selecione **Create Access Token**.
5. Na caixa de diálogo, selecione a duração para a qual o token será válido.

   Após o token expirar, as tentativas de autenticação do usuário falharão.

6. Clique em **Criar**.
7. Na caixa de diálogo, selecione uma das seguintes:
   - **Copiar** para salvar o texto do token na área de transferência.
   - **Download** para salvar o texto do token em um arquivo.

     Não se esqueça de salvar o texto do token. Esta é a sua única oportunidade de visualizar o texto antes de fechar a caixa de diálogo.

8. Clique em **Close**.
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>`

- **Secure CLI**: Para usar um token na CLI, adicione o valor do token na linha de comando ou use o caminho para um arquivo que contenha o valor do token. Por exemplo:
  - Valor do token na linha de comando: `-t access-token-value`
  - Caminho para um arquivo que contém 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 configurações de token de acesso em SANtricity System Manager

Você pode editar as configurações dos tokens de acesso, o que inclui os tempos de expiração e a possibilidade de criar novos tokens.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **Access Tokens**.
3. Selecione **Visualizar/Editar Access Token Settings**.
4. Na caixa de diálogo, você pode executar uma ou ambas estas tarefas:
   - Ativar ou desativar a criação de token.
   - Altere a expiração dos tokens existentes.

> Ao desmarcar a opção **Ativar tokens de acesso**, você impede tanto a criação quanto a autenticação de tokens. Se você reativar essa opção posteriormente, os tokens não expirados poderão ser reutilizados. Se desejar revogar permanentemente todos os tokens existentes, consulte "Revogar tokens de acesso".

5. Clique em **Salvar**.

Revogar tokens de acesso no SANtricity System Manager

Você pode revogar todos os tokens de acesso se determinar que um token foi comprometido ou se quiser realizar uma rotação manual das chaves criptográficas usadas para assinar e validar os tokens de acesso.

Esta operação regenera as chaves usadas para assinar os tokens. Assim que as chaves são redefinidas, *todos* os tokens emitidos são imediatamente invalidados. Como o array de storage não rastreia tokens, tokens individuais não podem ser revogados.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **Access Tokens**.
3. Selecione **Revoke All Access Tokens**.
4. Na caixa de diálogo, clique em **Yes**.

Após revogar todos os tokens, você pode criar novos tokens e usá-los imediatamente.

Gerenciar syslog

Visualizar atividade do log de auditoria no SANtricity System Manager

Ao visualizar os logs de auditoria, os usuários com permissões de Security Admin podem monitorar ações do usuário, falhas de autenticação, tentativas de login inválidas e a duração da sessão do usuário.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **log de auditoria**.

   A atividade do log de auditoria é apresentada em formato tabular, que inclui as seguintes colunas de informações:

   - **Data/Hora** — Registro de data e hora de quando o array de storage detectou o evento (em GMT).
   - **Nome de usuário** — O nome de usuário associado ao evento. Para quaisquer ações não autenticadas no array de storage, "N/A" aparece como o nome de usuário. Ações não autenticadas podem ser acionadas pelo proxy interno ou por algum outro mecanismo.
   - **Código de Status** — Código de status HTTP da operação (200, 400, etc.) e texto descritivo associado ao evento.
   - **URL acessada** — URL completa (incluindo host) e string de consulta.
   - **Endereço IP do cliente** — endereço IP do cliente associado ao evento.
   - **Origem** — 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 opções da página de log de auditoria para visualizar e gerenciar eventos.

Detalhes da seleção

Seleção	Descrição
Exibir eventos de…	Limite os eventos exibidos por intervalo de datas (últimas 24 horas, últimos 7 dias, últimos 30 dias ou um intervalo de datas personalizado).
Filtro	Limite os eventos exibidos aos caracteres inseridos no campo. Use aspas ("") para uma correspondência exata de palavras, insira `OR` para retornar uma ou mais palavras ou insira um hífen (—) para omitir palavras.
Atualizar	Selecione **Atualizar** para atualizar a página para os eventos mais atuais.
Ver/Editar configurações	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.
Excluir eventos	Selecione **Delete** 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: • **Método** — O método HTTP (por exemplo, POST, GET, DELETE, etc.). • **Comando CLI executado** — O comando CLI (gramática) executado para solicitações Secure CLI. • **Status de retorno da CLI** — Um código de status da CLI ou uma solicitação de arquivos de entrada do cliente. • **Procedimento SYMbol** — O procedimento SYMbol foi executado. • **Tipo de evento SSH** — Tipo de evento Secure Shell (SSH), como login, logout e login_fail. • **PID da sessão SSH** — Número de identificação do processo da sessão SSH. • **Duração da sessão SSH (s)** — O número de segundos em que o usuário esteve conectado. • **Tipo de autenticação** — Tipos podem incluir usuário local, LDAP, SAML e token de acesso. • **ID de autenticação** — ID da sessão autenticada.
Alternar filtros de coluna	Clique no ícone **Alternar** para abrir os campos de filtro de cada coluna. Digite caracteres em um campo da coluna para limitar os eventos exibidos por esses caracteres. Clique no ícone novamente para fechar os campos de filtro.
Desfazer alterações	Clique no ícone **Desfazer** para retornar a tabela à configuração padrão.

Seleção	Descrição
Exportar	Clique em **Exportar** para salvar os dados da tabela em um arquivo CSV (comma separated value).

Defina as políticas de log de auditoria no SANtricity System Manager

Você pode alterar a política de sobrescrita e os tipos de eventos registrados no log de auditoria.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.

Sobre esta tarefa

Esta tarefa descreve como alterar as configurações do log de auditoria, que incluem a política para sobrescrever eventos antigos e a política para registrar tipos de eventos.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **log de auditoria**.
3. Selecione **Visualizar/Editar Settings**.

   A caixa de diálogo Configurações do log de auditoria é aberta.

4. Altere a política de sobrescrita ou os tipos de eventos registrados.

Detalhes do campo

Configuração	Descrição
Política de sobrescrita	Determina a política para sobrescrever eventos antigos quando a capacidade máxima é atingida: • **Permitir que os eventos mais antigos no 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. • **Exigir que os eventos do log de auditoria sejam excluídos manualmente** — Especifica que os eventos não serão excluídos automaticamente; em vez disso, um aviso de limite será exibido na porcentagem definida. Os eventos devem ser excluídos manualmente. Se a política de sobrescrita 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 Security Admin. Para restaurar o acesso ao sistema para usuários sem permissões de Security Admin, um usuário atribuído à função de Security Admin deve excluir os registros de eventos antigos. As políticas de sobrescrita não se aplicam se um servidor syslog estiver configurado para arquivamento de logs de auditoria.
Nível de ações a serem registradas	Determina os tipos de eventos a serem registrados: • **Somente eventos de modificação de registros** — Mostra apenas os eventos em que uma ação do usuário envolve uma alteração no sistema. • **Registrar todos os eventos de modificação e somente leitura** — Exibe todos os eventos, incluindo uma ação do usuário que envolva a leitura ou o download de informações.

5. Clique em **Salvar**.

Excluir eventos do log de auditoria no SANtricity System Manager

Você pode limpar o log de auditoria de eventos antigos, o que torna a busca por eventos mais gerenciável. Você tem a opção de salvar eventos antigos em um arquivo CSV (valores separados por vírgula) ao excluí-los.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **log de auditoria**.
3. Selecione **Delete**.

   A caixa de diálogo Excluir log de auditoria é aberta.

4. Selecione ou insira o número de eventos mais antigos que você deseja excluir.
5. Se desejar exportar os eventos excluídos para um arquivo CSV (recomendado), mantenha a caixa de seleção marcada. Você será solicitado a inserir um nome e um local para o arquivo ao clicar em **Excluir** na próxima etapa. Caso contrário, se não quiser salvar os eventos em um arquivo CSV, clique na caixa de seleção para desmarcá-la.
6. Clique em **Delete**.

   Uma caixa de diálogo de confirmação é aberta.

7. Digite `delete` no campo e clique em **Excluir**.

   Os eventos mais antigos são removidos da página de log de auditoria.

Configurar o servidor syslog para log de auditoria no SANtricity System Manager

Se você quiser arquivar logs de auditoria em um servidor syslog externo, pode configurar a comunicação entre esse servidor e o array de storage. Após a conexão ser estabelecida, os logs de auditoria são salvos automaticamente no servidor syslog.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- O endereço do servidor syslog, o protocolo e o número da porta devem estar disponíveis. O endereço do servidor pode ser um domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- Se o seu servidor utiliza um protocolo seguro (por exemplo, TLS), um certificado de Autoridade Certificadora (CA) deve estar disponível no seu sistema local. Os certificados de CA identificam os proprietários de websites para conexões seguras entre servidores e clientes.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Na guia log de auditoria, selecione **Configurar servidores syslog**.

   A caixa de diálogo Configurar servidores syslog é aberta.

3. Clique em **Add**.

   A caixa de diálogo Adicionar Servidor syslog é aberta.

4. Insira as informações do servidor e clique em **Adicionar**.
   - **Endereço do servidor** — Insira um domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
   - **Protocolo** — selecione um protocolo na lista suspensa (por exemplo, TLS, UDP ou TCP).

- **Carregar certificado (opcional)** — Se você selecionou o protocolo TLS e ainda não carregou um certificado de CA assinado, clique em **Procurar** 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 posteriormente, o handshake TLS falhará. Como resultado, uma mensagem de erro será registrada no log de auditoria e as mensagens não serão mais enviadas para o servidor syslog. Para resolver esse problema, você deve corrigir o certificado no servidor syslog e então acessar menu:Configurações [Log de Auditoria > Configurar Servidores Syslog > Testar Todos].

- **Porta** — Insira o número da porta para o syslog receiver. Depois de clicar em **Adicionar**, a caixa de diálogo Configurar Servidores Syslog será aberta e exibirá o seu servidor syslog configurado na página.

5. Para testar a conexão do servidor com o array de storage, selecione **Test All**.

Resultados

Após a configuração, todos os novos logs de auditoria são enviados para o servidor syslog. Os logs anteriores não são transferidos. Para configurar ainda mais as definições do syslog para alertas, consulte "Configurar servidor syslog para alertas".

```
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 no SANtricity System Manager

Você pode alterar as configurações do servidor syslog usado para arquivamento de logs de auditoria e também carregar um novo certificado de Autoridade Certificadora (CA) para o servidor.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- O endereço do servidor syslog, o protocolo e o número da porta devem estar disponíveis. O endereço do servidor pode ser um 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 seu sistema local.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Na guia log de auditoria, selecione **Configurar servidores syslog**.

   Os servidores syslog configurados são exibidos na página.

3. Para editar as informações do servidor, selecione o ícone **Editar** (lápis) à direita do nome do servidor e, em seguida, faça as alterações desejadas nos seguintes campos:
   - **Endereço do servidor** — Insira um domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.

- **Protocolo** — selecione um protocolo na lista suspensa (por exemplo, TLS, UDP ou TCP).
- **Porta** — Insira o número da porta para o receptor syslog.

4. Se você alterou o protocolo para o protocolo seguro TLS (de UDP ou TCP), clique em **Import Trusted Certificate** para carregar um certificado de CA.
5. Para testar a nova conexão com o array de storage, selecione **Test All**.

Resultados

Após a configuração, todos os novos logs de auditoria são enviados para o servidor syslog. Os logs anteriores não são transferidos.

Perguntas frequentes sobre gerenciamento de acesso de usuário para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

Por que não consigo fazer login?

Se você receber um erro ao tentar fazer login no SANtricity System Manager, verifique estas possíveis causas.

Erros de login no System Manager podem ocorrer por um destes motivos:

- Você digitou um nome de usuário ou senha incorretos.
- Você não possui privilégios suficientes.
- O servidor de diretório (se configurado) pode estar indisponível. Se for esse o caso, tente fazer login com uma função de usuário local.
- Você tentou fazer login várias vezes sem sucesso, o que ativou o modo de bloqueio. Aguarde 10 minutos para fazer login novamente.
- Uma condição de bloqueio foi acionada e seu log de auditoria pode estar cheio. Vá para Gerenciamento de Acesso e exclua eventos antigos do log de auditoria.
- A autenticação SAML está ativada. Atualize seu navegador para fazer login.

Os erros de login em um array de storage remoto para tarefas de espelhamento podem ocorrer por um dos seguintes motivos:

- Você inseriu uma senha incorreta.
- Você tentou fazer login várias vezes sem sucesso, o que ativou o modo de bloqueio. Aguarde 10 minutos para fazer login novamente.
- O número máximo de conexões de clientes utilizadas no controlador foi atingido. Verifique se há vários usuários ou clientes.

O que preciso saber antes de adicionar um servidor de diretório?

Antes de adicionar um servidor de diretório em Access Management, certifique-se de atender aos seguintes requisitos.

- Os grupos de usuários devem ser definidos no 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 de vinculação.
- Para servidores LDAPS que utilizam um protocolo seguro, a cadeia de certificados do servidor LDAP deve estar instalada em sua máquina local.

O que preciso saber sobre o mapeamento para funções de array de storage?

Antes de associar grupos a funções, revise as seguintes diretrizes.

Os recursos RBAC (controle de acesso baseado em funções) integrados ao array de storage incluem as seguintes funções:

- **Administrador de armazenamento** — acesso completo de leitura/gravação aos objetos de armazenamento (por exemplo, volumes e conjuntos de discos), mas sem acesso à configuração de segurança.
- **Administrador de segurança** — Acesso à configuração de segurança no Gerenciamento de Acesso, gerenciamento de certificados, gerenciamento do log de auditoria e a capacidade de ativar ou desativar a interface de gerenciamento legada (SYMbol).
- **Administrador de suporte** — Acesso a todos os recursos de hardware no array de storage, dados de falhas, 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 storage, mas sem acesso à configuração de segurança.

Serviços de diretório

Se você estiver usando um servidor LDAP (Lightweight Directory Access Protocol) e Directory Services, certifique-se de que:

- Um administrador definiu grupos de usuários no serviço de diretório.
- Você conhece os nomes de domínio dos grupos de usuários LDAP. Expressões regulares são suportadas. Esses caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular:

```
\.[]{}()<>*+-=!?^$|
```

- A função de Monitor é obrigatória para todos os usuários, incluindo o administrador. System Manager não funcionará corretamente para nenhum usuário sem a função de Monitor presente.

SAML

Se você estiver usando os recursos de Security Assertion Markup Language (SAML) incorporados no array de storage, certifique-se de que:

- Um administrador do Identity Provider (IdP) configurou os atributos do usuário e a associação a grupos no sistema IdP.
- Você conhece os nomes de associação do grupo.
- Você conhece o valor do atributo para o grupo a ser mapeado. Expressões regulares são suportadas. Esses caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\ se não fizerem parte de um padrão de expressão regular:

```
\.[]{}()<>*+-=!?^$|
```

- A função de Monitor é obrigatória para todos os usuários, incluindo o administrador. System Manager não funcionará corretamente para nenhum usuário sem a função de Monitor presente.

Quais ferramentas de gerenciamento externo podem ser afetadas por essa mudança?

Ao fazer determinadas alterações no SANtricity System Manager, como trocar a interface de gerenciamento ou usar SAML como método de autenticação, algumas ferramentas e recursos externos podem ser restringidos de uso.

Interface de gerenciamento

Ferramentas que se comunicam diretamente com a interface de gerenciamento legada (SYMbol), como o SANtricity SMI-S Provider ou OnCommand Insight (OCI), não funcionam a menos que a configuração da Interface de Gerenciamento Legada esteja habilitada. Além disso, você não pode usar comandos CLI legados nem realizar operações de espelhamento se essa configuração estiver desabilitada.

Contate o suporte técnico para obter mais informações.

Autenticação SAML

Quando o SAML está ativado, os seguintes clientes não podem acessar os serviços e recursos do array de storage:

- Janela de gerenciamento empresarial (EMW)
- Interface de linha de comando (CLI)
- Clientes de Software Developer Kits (SDK)
- Clientes in-band
- Clientes de API REST com autenticação básica HTTP
- Faça login usando o endpoint padrão da API REST

Contate o suporte técnico para obter mais informações.

O que preciso saber antes de configurar e habilitar o SAML?

Antes de configurar e ativar os recursos do Security Assertion Markup Language (SAML) para autenticação, certifique-se de atender aos seguintes requisitos e compreender as restrições do SAML.

Requisitos

Antes de começar, certifique-se de que:

- Um Provedor de Identidade (IdP) está configurado em sua rede. Um IdP é um sistema externo usado para solicitar credenciais de um usuário e determinar se o usuário foi autenticado com sucesso. Sua equipe de segurança é responsável por manter o IdP.
- Um administrador do IdP configurou atributos de usuário e grupos no sistema IdP.
- Um administrador do IdP garantiu que o IdP suporta a capacidade de retornar um Name ID na autenticação.

- Um administrador assegurou que os relógios do servidor IdP e do controlador estão sincronizados (seja por meio de um servidor NTP ou ajustando as configurações do relógio do controlador).
- Um arquivo de metadados do IdP é baixado do sistema IdP e fica disponível no sistema local usado para acessar System Manager.
- Você conhece o endereço IP ou nome de domínio de cada controlador no array de storage.

Restrições

Além dos requisitos acima, certifique-se de entender as seguintes restrições:

- Uma vez que o SAML esteja habilitado, você *não* pode desabilitá-lo através da interface de usuário, nem editar as configurações do IdP. Se você precisar desabilitar ou editar a configuração do SAML, entre em contato com o suporte técnico para obter assistência. Recomendamos que você teste os logins SSO antes de habilitar o SAML na etapa final de configuração. (O sistema também realiza um teste de login SSO antes de habilitar o SAML.)
- Se você desativar o SAML no futuro, o sistema restaurará automaticamente a configuração anterior (Local User Roles e/ou Directory Services).
- Se os Serviços de Diretório estiverem configurados atualmente para autenticação de usuário, o SAML substituirá essa configuração.
- Quando o SAML está configurado, os seguintes clientes não podem acessar os recursos do array de storage:
  - Janela de gerenciamento empresarial (EMW)
  - Interface de linha de comando (CLI)
  - Clientes de Software Developer Kits (SDK)
  - Clientes in-band
  - Clientes de API REST com 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 registrar eventos de modificação ou eventos de modificação e somente leitura.

Dependendo das configurações da política, os seguintes tipos de eventos são exibidos:

- **Eventos de modificação** — Ações do usuário no System Manager que envolvem alterações no sistema, como provisionamento de storage.
- **Eventos de modificação e somente leitura** — Ações do usuário que envolvem alterações no sistema, bem como eventos que envolvem visualizar ou baixar informações, como visualizar atribuições de volume.

O que preciso saber antes de configurar um servidor syslog?

Você pode arquivar os logs de auditoria em um servidor syslog externo.

Antes de configurar um servidor syslog, tenha em mente as seguintes diretrizes.

- Certifique-se de saber 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 seu servidor utiliza um protocolo seguro (por exemplo, TLS), um certificado de Autoridade Certificadora (CA) deve estar disponível no seu sistema local. Os certificados de CA identificam os

proprietários de websites para conexões seguras entre servidores e clientes.

- Após a configuração, todos os novos logs de auditoria são enviados para o servidor syslog. Os logs anteriores não são transferidos.
- As configurações da Overwrite Policy (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 devo fazer?

Se você configurou um servidor syslog com o 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 registrada no log de auditoria.

Para resolver esse problema, primeiro você precisa corrigir o certificado do servidor syslog. Depois que uma cadeia de certificados válida estiver em vigor, acesse o menu:Configurações [Log de auditoria > Configurar servidores syslog > Testar todos].

Certificados

Saiba mais sobre certificados no SANtricity System Manager

Você pode usar SANtricity 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 certificadora (CA) e um *certificado autoassinado* é validado pelo proprietário da entidade em vez de uma terceira parte.

Saiba mais:

- "Como funcionam os certificados"
- "Terminologia de certificado"

Como faço para configurar certificados assinados?

Você pode gerar uma solicitação de assinatura a partir de System Manager ou externamente usando um par de chaves privada e pública. A solicitação de assinatura é enviada a uma CA para gerar os arquivos de certificado. Assim que a CA retornar os arquivos de certificado, você os importa usando System Manager.

Saiba mais:

- "Use certificados assinados por CA para os controladores"
- "Use certificados assinados por CA para autenticação com um servidor de gerenciamento de chaves"

Informações relacionadas

Saiba mais sobre tarefas relacionadas a certificados:

- "Visualizar informações do certificado importado"
- "Ativar verificação de revogação de certificado"

Conceitos

Como funcionam os certificados no SANtricity System Manager

Certificados são arquivos digitais que identificam entidades online, como sites e servidores, para comunicações seguras na internet.

Os certificados garantem que as comunicações web sejam transmitidas de forma criptografada, privada e inalterada, somente entre o servidor especificado e o cliente. Usando System Manager, você pode gerenciar certificados entre o navegador em um sistema de gerenciamento de host (atuando como o cliente) e os controladores em um sistema de storage (atuando como os servidores).

Um certificado pode ser assinado por uma autoridade confiável ou pode ser autoassinado. "Assinar" significa simplesmente que alguém validou a identidade do proprietário e determinou que seus dispositivos podem ser confiáveis. Os arrays de storage são fornecidos com um certificado autoassinado gerado automaticamente em cada controlador. Você pode continuar a usar os certificados autoassinados ou pode obter certificados assinados por CA para uma conexão mais segura entre os controladores e os sistemas host.

> Embora os certificados assinados por uma Autoridade Certificadora (CA) ofereçam melhor proteção de segurança (por exemplo, prevenindo ataques do tipo "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 frequentemente usados em ambientes de teste internos, não em ambientes de produção.

Certificados assinados

Um certificado assinado é validado por uma autoridade certificadora (CA), que é uma organização de terceiro 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.

Ao abrir um navegador e digitar um endereço da web, seu sistema realiza um processo de verificação de certificado em segundo plano para determinar se você está se conectando a um site que inclui um certificado válido, assinado por uma CA. Geralmente, um site protegido com um certificado assinado inclui um ícone de cadeado e uma designação https no endereço. Se você tentar se conectar a um site que não contenha um certificado assinado por uma CA, seu navegador exibirá um aviso de que o site não é seguro.

A Autoridade Certificadora (CA) toma medidas para verificar sua identidade durante o processo de solicitação. Ela pode enviar um e-mail para o endereço comercial registrado da sua empresa, verificar o endereço comercial e realizar uma verificação HTTP ou DNS. Quando o processo de solicitação estiver concluído, a CA envia arquivos digitais para você carregar em um sistema de gerenciamento de host. Normalmente, esses arquivos incluem uma cadeia de confiança, conforme a seguir:

- **Raiz** — No topo da hierarquia está o certificado raiz, que contém uma chave privada usada para assinar outros certificados. A raiz identifica uma organização CA específica. Se você usar a mesma CA para todos os seus dispositivos de rede, precisará apenas de um certificado raiz.
- **Intermediário** — Ramificando-se a partir da raiz estão os certificados intermediários. A CA emite um ou mais certificados intermediários para atuarem como intermediários entre uma raiz protegida e os certificados do servidor.

- **Servidor** — Na base da cadeia está o certificado do servidor, que identifica sua entidade específica, como um site ou outro dispositivo. Cada controlador em um array de storage requer um certificado de servidor separado.

Certificados autoassinados

Cada controlador no array de storage inclui um certificado autoassinado pré-instalado. Um certificado autoassinado é semelhante a um certificado assinado por uma CA, exceto que é validado pelo proprietário da entidade em vez de um terceiro. Assim como um certificado assinado por uma 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 cliente. No entanto, um certificado autoassinado não utiliza a mesma cadeia de confiança que um certificado assinado por uma CA.

Os certificados autoassinados não são "trusted" pelos navegadores. Cada vez que você tenta se conectar 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 prosseguir para o site; ao fazer isso, você está essencialmente aceitando o certificado autoassinado.

Certificados usados para o servidor de gerenciamento de chaves

Se você estiver usando um servidor de gerenciamento de chaves externo com o recurso Drive Security, também pode gerenciar certificados para autenticação entre esse servidor e os controladores.

Aprenda sobre a terminologia de certificados no software SANtricity

Os seguintes termos aplicam-se ao gerenciamento de certificados.

Termo	Descrição
CA	Uma autoridade certificadora (CA) é uma entidade confiável que emite documentos eletrônicos, chamados certificados digitais, para segurança na Internet. Esses certificados identificam os proprietários de sites, permitindo conexões seguras entre clientes e servidores.
CSR	Uma Solicitação de Assinatura de Certificado (CSR, na sigla em inglês) é uma mensagem enviada por um solicitante a uma autoridade certificadora (CA, na sigla em inglês). A CSR valida as informações que a CA exige para emitir um certificado.
Certificado	Um certificado identifica o proprietário de um site para fins de segurança, o que impede que invasores se façam passar pelo 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 no topo da hierarquia, um ou mais certificados intermediários e os certificados de servidor que identificam as entidades.
Certificado do cliente	Para o gerenciamento de chaves de segurança, um certificado de cliente valida os controladores do array de storage, para que o servidor de gerenciamento de chaves possa confiar em seus endereços IP.

Termo	Descrição
Certificado intermediário	Um ou mais certificados intermediários ramificam-se a partir da raiz na cadeia de certificados. A CA emite um ou mais certificados intermediários para atuarem como intermediários entre uma raiz protegida e os certificados do servidor.
Certificado do servidor de gerenciamento de chaves	Para o gerenciamento de chaves de segurança, um certificado de servidor de gerenciamento de chaves valida o servidor, assim o array de storage pode confiar em seu endereço IP.
Keystore	Um keystore é um repositório no seu sistema de gerenciamento de hosts que contém chaves privadas, juntamente com suas respectivas chaves públicas e certificados. Essas chaves e certificados identificam suas próprias entidades, como os controladores.
Servidor OCSP	O servidor do Protocolo de Status de Certificado Online (OCSP) determina se a autoridade certificadora (CA) revogou algum certificado antes da data de expiração programada 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 CA específica. Se você usar a mesma CA para todos os seus dispositivos de rede, precisará de apenas um certificado raiz.
Certificado assinado	Um certificado validado por uma autoridade certificadora (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 por meio de uma conexão HTTPS. Além disso, um certificado assinado inclui detalhes sobre o proprietário da entidade (normalmente, um servidor ou website) e uma assinatura digital composta por letras e números. Um certificado assinado utiliza uma cadeia de confiança e, portanto, é mais frequentemente usado em ambientes de produção. Também conhecido como "certificado assinado por CA" ou "certificado de gerenciamento".
Certificado autoassinado	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 por meio de uma conexão HTTPS. Ele também inclui uma assinatura digital composta por letras e números. Um certificado autoassinado não utiliza a mesma cadeia de confiança que um certificado assinado por uma CA e, portanto, é mais frequentemente usado em ambientes de teste. Também é conhecido como um certificado "pré-instalado".
Certificado do servidor	O certificado do servidor está na base 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.

Usar certificados

Use certificados assinados por CA para controladores no SANtricity System Manager

Você pode obter certificados assinados por CA para comunicações seguras entre os controladores e o navegador usado para acessar SANtricity System Manager.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.
- Você precisa saber o endereço IP ou os nomes DNS de cada controlador.

Sobre esta tarefa

Utilizar certificados assinados por uma CA é um procedimento de três etapas.

Etapa 1: preencha os CSRs para os controladores

Primeiro, você deve gerar um arquivo de solicitação de assinatura de certificado (CSR) para cada controlador no array de storage.

Sobre esta tarefa

Esta tarefa descreve como gerar um arquivo CSR a partir do System Manager. O CSR fornece informações sobre sua organização e, ou o endereço IP ou o nome DNS do controlador. Durante esta tarefa, um arquivo CSR é gerado se o array de storage 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 Etapa 2: enviar os arquivos CSR.

Passos

1. Selecione **Configurações › Certificados**.
2. Na aba Array Management, selecione **Complete CSR**.

> Se você vir uma caixa de diálogo solicitando que aceite um certificado autoassinado para o segundo controlador, clique em **Accept Self-Signed Certificate** para prosseguir.

3. Insira as seguintes informações e clique em **Avançar**:
   - **Organização** — O nome completo e legal da sua empresa ou organização. Inclua sufixos, como Inc. ou Corp.
   - **Unidade organizacional (opcional)** — A divisão da sua organização que está lidando com o certificado.
   - **Cidade/Localidade** — A cidade onde seu array de storage ou empresa está localizado.
   - **Estado/Região (opcional)** — O estado ou região onde seu array de storage ou empresa está localizado.
   - **Código ISO do país** — O código ISO (Organização Internacional de Normalização) de dois dígitos do seu país, como US.

Alguns campos podem estar preenchidos previamente com as informações apropriadas, como o endereço IP do controlador. Não altere os valores preenchidos previamente, a menos que tenha certeza de que estão incorretos. Por exemplo, se você ainda não concluiu um CSR, o endereço IP do controlador está definido como “localhost.” Nesse 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 em seu array de storage:
   - **Nome comum do Controlador A** — O endereço IP ou o nome DNS do controlador A é exibido por padrão. Certifique-se de que este endereço esteja correto; ele deve corresponder exatamente ao que você digita para acessar System Manager no navegador. O nome DNS não pode começar com um caractere curinga.
   - **Endereços IP alternativos do Controlador A** — Se o nome comum for um endereço IP, você pode, opcionalmente, inserir quaisquer endereços IP adicionais ou aliases para o controlador A. Para múltiplas entradas, use um formato separado por vírgulas.
   - **Nomes DNS alternativos do controlador A** — Se o nome comum for um nome DNS, insira quaisquer nomes DNS adicionais para o controlador A. Para várias entradas, use o formato separado por vírgulas. Se não houver nomes DNS alternativos, mas você tiver inserido um nome DNS no primeiro campo, copie esse nome aqui. O nome DNS não pode começar com um caractere curinga. Se o array de storage tiver apenas um controlador, o botão **Finish** estará disponível.

     Se o array de storage tiver dois controladores, o botão **Next** estará disponível.

Não clique no link **Pular esta etapa** ao criar 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 pule a etapa de criação de uma solicitação CSR no controlador A, caso ela já esteja definida, e continue para a próxima etapa para recriar uma solicitação CSR no controlador B.

5. Se houver apenas um controlador, clique em **Concluir**. Se houver dois controladores, clique em **Avançar** para inserir as informações do controlador B (como acima) e, em seguida, clique em **Concluir**.

   Para um único controlador, um arquivo CSR é baixado para o seu sistema local. Para dois controladores, dois arquivos CSR são baixados. O local da pasta de download depende do seu navegador.

6. Vá para Etapa 2: enviar os arquivos CSR.

Etapa 2: enviar os arquivos CSR

Após criar os arquivos de solicitação de assinatura de certificado (CSR), envie os arquivos para uma autoridade certificadora (CA). E-Series systems 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 arquivos CSR baixados.
2. Envie os arquivos CSR para uma Autoridade Certificadora (por exemplo, Verisign ou DigiCert), e solicite certificados assinados no formato PEM.

Após enviar um arquivo CSR para a CA, NÃO gere outro arquivo CSR. Sempre que você gera um CSR, o sistema cria um par de chaves privada e pública. A chave pública faz parte do CSR, enquanto a chave privada é mantida no keystore do sistema. Quando você recebe os certificados assinados e os importa, o sistema garante que tanto a chave privada quanto a pública sejam o par original. Se as chaves não corresponderem, os certificados assinados não funcionarão e você deve 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

Após receber os certificados assinados da Certificate Authority (CA), importe os arquivos dos controladores.

Antes de começar

- A Autoridade Certificadora (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 em cadeia (por exemplo, um arquivo .p7b), você deve descompactar o arquivo em cadeia 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 do Windows `certmgr` para descompactar os arquivos (clique com o botão direito e selecione **All Tasks › Export**). A codificação Base-64 é recomendada. Quando as exportações forem concluídas, um arquivo CER será exibido para cada arquivo de certificado na cadeia.
- Você copiou os arquivos de certificado para o sistema host onde acessa System Manager.

Passos

1. Selecione o menu: Configurações[Certificados]
2. Na guia Array Management, selecione **Import**.

   Uma caixa de diálogo é aberta para importar o(s) arquivo(s) de certificado.

3. Clique nos botões **Procurar** para primeiro selecionar 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. Somente 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 junto 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 encerrada automaticamente. Você deve fazer login novamente para que os certificados entrem em vigor. Ao fazer login novamente, os novos certificados assinados pela CA são usados para sua sessão.

Redefinir certificados de gerenciamento em SANtricity System Manager

Você pode reverter os certificados nos controladores de certificados assinados por CA para os certificados autoassinados definidos de fábrica.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.
- Os certificados assinados pela CA devem ser importados previamente.

Sobre esta tarefa

A função Reset exclui os arquivos de certificado assinados pela CA de cada controlador. Os controladores voltarão então a usar certificados autoassinados.

Passos

1. Selecione **Configurações › Certificados**.
2. Na guia Array Management, selecione **Reset**.

   Uma caixa de diálogo Confirm Reset Management Certificates será aberta.

3. Digite `reset` no campo e clique em **Redefinir**.

   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 ocorre quando você volta a usar 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 voltam a usar certificados autoassinados. Como resultado, o sistema solicita aos usuários que aceitem manualmente o certificado autoassinado para suas sessões.

Visualizar informações do certificado importado no SANtricity System Manager

Na página Certificados, você pode visualizar o tipo de certificado, a autoridade emissora e o intervalo de datas de validade dos certificados para o array de storage.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.

Passos

1. Selecione **Configurações › Certificados**.
2. Selecione uma das abas para visualizar informações sobre os certificados.

Aba	Descrição
Gerenciamento de array	Visualize informações sobre os certificados assinados pela CA importados para cada controlador, incluindo o arquivo root, o(s) arquivo(s) intermediate e o(s) arquivo(s) server.

Aba	Descrição
Confiável	Visualize informações sobre todos os outros tipos de certificados importados para os controladores. Use o campo de filtro em **Mostrar certificados que são…** para visualizar certificados instalados pelo usuário ou pré-instalados. • **Instalados pelo usuário** — Certificados que um usuário carregou para o array de storage, que podem incluir certificados confiáveis quando o controlador atua como cliente (em vez de servidor), certificados LDAPS e certificados de Federação de Identidade. • **Pré-instalado** — Certificados autoassinados incluídos com o array de storage.
Gerenciamento de chaves	Veja informações sobre os certificados assinados pela CA importados para um servidor de gerenciamento de chaves externo.

Importar certificados para controladores ao atuar como clientes no SANtricity System Manager

Se o controlador rejeitar uma conexão por não conseguir validar a cadeia de confiança de um servidor de rede, você pode importar um certificado da guia Trusted que permite ao controlador (atuando como cliente) aceitar comunicações desse servidor.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.
- Os arquivos de certificado estão instalados no seu sistema local.

Sobre esta tarefa

Pode ser necessário importar certificados da guia Confiáveis 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 **Configurações › Certificados**.
2. Na aba Trusted, selecione **Importar**.

   Uma caixa de diálogo é aberta para importar os arquivos de certificado confiáveis.

3. Clique em **Procurar** para selecionar os arquivos de certificado dos controladores.

   Os nomes dos arquivos são exibidos na caixa de diálogo.

4. Clique em **Importar**.

Resultados

Os arquivos são carregados e validados.

${post_edited_translations.segment}

${post_edited_translations.segment}

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.
- Um servidor DNS está configurado em ambos os controladores, o que permite o uso de um domínio totalmente qualificado para o servidor OCSP. Esta tarefa está disponível na página Hardware.
- Se você deseja 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 CA emitiu um certificado indevidamente ou uma chave privada foi 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 algum certificado antes da data de expiração programada e, em seguida, bloqueia o usuário de acessar um site se o certificado estiver revogado.

Passos

1. Selecione **Configurações › Certificados**.
2. Selecione a guia **Trusted**.

   Você também pode ativar a verificação de revogação na guia **Key Management**.

3. Clique em **Tarefas incomuns** e, em seguida, selecione **Ativar verificação de revogação** no menu suspenso.
4. Selecione **Desejo 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 **Endereço do servidor OCSP**, você pode opcionalmente inserir uma URL para um servidor OCSP. Se você não inserir um endereço, o sistema usará a URL do servidor OCSP do arquivo de certificado.
6. Clique em **Test Address** para garantir que o sistema consiga abrir uma conexão com o URL especificado.
7. Clique em **Salvar**.

Resultados

Se o array de storage tentar se conectar a um servidor com um certificado revogado, a conexão é negada e um evento é registrado.

Excluir certificados confiáveis no SANtricity System Manager

Você pode excluir os certificados instalados pelo usuário importados anteriormente da guia Confiáveis.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.
- Se você estiver atualizando um certificado confiável para uma nova versão, o certificado atualizado deve ser importado antes de excluir o certificado antigo.

Você pode perder o acesso a um sistema se excluir um certificado usado 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 excluir certificados instalados pelo usuário. Os certificados autoassinados pré-instalados não podem ser excluídos.

Passos

1. Selecione **Configurações › Certificados**.
2. Selecione a guia **Trusted**.

   A tabela mostra os certificados confiáveis do array de storage.

3. Na tabela, selecione o certificado que você deseja remover.
4. Clique em **Tarefas incomuns › Excluir**.

   Uma caixa de diálogo Confirmar Exclusão de Certificado Confiável é aberta.

5. Digite `delete` no campo e clique em **Excluir**.

Use certificados assinados por CA para autenticação com um servidor de gerenciamento de chaves no SANtricity System Manager

Para garantir a comunicação segura entre um servidor de gerenciamento de chaves e os controladores do array de storage, você deve configurar os conjuntos de certificados apropriados.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de 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: preencha e envie o CSR para autenticação com um servidor de gerenciamento de chaves

Primeiro, você deve gerar um arquivo de solicitação de assinatura de certificado (CSR) e, em seguida, 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 do servidor de gerenciamento de chaves usando o arquivo CSR baixado. Um certificado de cliente valida os controladores do array de storage, permitindo que o servidor de gerenciamento de chaves confie em suas solicitações do Key Management Interoperability Protocol (KMIP).

Os arquivos CSR gerados externamente por meio de pares de chaves pública e privada podem ser importados através da caixa de diálogo Criar Chave de Segurança Externa. Para obter mais informações sobre como importar um arquivo CSR gerado externamente, consulte "Etapa 2: importar certificados para o servidor de gerenciamento de chaves".

Passos

1. Selecione **Configurações › Certificados**.
2. Na guia Key Management, selecione **Complete CSR**.
3. Insira as seguintes informações:
   - **Nome comum** — Um nome que identifica o cliente. É prática comum que o nome comum corresponda aos requisitos do servidor KMS para convenções de nomenclatura de certificados de cliente. O nome comum geralmente ajuda o KMS a identificar o certificado do cliente quando este é apresentado durante um handshake.
   - **Organização** — O nome completo e legal da sua empresa ou organização. Inclua sufixos, como Inc. ou Corp.
   - **Unidade organizacional (opcional)** — A divisão da sua organização que está lidando com o certificado.
   - **Cidade/Localidade** — A cidade ou localidade onde sua organização está localizada.
   - **Estado/Região (opcional)** — O estado ou região onde sua organização está localizada.
   - **Código ISO do país** — O código ISO (International Organization for Standardization) de dois dígitos, como US, onde sua organização está localizada.
4. Clique em **Download**.

   Um arquivo CSR é salvo em seu sistema local.

5. Solicite um certificado de cliente assinado pela CA que seja confiável para o servidor de gerenciamento de chaves.

   É comum que o servidor de gerenciamento de chaves possua um recurso que gera certificados assinados diretamente, pois funciona como sua própria CA.

6. Quando você tiver um certificado de cliente, acesse Etapa 2: importar certificados para o servidor de gerenciamento de chaves.

Etapa 2: importar certificados para o servidor de gerenciamento de chaves

Como próximo passo, você importa certificados para autenticação entre o array de storage e o servidor de gerenciamento de chaves. Existem dois tipos de certificados: o certificado do cliente valida os controladores do array de storage, enquanto o certificado do servidor de gerenciamento de chaves valida o servidor. Você deve carregar tanto o arquivo de certificado do cliente para os controladores quanto o arquivo de certificado do servidor para o servidor de gerenciamento de chaves.

Antes de começar

- Você possui um arquivo de certificado de cliente assinado (consulte Etapa 1: preencha e envie o CSR para autenticação com um servidor de gerenciamento de chaves), e copiou esse arquivo para o host onde está acessando System Manager. Um certificado de cliente valida os controladores do array de storage, permitindo que o servidor de gerenciamento de chaves confie em suas solicitações do Key Management Interoperability Protocol (KMIP).
- Você deve obter um arquivo de certificado do servidor de gerenciamento de chaves e, em seguida, copiar esse arquivo para o host onde você está acessando System Manager. Um certificado de servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, então o array de storage pode confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.

Para obter mais informações sobre o certificado do servidor, consulte a documentação do seu key management server.

Passos

1. Selecione **Configurações › Certificados**.
2. Na guia Key Management, selecione **Import**.

   Uma caixa de diálogo é aberta para importar os arquivos de certificado.

3. Ao lado de **Selecionar certificado do cliente**, clique no botão **Procurar** para selecionar o arquivo de certificado do cliente para os controladores do array de storage.

   O nome do arquivo é exibido na caixa de diálogo.

4. Se você gerou um arquivo de certificado externamente usando um par de chaves privada e pública, clique no botão **Procurar** ao lado de **Selecionar arquivo de chave privada** para selecionar o arquivo de certificado para os controladores do array de storage.

   O nome do arquivo é exibido na caixa de diálogo.

5. Ao lado de **Selecionar certificado do servidor de gerenciamento de chaves**, clique no botão **Procurar** para selecionar o arquivo de certificado do servidor para o seu servidor de gerenciamento de chaves. Você pode escolher um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.

   O nome do arquivo é exibido na caixa de diálogo.

6. Clique em **Importar**.

   Os arquivos são carregados e validados.

Exportar certificados do servidor de gerenciamento de chaves no SANtricity System Manager

Você pode salvar um certificado para um servidor de gerenciamento de chaves na sua máquina local.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.
- Os certificados devem ser importados previamente.

Passos

1. Selecione **Configurações › Certificados**.
2. Selecione a guia **Gerenciamento de Chaves**.
3. Na tabela, selecione o certificado que deseja exportar e clique em **Export**.

   Uma caixa de diálogo Salvar é aberta.

4. Digite um nome de arquivo e clique em **Save**.

Perguntas frequentes sobre certificados assinados por CA e autoassinados para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

Por que a caixa de diálogo Não é possível acessar outro controlador aparece?

Ao executar determinadas operações relacionadas a certificados de CA (por exemplo, importar um certificado), você pode ver uma caixa de diálogo solicitando que aceite um certificado autoassinado para o segundo controlador.

Em arrays de storage com dois controladores (configurações duplex), esta caixa de diálogo pode aparecer se SANtricity System Manager não conseguir se comunicar com o segundo controlador ou se o seu navegador não aceitar o certificado em determinado momento da operação.

Se esta caixa de diálogo abrir, clique em **Aceitar certificado autoassinado** para prosseguir. Se outra caixa de diálogo solicitar uma senha, digite sua senha de Administrador usada para acessar System Manager.

Se esta caixa de diálogo aparecer novamente e você não conseguir concluir uma tarefa de certificado, tente um dos seguintes procedimentos:

- Use um navegador diferente para acessar este controlador, aceite o certificado e continue.
- Acesse o segundo controlador withSystem Manager, aceite o certificado autoassinado e, em seguida, retorne ao primeiro controlador e continue.

Como posso saber quais certificados precisam ser carregados no SANtricity System Manager para gerenciamento de chaves externas?

Para o gerenciamento de chaves externas, você importa dois tipos de certificados para autenticação entre o array de storage e o servidor de gerenciamento de chaves para que as duas entidades possam confiar uma na outra.

Um certificado de cliente valida os controladores do array de storage, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações do Key Management Interoperability Protocol (KMIP).

Para obter um certificado de cliente, você usa System Manager para concluir uma CSR para o array de storage. Você também pode gerar uma CSR externamente usando um par de chaves privada e pública.

Em seguida, você pode enviar o CSR para um servidor de gerenciamento de chaves e gerar um certificado de cliente a partir daí. Depois de obter um certificado de cliente, copie esse arquivo para o host onde você está acessando System Manager.

Um certificado de servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, permitindo que o array de storage confie em seu endereço IP. Recupere o arquivo de certificado do servidor de gerenciamento de chaves e, em seguida, copie esse arquivo para o host onde você está acessando System Manager.

O que preciso saber sobre a verificação de revogação de certificados?

SANtricity System Manager permite verificar certificados revogados usando um servidor Online Certificate Status Protocol (OCSP), em vez de enviar Certificate Revocation Lists (CRLs).

Certificados revogados não devem mais ser considerados confiáveis. Um certificado pode ser revogado por

diversos motivos; por exemplo, se a Certificate Authority (CA) emitiu o certificado indevidamente, uma chave privada foi comprometida ou a entidade identificada não cumpriu os requisitos da política.

Após estabelecer uma conexão com um servidor OCSP no System Manager, o array de storage realiza uma verificação de revogação sempre que se conecta a um AutoSupport server, servidor External Key Management Server (EKMS), servidor Lightweight Directory Access Protocol over SSL (LDAPS) ou servidor Syslog. O array de storage tenta validar os certificados desses servidores para garantir que não tenham sido revogados. O servidor então retorna um valor de "good", "revoked" ou "unknown" para esse certificado. Se o certificado estiver revogado ou se o array não conseguir contatar o servidor OCSP, a conexão é 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 quais tipos de servidores a verificação de revogação será habilitada?

O array de storage realiza a verificação de revogação sempre que se conecta a um AutoSupport server, External Key Management Server (EKMS), servidor Lightweight Directory Access Protocol over SSL (LDAPS) ou a um servidor Syslog.

Suporte

Obtenha suporte no SANtricity System Manager

A página de Suporte fornece acesso a recursos de suporte técnico.

Quais tarefas de suporte estão disponíveis?

Na seção Suporte, você pode visualizar contatos de suporte técnico, realizar diagnósticos, configurar AutoSupport, visualizar o registro de eventos e realizar atualizações de software.

Saiba mais:

- "AutoSupport visão geral do recurso"
- "Visão geral do log de eventos"
- "Visão geral do Upgrade Center"

Como faço para entrar em contato com o suporte técnico?

Na página principal, clique em **Support › Support Center › guia Support Resources**. As informações de contato do suporte técnico estão listadas no canto superior direito da interface.

Visualizar informações e diagnósticos

Visualize o perfil de um array de storage no SANtricity System Manager

O perfil do array de storage fornece uma descrição de todos os componentes e propriedades do array de storage.

Sobre esta tarefa

Você pode usar o perfil do array de storage como auxílio durante a recuperação ou como uma visão geral da configuração atual do array de storage. Você pode querer salvar uma cópia do perfil do array de storage no

cliente de gerenciamento e manter uma versão impressa do perfil do array de storage junto ao array de storage. Crie uma nova cópia do perfil do array de storage se sua configuração mudar.

Passos

1. Selecione o menu: guia Support [Support Center > Support Resources].
2. Desça até **Launch detailed storage array information** e selecione **Storage Array Profile**.

   O relatório aparece na sua tela.

Detalhes do campo

Seção	Descrição
Array de storage	Exibe todas as opções que você pode configurar e as opções estáticas do sistema para seu array de storage. Essas opções incluem o número de controladoras, gavetas de unidades, unidades, pools de discos, grupos de volume, volumes e hot spare; o número máximo de gavetas de unidades, unidades, Solid State Disks (SSDs) e volumes permitidos; o número de grupos de snapshot, imagens de snapshot, volumes de snapshot e grupos de consistência; informações sobre recursos; informações sobre versões de firmware; informações sobre o número de série do chassi; status do AutoSupport e informações de agendamento do AutoSupport; as configurações para coleta automática de dados de suporte e coleta de dados de suporte agendada; o World-Wide Identifier (WWID) do array de storage; e as configurações de verificação de mídia e cache.
Storage	Exibe uma lista de todos os dispositivos de armazenamento no array de storage. Dependendo da configuração do seu array de storage, a seção Armazenamento pode exibir estas subseções. • **Conjuntos de discos** — Exibe uma lista de todos os conjuntos de discos no array de storage. • **Grupos de Volumes** — Exibe uma lista de todos os grupos de volumes no array de storage. Volumes e capacidade livre são listados na ordem em que foram criados. • **Volumes** — Exibe uma lista de todos os volumes no array de storage. As informações listadas incluem o nome do volume, o status do volume, a capacidade, o nível RAID, o grupo de volume ou disk pool, o tipo de drive e detalhes adicionais. • **Volumes Ausentes** — Exibe uma lista de todos os volumes no array de storage que atualmente estão com status ausente. As informações listadas incluem o World Wide Identifier (WWID) para cada volume ausente.

Seção	Descrição
Serviços de cópia	Exibe uma lista de todos os serviços de cópia usados para o array de storage. Dependendo da configuração do seu array de storage, a seção Copy Services pode exibir estas subseções: • **Cópias de Volume** — Exibe uma lista de todos os pares de cópias no array de storage. As informações listadas incluem o número de cópias, os nomes dos pares de cópias, o status, o carimbo de data/hora de início e detalhes adicionais. • **Snapshot Groups** — Exibe uma lista de todos os snapshot groups no array de storage. • **Snapshot Images** — Mostra uma lista de todos os snapshots no array de storage. • **Snapshot Volumes** — Exibe uma lista de todos os volumes de snapshot no array de storage. • **Grupos de consistência** — Exibe uma lista de todos os grupos de consistência no array de storage. • **Volumes de membros** — Exibe uma lista de todos os volumes de membros do grupo de consistência na array de storage. • **Mirror Groups** — Exibe uma lista de todos os volumes espelhados. • **Capacidade Reservada** — Exibe uma lista de todos os volumes de capacidade reservada no array de storage.
Atribuições de hosts	Exibe uma lista de atribuições de host no array de storage. As informações listadas incluem o nome do volume, o número da unidade lógica (LUN), o ID do controlador, o nome do host ou o nome do cluster de hosts e o status do volume. Informações adicionais listadas incluem definições de topologia e definições de tipo de host.

Seção	Descrição
Hardware	Exibe uma lista de todo o hardware no array de storage. Dependendo da configuração do seu array de storage, a seção Hardware pode exibir estas subseções. • **Controladores** — Exibe uma lista de todos os controladores no array de storage e inclui a localização, o status e a configuração de cada controlador. Além disso, inclui informações sobre os canais das unidades, os canais dos hosts e as informações das portas Ethernet. • **Drives** — Exibe uma lista de todos os drives no array de storage. Os drives são listados em ordem de ID da prateleira, ID da gaveta e ID do slot. As informações listadas incluem o ID da prateleira, 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 drive. A seção Drive também inclui informações sobre o canal do drive, informações sobre a cobertura de hot spare e informações sobre a vida útil (somente para drives SSD). As informações sobre a vida útil incluem a porcentagem de endurance utilizada, que é a quantidade de dados gravados nos drives SSD até o momento, dividida pelo limite teórico total de gravação dos drives. • **Canais de Unidade** — Exibe informações para todos os canais de unidade no array de storage. As informações listadas incluem o status do canal, o status do link (se aplicável), contagens de unidades e contagens cumulativas de erros. • **Prateleiras** — Exibe informações de todas as prateleiras no array de storage. As informações listadas incluem tipos de unidades e informações de status para cada componente da prateleira. Os componentes da prateleira podem incluir baterias, transceptores Small Form-factor Pluggable (SFP), módulos de alimentação/ventoinha ou módulos de entrada/saída (IOM). A seção Hardware também exibe o identificador da chave de segurança, caso uma chave de segurança seja usada pelo array de storage.
Características	Exibe uma lista dos pacotes de recursos instalados e o número máximo permitido de grupos de snapshot, snapshots (legado) e volumes por host ou cluster de hosts. As informações na seção Recursos também incluem Drive Security; ou seja, se o array de storage está com a segurança habilitada ou desabilitada.

3. Para pesquisar o perfil do array de storage, digite um termo de pesquisa na caixa de texto **Localizar** e clique em **Localizar**.

   Todos os termos correspondentes são destacados. Para percorrer todos os resultados um por um, continue clicando em **Localizar**.

4. Para salvar o perfil do array de storage, clique em **Salvar**.

   O arquivo é salvo na pasta Downloads do seu navegador com o nome `storage-array-profile.txt`.

Visualize o inventário de software e firmware no SANtricity System Manager

O inventário de software e firmware lista as versões de firmware para cada componente em seu array de storage.

Sobre esta tarefa

Um array de storage é composto por diversos componentes, que podem incluir controladores, drives, gavetas e módulos de entrada/saída (IOMs). Cada um desses componentes contém firmware. Algumas versões de firmware dependem de outras versões de firmware. Para capturar informações sobre todas as versões de firmware em seu array de storage, visualize o inventário de software e firmware. O suporte técnico pode analisar o inventário de software e firmware para detectar quaisquer incompatibilidades de firmware.

Passos

1. Selecione o menu: guia Support [Support Center > Support Resources].
2. Desça até **Launch detailed storage array information** e, em seguida, selecione **Software and Firmware Inventory**.

   O relatório de inventário de software e firmware aparece na tela.

3. Para salvar o inventário de software e firmware, clique em **Salvar**.

   O arquivo é salvo na pasta Downloads do seu navegador com o nome de arquivo `firmware-inventory.txt`.

4. Siga as instruções fornecidas pelo suporte técnico para enviar o arquivo para eles.

Coletar dados de diagnóstico

Coletar dados de suporte manualmente no SANtricity System Manager

Você pode reunir diversos tipos de dados de inventário, status e desempenho do seu array de storage em um único arquivo. O suporte técnico pode usar o arquivo para solucionar problemas e realizar análises adicionais.

Sobre esta tarefa

> Se o recurso AutoSupport estiver ativado, você também pode coletar esses dados acessando a guia **AutoSupport** e selecionando **Enviar despacho de AutoSupport**.

Você só pode executar uma operação de coleta por vez. Se tentar iniciar outra operação, você receberá uma mensagem de erro.

> Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

Passos

1. Selecione menu: guia Suporte [Support Center > Diagnostics].
2. Selecione **Collect Support Data**.
3. Clique em **Coletar**.

O arquivo é salvo na pasta Downloads do seu navegador com o nome `support-data.7z`. Se sua estante contiver gavetas, os dados de diagnóstico dessa estante são arquivados em um arquivo zipado separado chamado `tray-component-state-capture.7z`.

4. Siga as instruções fornecidas pelo suporte técnico para enviar o arquivo para eles.

Coletar dados de configuração no SANtricity System Manager

Você pode salvar os dados de configuração RAID do controlador, incluindo todos os dados de grupos de volumes e pools de discos. Em seguida, você pode entrar em contato com o suporte técnico para obter assistência na restauração dos dados.

Sobre esta tarefa

Esta tarefa descreve como salvar o estado atual do banco de dados de configuração RAID. Esses dados são recuperados da localização de memória RPA do controlador.

> O recurso Coletar Dados de Configuração salva as mesmas informações que o comando da interface de linha de comando para `save storageArray dbmDatabase`.

Você só deve executar esta tarefa quando instruído por uma operação do Recovery Guru ou pelo suporte técnico.

Passos

1. Selecione menu: guia Suporte [Support Center > Diagnostics].
2. Selecione **Collect Configuration Data**.
3. Na caixa de diálogo, clique em **Collect**.

   O arquivo, `configurationData-<arrayName>-<dateTime>.7z`, está salvo na pasta Downloads do seu navegador.

4. Contate o suporte técnico para obter mais informações sobre como enviar o arquivo para eles e para carregar os dados de volta no sistema.

Recuperar arquivos de suporte à recuperação no SANtricity System Manager

O suporte técnico pode usar arquivos de suporte de recuperação para solucionar problemas. SANtricity System Manager salva esses arquivos automaticamente.

Antes de começar

O suporte técnico solicitou que você envie arquivos adicionais para troubleshooting.

Sobre esta tarefa

Os arquivos de suporte à recuperação incluem estes tipos de arquivos:

- Arquivos de dados de suporte
- Histórico do 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 Suporte [Support Center > Diagnostics].
2. Selecione **Recuperar arquivos de suporte à recuperação**.

   Uma caixa de diálogo lista todos os arquivos de suporte à recuperação que seu array de storage coletou. Para encontrar arquivos específicos, você pode classificar qualquer uma das colunas ou digitar caracteres na caixa **Filter**.

3. Selecione um arquivo e, em seguida, clique em **Download**.

   O arquivo é salvo na pasta Downloads do seu navegador.

4. Se você precisar salvar arquivos adicionais, repita a etapa anterior.
5. Clique em **Close**.
6. Siga as instruções fornecidas pelo suporte técnico para enviar o arquivo para eles.

Recuperar buffers de rastreamento no SANtricity System Manager

Você pode recuperar os buffers de rastreamento dos controladores e enviar o arquivo para suporte técnico para análise.

Sobre esta tarefa

O firmware utiliza os buffers de rastreamento para registrar o processamento, especialmente condições de exceção, que podem ser úteis para depuração. Você pode recuperar os buffers de rastreamento sem interromper a operação do array de storage e com impacto mínimo no desempenho.

Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

Passos

1. Selecione menu: guia Suporte [Support Center > Diagnostics].
2. Selecione **Retrieve Trace Buffers**.
3. Selecione a caixa de seleção ao lado de cada controlador para o qual deseja recuperar buffers de rastreamento.

   Você pode selecionar um ou ambos os controladores. Se a mensagem de status do controlador à direita de uma caixa de seleção for Failed ou Disabled, a caixa de seleção estará desativada.

4. Clique em **Yes**.

   O arquivo é salvo na pasta Downloads do seu navegador com o nome de arquivo `trace-buffers.7z`.

5. Siga as instruções fornecidas pelo suporte técnico para enviar o arquivo para eles.

Coletar estatísticas do caminho de E/S no SANtricity System Manager

Você pode salvar o arquivo de estatísticas do caminho de E/S e enviá-lo para suporte técnico para análise.

Sobre esta tarefa

O suporte técnico utiliza as estatísticas do caminho de I/O para ajudar a diagnosticar problemas de desempenho. Problemas de desempenho de aplicativos podem ser causados por utilização de memória, utilização de CPU, latência de rede, latência de I/O ou outros problemas. As estatísticas do caminho de I/O são coletadas automaticamente durante a coleta de dados de suporte ou você pode coletá-las manualmente. Além disso, se você tiver AutoSupport ativado, as estatísticas do caminho de I/O são coletadas e enviadas automaticamente para o suporte técnico.

Os contadores das estatísticas do caminho de I/O são reinicializados após você confirmar que deseja coletar as estatísticas do caminho de I/O. Os contadores são reinicializados mesmo se você cancelar a operação posteriormente. Os contadores também são reinicializados quando o controlador é reinicializado (reiniciado).

Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

Passos

1. Selecione menu: guia Suporte [Support Center > Diagnostics].
2. Selecione **Collect I/O Path Statistics**.
3. Confirme que deseja realizar a operação digitando `collect`, e em seguida clique em **Coletar**.

   O arquivo é salvo na pasta Downloads do seu navegador com o nome de arquivo `io-path-statistics.7z`.

4. Siga as instruções fornecidas pelo suporte técnico para enviar o arquivo para eles.

Recuperar imagem de integridade no SANtricity System Manager

Você pode visualizar uma imagem de integridade 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 detecta determinados erros. Após a geração de uma imagem de integridade, o controlador que apresentou o erro é reinicializado e um evento é registrado no log de eventos.

Se você tem o AutoSupport ativado, a imagem de integridade é enviada automaticamente para o suporte técnico. Se você não tem o AutoSupport ativado, é necessário entrar em contato com o suporte técnico para obter instruções sobre como recuperar a imagem de integridade e enviá-la para análise.

Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

Passos

1. Selecione menu: guia Suporte [Support Center > Diagnostics].
2. Selecione **Retrieve Health Image**.

   Você pode consultar a seção de detalhes para ver o tamanho da imagem de saúde antes de baixar o arquivo.

3. Clique em **Coletar**.

O arquivo é salvo na pasta Downloads do seu navegador com o nome `health-image.7z`.

4. Siga as instruções fornecidas pelo suporte técnico para enviar o arquivo para eles.

Adote medidas de recuperação

Visualize o registro de setores ilegíveis no SANtricity System Manager

Você pode salvar o registro de setores ilegíveis e enviar o arquivo para o suporte técnico para análise.

Sobre esta tarefa

O registro de setores ilegíveis contém informações detalhadas sobre setores ilegíveis causados por unidades que reportam erros de mídia irrecuperáveis. Setores ilegíveis são detectados durante operações normais de E/S e durante operações de modificação, como reconstruções. Quando setores ilegíveis são detectados em um array de storage, um alerta Needs Attention é exibido para o array de storage. O Recovery Guru distingue qual condição de setor ilegível requer atenção. Quaisquer dados contidos em um setor ilegível não podem ser recuperados e devem ser considerados perdidos.

O registro de setores ilegíveis pode armazenar até 1.000 setores ilegíveis. Quando o registro de setores ilegíveis atinge 1.000 entradas, as seguintes condições se aplicam:

- Se novos setores ilegíveis forem detectados durante a reconstrução, a reconstrução falha e nenhuma entrada é registrada.
- Para novos setores ilegíveis detectados 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 overflow.

> **Possível perda de dados** — A recuperação de setores ilegíveis é um procedimento complexo que pode envolver diversos métodos diferentes. Execute esta operação somente quando instruído a fazê-lo pelo suporte técnico.

Passos

1. Selecione menu: guia Suporte [Support Center > Diagnostics].
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 caracteres na caixa **Filter**.

   b. Clique em **Salvar**.

   O arquivo é salvo na pasta Downloads do seu navegador com o nome `unreadable-sectors.txt`.

4. Se o suporte técnico instruir você a limpar o registro 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 **Limpar** e confirme que você deseja realizar a operação.

Reative as portas de unidade no SANtricity System Manager

Você pode indicar ao controlador que uma ação corretiva foi tomada para recuperar de uma condição de fiação incorreta.

Passos

1. Selecione menu: guia Suporte [Support Center > Diagnostics].
2. Selecione **Re-enable Drive Ports** e confirme que deseja realizar a operação.

   Essa opção aparece somente quando o array de storage tem portas de unidade desativadas.

   O controlador reativa quaisquer portas SAS que tenham sido desativadas quando uma falha de fiação foi detectada.

Limpar o modo de recuperação no software SANtricity

Após restaurar a configuração do array de storage, use a operação Limpar Modo de Recuperação para retomar a E/S no array de storage e retornar ao funcionamento normal.

Antes de começar

- Se você deseja retornar o array de storage a uma configuração anterior, é necessário restaurar a configuração a partir do backup antes de limpar o modo de recuperação.
- Você deve realizar verificações de validação ou consultar o suporte técnico para garantir que a restauração foi bem-sucedida. Após determinar que a restauração foi bem-sucedida, o modo de recuperação pode ser desativado.

Sobre esta tarefa

O array de storage contém um banco de dados de configuração que inclui um registro de sua configuração lógica (pools, grupos de volumes, volumes e assim por diante). Se você limpar intencionalmente a configuração do array de storage ou se o banco de dados de configuração for corrompido, o array de storage entra no modo de recuperação. O modo de recuperação interrompe a E/S e congela o banco de dados de configuração, o que lhe dá tempo para fazer uma das seguintes opções:

- Restaure a configuração a partir do backup automático que está armazenado nos dispositivos de memória flash do controlador. Você deve entrar em contato com o suporte técnico para fazer isso.
- Restaure a configuração de uma operação anterior de Save Configuration Database. As operações de Save Configuration Database são realizadas por meio da interface de linha de comando (CLI).
- Reconfigure o array de storage do zero.

Após a configuração do array de storage ter sido restaurada ou redefinida e você ter verificado que tudo está funcionando corretamente, você deve limpar manualmente o modo de recuperação.

Não é possível cancelar a operação Clear Recovery Mode depois de iniciada. Limpar o recovery mode pode levar muito tempo. Execute esta operação somente quando for instruído a fazê-lo pelo suporte técnico.

Passos

1. Selecione menu: guia Suporte [Support Center > Diagnostics].
2. Selecione **Limpar Modo de Recuperação** e confirme que deseja realizar esta operação.

   Essa opção aparece somente se o array de storage estiver em modo de recuperação.

Gerenciar AutoSupport

Saiba mais sobre AutoSupport para E-Series

O recurso AutoSupport monitora a integridade de um array de storage e envia despachos automáticos para suporte técnico.

O suporte técnico utiliza os dados do AutoSupport de forma reativa para agilizar o diagnóstico e a resolução de problemas dos clientes e de forma proativa para detectar e evitar problemas potenciais.

AutoSupport data inclui informações sobre a configuração, o status, o desempenho e os eventos do sistema de um array de storage. Os dados do AutoSupport não contêm quaisquer dados de usuário. Os despachos podem ser enviados imediatamente ou de acordo com uma programação (diária e semanal).

Principais benefícios

Alguns dos principais benefícios do recurso AutoSupport incluem:

- Tempos de resolução de casos acelerados
- Monitoramento sofisticado para gerenciamento de incidentes mais rápido
- 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
- Alertas não intrusivos para notificá-lo sobre um problema e fornecer informações para que o suporte técnico tome medidas corretivas
- AutoSupport analysis tools que monitoram despachos em busca de problemas de configuração conhecidos

Recursos individuais do AutoSupport

O recurso AutoSupport é composto por três funcionalidades individuais que você ativa separadamente.

- **Básico AutoSupport** — Permite que seu array de storage colete e envie dados automaticamente para o suporte técnico.
- **AutoSupport OnDemand** — Permite que o suporte técnico solicite a retransmissão de um despacho anterior do AutoSupport quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir do array de storage, não do servidor AutoSupport. O array de storage verifica periodicamente com o servidor AutoSupport se há alguma solicitação de retransmissão pendente e responde de acordo.

- **Diagnóstico Remoto** — Permite que o suporte técnico solicite um novo, atualizado AutoSupport dispatch quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir do array de storage, não do AutoSupport server. O array de storage verifica periodicamente com o AutoSupport server se há novas solicitações pendentes e responde de acordo.

Diferença entre AutoSupport e Coletar Dados de Suporte

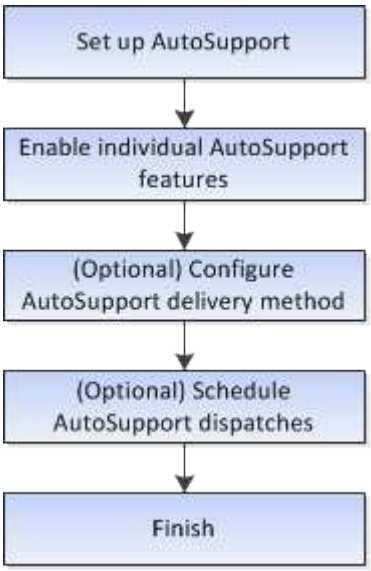
Existem dois métodos de coleta de dados de suporte no array de storage:

- **AutoSupport feature** — 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 prevenir problemas antes que eles ocorram. O recurso AutoSupport agiliza a resolução 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 para usar.

Configurar AutoSupport no SANtricity System Manager

No SANtricity System Manager, você configura o recurso AutoSupport seguindo estes passos.



Ative ou desative os recursos do AutoSupport no SANtricity System Manager

Você ativa o recurso AutoSupport e os recursos individuais AutoSupport durante a configuração inicial ou pode ativá-los ou desativá-los posteriormente.

Antes de começar

Se você deseja habilitar AutoSupport OnDemand ou 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 mantê-lo ativado. Habilitar o recurso AutoSupport pode acelerar significativamente a determinação e resolução de problemas caso ocorra algum problema em seu array de storage.

O recurso AutoSupport é composto por três funcionalidades individuais que você ativa separadamente.

- **Básico AutoSupport** — Permite que seu array de storage colete e envie dados automaticamente para o suporte técnico.
- **AutoSupport OnDemand** — Permite que o suporte técnico solicite a retransmissão de um despacho anterior do AutoSupport quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir do array de storage, não do servidor AutoSupport. O array de storage verifica periodicamente com o servidor AutoSupport se há alguma solicitação de retransmissão pendente e responde de acordo.
- **Diagnóstico Remoto** — Permite que o suporte técnico solicite um novo, atualizado AutoSupport dispatch quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir do array de storage, não do AutoSupport server. O array de storage verifica periodicamente com o AutoSupport server se há novas solicitações pendentes e responde de acordo.

Passos

1. Selecione o menu:Suporte [Support Center > AutoSupport] tab.
2. Selecione **Ativar/Desativar AutoSupport Features**.
3. Selecione as caixas de seleção ao lado dos recursos do AutoSupport que você deseja ativar.

   As funcionalidades dependem umas das outras, como indicado pelo recuo dos itens na caixa de diálogo. Por exemplo, você deve habilitar AutoSupport OnDemand antes de poder habilitar Remote Diagnostics.

4. Clique em **Salvar**.

   Se você desativar AutoSupport, uma notificação aparecerá na página inicial. Você pode descartar a notificação clicando em **Ignorar**.

Configure o método de entrega do AutoSupport no SANtricity System Manager

O recurso AutoSupport oferece suporte aos protocolos HTTPS e SMTP para o envio de despachos ao suporte técnico.

Antes de começar

- O recurso AutoSupport deve estar ativado. Você pode verificar se ele está ativado na página AutoSupport.
- Um servidor DNS deve ser instalado e configurado na sua rede. O endereço do servidor DNS deve ser configurado no System Manager (essa tarefa está disponível na página Hardware).

Sobre esta tarefa

Analise os diferentes protocolos:

- **HTTPS** — Permite que você se conecte diretamente ao servidor de suporte técnico de destino usando HTTPS. Se você quiser habilitar AutoSupport OnDemand ou Diagnóstico Remoto, o método de entrega do AutoSupport deve ser definido como HTTPS.
- **E-mail** — Permite usar um servidor de e-mail como método de entrega para o envio de despachos AutoSupport.

Diferenças entre os métodos HTTPS e Email. O método de entrega por Email, que utiliza SMTP, apresenta algumas diferenças importantes em relação ao método de entrega HTTPS. Primeiro, o tamanho dos despachos para o método Email é limitado a 5MB, o que significa que algumas coletas de dados do ASUP não serão despachadas. Segundo, o recurso AutoSupport OnDemand está disponível apenas no método de entrega HTTPS.

Passos

1. Selecione o menu:Suporte [Support Center > AutoSupport] tab.
2. Selecione **Configurar AutoSupport Delivery Method**.

   Uma caixa de diálogo aparece, que lista os métodos de entrega do despacho.

3. Selecione o método de entrega desejado e, em seguida, selecione os parâmetros para esse método de entrega. Faça um dos seguintes procedimentos:
   - Se você selecionou HTTPS, selecione um dos seguintes parâmetros de entrega:
     - **Diretamente** — Este parâmetro de entrega é a seleção padrão. Escolher esta opção permite que você se conecte diretamente ao sistema de suporte técnico de destino usando o protocolo HTTPS.
     - **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 script de autoconfiguração de proxy (PAC)** — Especifique o local de um arquivo de script de autoconfiguração 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 Email, insira as seguintes informações:
     - O endereço do servidor de e-mail como um domínio totalmente qualificado, endereço IPv4 ou endereço IPv6.
     - O endereço de e-mail que aparece no campo De do e-mail de despacho do AutoSupport.
     - **Opcional; caso deseje realizar um teste de configuração**: O endereço de e-mail para onde será enviada uma confirmação quando o sistema AutoSupport receber o despacho de teste.
     - Se desejar criptografar as mensagens, selecione **SMTPS** ou **STARTTLS** para o tipo de criptografia e, em seguida, selecione o número da porta para as mensagens criptografadas. Caso contrário, selecione **None**.
     - Caso necessário, insira um nome de usuário e uma senha para autenticação com o remetente de saída e o servidor de e-mail.
4. Se você possui um firewall que bloqueia o envio dessas mensagens ASUP, adicione o seguinte URL à sua whitelist: `https://support.netapp.com/put/AsupPut/`
5. Clique em **Testar configuração** para testar a conexão com o servidor de suporte técnico usando os parâmetros de entrega especificados. Se você habilitou o recurso AutoSupport On-Demand, o sistema também testará a conexão para entrega de despacho AutoSupport OnDemand.

   Se o teste de configuração falhar, verifique suas configurações e execute o teste novamente. Se o teste continuar falhando, entre em contato com o suporte técnico.

6. Clique em **Salvar**.

Agende despachos do AutoSupport no SANtricity System Manager

SANtricity System Manager cria automaticamente uma programação padrão para os despachos do AutoSupport. Se preferir, você pode especificar sua própria programação.

Antes de começar

O recurso AutoSupport deve estar ativado. Você pode verificar se ele está ativado na página AutoSupport.

Sobre esta tarefa

- **Horário diário** — Os despachos diários são coletados e enviados todos os dias durante o intervalo de tempo que você especificar. System Manager seleciona um horário aleatório dentro desse intervalo. Todos os horários estão em Tempo Universal Coordenado (UTC), que pode ser diferente do horário local do array de storage. Você deve converter o horário local do seu array de storage para UTC.
- **Dia da semana** — Os despachos semanais são coletados e enviados uma vez por semana. System Manager seleciona um dia aleatório dentre os dias que você especificar. Desmarque os dias nos quais você não deseja permitir que ocorra um despacho semanal. System Manager seleciona um dia aleatório dentre os dias que você permitir.
- **Horário semanal** — Os despachos semanais são coletados e enviados uma vez por semana durante o intervalo de tempo que você especificar. System Manager seleciona um horário aleatório dentro desse intervalo. Todos os horários estão em Tempo Universal Coordenado (UTC), que pode ser diferente do horário local do array de storage. Você deve converter o horário local do array de storage para UTC.

Passos

1. Selecione o menu:Suporte [Support Center > AutoSupport] tab.
2. Selecione **Agendar AutoSupport Dispatches**.

   O assistente de agendamento de despachos do AutoSupport é exibido.

3. Siga as etapas no assistente.

Enviar despachos do AutoSupport no SANtricity System Manager

SANtricity System Manager permite enviar despachos do AutoSupport para o suporte técnico, sem precisar esperar por um despacho agendado.

Antes de começar

O recurso AutoSupport deve estar ativado. Você pode verificar se ele está ativado na página AutoSupport.

Sobre esta tarefa

Esta operação coleta dados de suporte e os envia automaticamente para o suporte técnico, para que eles possam solucionar problemas.

Passos

1. Selecione o menu:Suporte [Support Center > AutoSupport] tab.
2. Selecione **Enviar AutoSupport Dispatch**.

   A caixa de diálogo Enviar AutoSupport Dispatch é exibida.

3. Confirme a operação selecionando **Send**.

Visualizar o status do AutoSupport no SANtricity System Manager

A página AutoSupport mostra se o recurso AutoSupport e os recursos individuais AutoSupport estão ativados no momento.

Passos

1. Selecione o menu:Suporte [Support Center > AutoSupport] tab.
2. Observe o lado direito da página, logo abaixo das abas, para verificar se o recurso básico AutoSupport está ativado.
3. Passe o cursor sobre o ponto de interrogação para ver se as funcionalidades individuais do AutoSupport estão ativadas.

Visualizar AutoSupport log no SANtricity System Manager

O AutoSupport log fornece informações sobre status, histórico de despachos e erros encontrados durante a entrega dos despachos de AutoSupport.

Sobre esta tarefa

Podem existir vários arquivos de log. 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 arquivos de log, você pode optar por visualizar o log mais recente ou um log anterior.

- **Registro atual** — Exibe uma lista dos eventos capturados mais recentes.
- **Registro arquivado** — Exibe uma lista de eventos anteriores.

Passos

1. Selecione o menu:Suporte [Support Center > AutoSupport] tab.
2. Selecione **Exibir AutoSupport Log**.

   Aparece uma caixa de diálogo, que lista o AutoSupport log atual.

3. Se você quiser ver registros anteriores do AutoSupport, selecione o botão de opção **Arquivado** e, em seguida, selecione um registro na lista suspensa **Selecionar log do AutoSupport**.

   A opção Arquivado só aparece se existirem registros arquivados no array de storage.

   O AutoSupport log selecionado aparece na caixa de diálogo.

4. **Opcional:** Para pesquisar o log do AutoSupport, digite um termo na caixa **Localizar** e clique em **Localizar**.

   Clique em **Localizar** novamente para pesquisar outras ocorrências do termo.

Habilite a janela de manutenção do AutoSupport no SANtricity System Manager

Habilite a janela de manutenção do AutoSupport para suprimir a criação automática de chamados em eventos de erro. No modo de operação normal, o array de storage usa o AutoSupport para abrir um chamado com o suporte se houver algum problema.

Passos

1. Selecione o menu:Suporte [Support Center > AutoSupport] tab.
2. Selecione **Ativar AutoSupport Maintenance window**.
3. Insira o endereço de e-mail para receber uma confirmação de que a solicitação de janela de manutenção foi processada.

   Dependendo da sua configuração, você pode inserir até cinco endereços de e-mail. Se quiser adicionar mais de um endereço, selecione **Adicionar outro e-mail** para abrir outro campo.

4. Especifique a duração (em horas) para habilitar a janela de manutenção.

   A duração máxima suportada é de 72 horas.

5. Clique em **Yes**.

   AutoSupport a criação automática de tickets em eventos de erro está temporariamente suprimida pela janela de duração especificada.

Depois que você terminar

A janela de manutenção não começa até que a solicitação do array de storage seja processada pelos servidores AutoSupport. Aguarde até receber um e-mail de confirmação antes de realizar qualquer atividade de manutenção no seu array de storage.

Desative a janela de manutenção do AutoSupport no SANtricity System Manager

Desative a janela de manutenção do AutoSupport para permitir a criação automática de chamados em eventos de erro. Quando a janela de manutenção do AutoSupport estiver desativada, o array de storage usará o AutoSupport para abrir um chamado com o suporte se houver um problema.

Passos

1. Selecione o menu:Suporte [Support Center > AutoSupport] tab.
2. Selecione **Desativar AutoSupport Maintenance window**.
3. Insira o endereço de e-mail para receber uma confirmação de que a solicitação para desativar a janela de manutenção foi processada.

   Dependendo da sua configuração, você pode inserir até cinco endereços de e-mail. Se quiser adicionar mais de um endereço, selecione **Adicionar outro e-mail** para abrir outro campo.

4. Clique em **Yes**.

   AutoSupport a criação automática de tickets em eventos de erro está ativada.

Depois que você terminar

A janela de manutenção não terminará até que a solicitação do array de storage tenha sido processada pelos servidores AutoSupport. Aguarde até receber um e-mail de confirmação antes de prosseguir.

Ver eventos

Saiba mais sobre o registro de eventos no software SANtricity

O registro de eventos fornece um histórico dos eventos que ocorreram no array de storage, o que auxilia o suporte técnico na resolução de problemas que levaram a falhas.

Você pode usar o registro de eventos como uma ferramenta de diagnóstico complementar ao Recovery Guru para rastrear eventos do array de storage. Sempre consulte o Recovery Guru primeiro ao tentar se recuperar de falhas de componentes no array de storage.

Categorias de eventos

Os eventos no registro de eventos são categorizados com diferentes status. Eventos que exigem ação têm os seguintes status:

- Crítico
- Aviso

Eventos que são informativos e não exigem nenhuma ação imediata são os seguintes:

- Informativo

Eventos críticos

Eventos críticos indicam um problema com o array de storage. 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 da prateleira não for conhecido no momento do evento, o ID da prateleira será listado como "Shelf unknown."

Ao receber um evento crítico, consulte o procedimento do Recovery Guru para obter uma descrição detalhada do evento crítico. Conclua o procedimento do Recovery Guru para corrigir o evento crítico. Para corrigir determinados eventos críticos, pode ser necessário entrar em contato com o suporte técnico.

Visualize eventos usando o registro de eventos no SANtricity System Manager

Você pode visualizar o registro de eventos, que fornece um histórico de eventos que ocorreram no array de storage.

Passos

1. Selecione o menu: suporte [Registro de eventos].

   A página de log de eventos é exibida.

Detalhes da página

Item	Descrição
Ver todos os campos	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 de colunas.	Permite selecionar outras colunas para visualizar. Outras colunas fornecem informações adicionais sobre o evento.
Caixas de seleção	Permite selecionar os eventos a serem salvos. A caixa de seleção no cabeçalho da tabela seleciona todos os eventos.
Coluna Data/Hora	A data e o carimbo de hora do evento, de acordo com o relógio do controlador. Inicialmente, o registro de eventos classifica os eventos com base no número de sequência. Normalmente, essa sequência corresponde à data e hora. No entanto, os dois relógios do controlador no array de storage podem estar dessincronizados. Nesse caso, algumas inconsistências percebidas podem aparecer no registro de eventos em relação aos eventos e à data e hora exibidas.
Coluna de prioridade	Estes valores de prioridade existem: • **Crítico** — Existe um problema com o array de storage. No entanto, se você agir imediatamente, poderá evitar perder o 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. • **Aviso** — Ocorreu um erro que degradou o desempenho e a capacidade do array de storage de recuperar-se de outro erro. • **Informativo** — Informações não críticas relacionadas ao array de storage.
Coluna Tipo de componente	O componente afetado pelo evento. O componente pode ser hardware, como um drive ou um controlador, ou pode ser software, como firmware do controlador.
Coluna de localização do componente	A localização física do componente no array de storage.

Item	Descrição
Coluna Description	Uma descrição do evento. **Exemplo** — `Drive write failure - retries exhausted`
Coluna Número de sequência	Um número de 64 bits que identifica exclusivamente uma entrada de log específica para um array de storage. Esse número é incrementado em um a cada nova entrada de log de eventos. Para exibir essa informação, clique no ícone **Selecionar colunas**.
Coluna Event Type	Um número de 4 dígitos que identifica cada tipo de evento registrado. Para exibir essas informações, clique no ícone **Selecionar colunas**.
Coluna de códigos específicos do evento	Essas informações são utilizadas pelo suporte técnico. Para exibir essas informações, clique no ícone **Selecionar colunas**.
Coluna Categoria de Evento	• **Falha** – Um componente no array de storage apresentou falha; por exemplo, falha na drive ou falha na bateria. • **Alteração de estado** – Um elemento do array de storage que teve seu estado alterado; por exemplo, um volume passou para o status Optimal ou um controlador passou para o status Offline. • **Interno** – Operações internas do controlador que não exigem ação do usuário; por exemplo, o controlador concluiu start-of-day. • **Comando** – Um comando que foi emitido para o array de storage; por exemplo, um hot spare foi atribuído. • **Erro** – Foi detectada uma condição de erro no array de storage; por exemplo, um controlador não consegue sincronizar e limpar o cache, ou um erro de redundância é detectado no array de storage. • **Geral** – Qualquer evento que não se encaixe bem em nenhuma outra categoria. Para exibir essas informações, clique no ícone **Select columns**.
Coluna Logged By	O nome do controlador que registrou o evento. Para exibir essas informações, clique no ícone **Select columns**.

2. Para recuperar novos eventos do array de storage, clique em **Refresh**.

   Pode levar alguns minutos para que um evento seja registrado e se torne visível na página Event Log.

3. Para salvar o registro de eventos em um arquivo:
   a. Selecione 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 seu navegador com o nome `major-event-log-timestamp.log`.

4. Para limpar eventos do registro de eventos:

   O registro de eventos armazena aproximadamente 8.000 eventos antes de substituir um evento por um novo. Se você quiser manter os eventos, pode salvá-los e removê-los do registro de eventos.

   a. Primeiro, salve o log de eventos.
   b. Clique em **Limpar tudo** e confirme que deseja realizar a operação.

Gerenciar atualizações

Saiba mais sobre como atualizar o software SANtricity

Utilize o Upgrade Center para baixar o software e firmware mais recentes e para atualizar seus controladores e unidades.

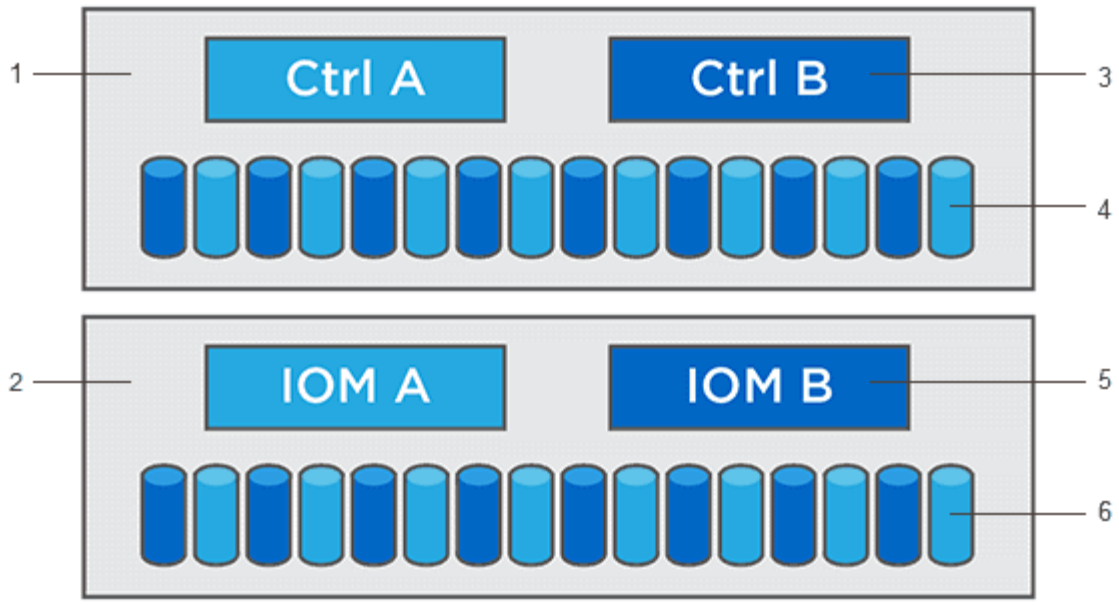
Visão geral da upgrade do controlador

Você pode atualizar o software e firmware do seu array de storage para obter todos os recursos mais recentes e correções de bugs.

Componentes incluídos na atualização do controlador do OS

Diversos componentes do array de storage contêm software ou hardware que você pode querer atualizar ocasionalmente.

- **Software de gerenciamento** — System Manager é o software que gerencia o array de storage.
- **Controller firmware** — O firmware do controlador gerencia a E/S entre hosts e volumes.
- **Controller NVSRAM** — O Controller NVSRAM é um arquivo de controlador que especifica as configurações padrão para os controladores.
- **IOM firmware** — O firmware do módulo de E/S (IOM) gerencia a conexão entre um controlador e um compartimento de unidades. Ele também monitora o status dos componentes.
- **Software supervisor** — O software supervisor é a máquina virtual em um controlador na qual o software é executado.



[1] Prateleira do controlador; [2] Prateleira da unidade; [3] Software, firmware do controlador, NVSRAM do controlador, software supervisor; [4] firmware da unidade; [5] firmware do IOM; [6] firmware da unidade

Você pode visualizar suas versões atuais de software e firmware na caixa de diálogo Inventário de Software e Firmware. Acesse o **suporte › Upgrade Center** e clique no link para **Software e Firmware Inventory**.

Como parte do processo de upgrade, o driver multipath/failover e/ou o driver HBA do host também pode precisar ser atualizado para que o host possa interagir corretamente com os controladores. Para determinar se este é o caso, consulte a "Ferramenta de Matriz de Interoperabilidade".

Quando interromper E/S

Se o seu array de storage contiver dois controladores e você tiver um driver multipath instalado, o array de storage poderá continuar processando E/S enquanto a atualização ocorre. Durante a atualização, o controlador A transfere todos os seus volumes para o controlador B, atualiza, retoma seus volumes e todos os volumes do controlador B e, em seguida, atualiza o controlador B.

Verificação de integridade pré-upgrade

Uma verificação de integridade pré-atualização é executada como parte do processo de upgrade. A verificação de integridade pré-atualização avalia todos os componentes do array de storage para garantir que o upgrade possa prosseguir. As seguintes condições podem impedir o upgrade:

- Unidades atribuídas com falha
- Hot spares em uso
- Grupos de volume incompletos
- Operações exclusivas em andamento
- Volumes ausentes
- Controlador em estado não ideal
- Número excessivo de eventos de log de eventos
- Falha na validação do banco de dados de configuração

- Unidades com versões antigas do DACstore

Você também pode executar a verificação de integridade separadamente, sem realizar um upgrade.

Visão geral do upgrade da unidade

O firmware da unidade controla as características operacionais de baixo nível de uma unidade. Periodicamente, os fabricantes de unidades lançam atualizações de firmware para adicionar novos recursos, melhorar o desempenho e corrigir defeitos.

Upgrades de firmware da unidade online e offline

Existem dois tipos de upgrade do formware da unidade: online e offline.

Online

Durante uma atualização online, as unidades são atualizadas sequencialmente, uma de cada vez. O array de storage continua processando E/S enquanto a atualização ocorre. Você não precisa interromper a E/S. Se uma unidade puder fazer uma atualização online, o método online será usado automaticamente.

As unidades que podem fazer um upgrade online incluem o seguinte:

- Drives em um pool Ótimo
- Unidades em um grupo de volume redundante ideal (RAID 1, RAID 5 e RAID 6)
- Unidades não atribuídas
- Unidades hot spare de reserva

Fazer um upgrade do formware da unidade online pode levar várias horas, expondo o array de storage a possíveis falhas de volume. A falha de volume pode ocorrer nesses casos:

- Em um grupo de volume RAID 1 ou RAID 5, uma unidade falha enquanto outra unidade no grupo de volume está sendo atualizada.
- Em um pool ou grupo de volume RAID 6, duas unidades falham enquanto uma unidade diferente no pool ou grupo de volume está sendo atualizada.

Offline (paralelo)

Durante uma atualização offline, todas as unidades do mesmo tipo de unidade são atualizadas ao mesmo tempo. Esse método requer a interrupção da atividade de E/S nos volumes associados às unidades selecionadas. Como várias unidades podem ser atualizadas simultaneamente (em paralelo), o tempo total de inatividade é significativamente reduzido. Se uma unidade só puder fazer uma atualização offline, o método offline será utilizado 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 volume não otimizados
- Unidades no cache SSD

Compatibilidade

Cada arquivo de firmware da unidade contém informações sobre o tipo de unidade na qual o firmware é

executado. Você pode baixar o arquivo de firmware especificado apenas para uma unidade compatível. System Manager verifica automaticamente a compatibilidade durante o processo de upgrade.

Atualize o software e o firmware no SANtricity System Manager

Você pode atualizar o software do seu array de storage e, opcionalmente, o firmware do IOM e a memória estática de acesso aleatório não volátil (NVSRAM) para garantir que tenha todos os recursos e correções de bugs mais recentes.

Antes de começar

- Você sabe se deseja atualizar o firmware do seu IOM.

  Normalmente, você deve atualizar todos os componentes ao mesmo tempo. No entanto, você pode optar por não atualizar o firmware do IOM se não quiser atualizá-lo como parte da atualização do software SANtricity OS ou se o suporte técnico tiver instruído você a fazer o downgrade do firmware do IOM (você só pode fazer o downgrade do firmware usando a interface de linha de comando).

- Você sabe se deseja atualizar o arquivo NVSRAM do controlador.

  Normalmente, você deve atualizar todos os componentes ao mesmo tempo. No entanto, você pode optar por não atualizar o arquivo NVSRAM do controlador se o seu arquivo tiver sido modificado ou for uma versão personalizada e você não quiser sobrescrevê-lo.

- Você sabe se deseja ativar o upgrade do sistema operacional agora ou mais tarde.

  Os motivos para ativar mais tarde podem incluir:

  - **Horário do dia** — A ativação do software e firmware pode demorar bastante, então talvez seja melhor esperar até que as cargas de E/S estejam mais leves. Os controladores fazem failover durante a ativação, portanto o desempenho pode ser inferior ao normal até que a atualização seja concluída.
  - **Tipo de pacote** — Você pode querer testar o novo software e firmware em um array de storage antes de atualizar os arquivos em outros arrays de storage.

- Você sabe se deseja migrar de unidades não seguras ou unidades com segurança interna para usar um servidor de gerenciamento de chaves externo (KMS) para segurança da unidade.
- Você sabe se deseja usar controle de acesso baseado em funções em seu array de storage.

Sobre esta tarefa

Você pode optar por atualizar apenas o arquivo de software do sistema operacional, 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 ao array de storage** — Não faça alterações no array de storage enquanto a atualização estiver em andamento. Mantenha a alimentação do array de storage.

Passos

1. Se o seu array de storage contiver apenas um controlador ou se você não tiver um driver multipath instalado, interrompa a atividade de E/S para o array de storage para evitar erros de aplicativo. Se o seu array de storage tiver dois controladores e você tiver um driver multipath instalado, não é necessário interromper a atividade de E/S.

2. Selecione o menu: suporte [Upgrade Center].
3. Faça o download do novo arquivo do site de suporte para o seu cliente de gerenciamento.

   a. Clique em **NetApp Support** para acessar o site de suporte.

   b. No site de suporte, clique na guia **Downloads** e, em seguida, selecione **Downloads**.

   c. Selecione **E-Series SANtricity OS Controller Software**.

   d. Siga as instruções restantes.

   > O firmware assinado digitalmente é necessário na versão 8.42 e superiores. Se você tentar baixar firmware não assinado, um erro será exibido e o download será interrompido.

4. Se você NÃO deseja atualizar o firmware do IOM neste momento, clique em **Suspender sincronização automática do IOM**.

   Se você tiver um array de storage com um único controlador, o firmware do IOM não será atualizado.

5. Em SANtricity OS Software upgrade, clique em **Begin Upgrade**.

   A caixa de diálogo Atualizar o software do sistema operacional SANtricity é exibida.

6. Selecione um ou mais arquivos para iniciar o processo de upgrade:

   a. Selecione o arquivo do software SANtricity OS clicando em **Procurar** e navegando até o arquivo do software que você baixou do site de suporte.

   b. Selecione o arquivo NVSRAM do controlador clicando em **Procurar** e navegando até o arquivo NVSRAM que você baixou do site de suporte. Os arquivos NVSRAM do controlador têm um nome de arquivo semelhante a `N2800-830000-000.dlp`.

      Essas ações ocorrem:

      - Por padrão, apenas os arquivos compatíveis com a configuração atual do array de storage são exibidos.
      - Ao selecionar um arquivo para upgrade, o nome e o tamanho do arquivo aparecem.

7. **Opcional:** Se você selecionou um arquivo de software SANtricity OS para upgrade, pode transferir os arquivos para o controlador sem ativá-los selecionando a caixa de seleção **Transferir arquivos agora, mas não fazer upgrade (ativar upgrade depois)**.
8. Clique em **Iniciar** e confirme que deseja realizar a operação.

   Você pode cancelar a operação durante a verificação de integridade pré-upgrade, 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 seu navegador com o nome `drive_upgrade_log-timestamp.txt`.

Depois que você terminar

- Verifique se todos os componentes aparecem na página de Hardware.
- Verifique as novas versões de software e firmware consultando a caixa de diálogo Inventário de Software e Firmware (acesse o **Support › Upgrade Center** e clique no link para **Software and Firmware**

Inventory).

- Se você atualizou a NVSRAM do controlador, todas as configurações personalizadas que você aplicou à NVSRAM existente serão perdidas durante o processo de ativação. Você precisa aplicar as configurações personalizadas à NVSRAM novamente após a conclusão do processo de ativação.

Ative o software e o firmware no SANtricity System Manager

Você pode optar por ativar os arquivos de upgrade imediatamente ou aguardar um momento mais conveniente.

Sobre esta tarefa

Você pode baixar e transferir os arquivos sem ativá-los. Você pode optar por ativar depois pelos seguintes motivos:

- **Horário do dia** — A ativação do software e firmware pode demorar bastante, então talvez seja melhor esperar até que as cargas de E/S estejam mais leves. Os controladores fazem failover durante a ativação, portanto o desempenho pode ser inferior ao normal até que a atualização seja concluída.
- **Tipo de pacote** — Você pode querer testar o novo software e firmware em um array de storage antes de atualizar os arquivos em outros arrays de storage.

Quando você tiver um software ou firmware que foi transferido, mas ainda não ativado, verá uma notificação na área de Notificações da página inicial do System Manager e também na página do Upgrade Center.

Não é possível interromper o processo de ativação depois que ele começa.

Passos

1. Selecione o menu: suporte [Upgrade Center].
2. Na área rotulada SANtricity OS Controller Software upgrade, clique em **Ativar** e confirme que deseja realizar a operação.

   Você pode cancelar a operação durante a verificação de integridade pré-atualização, mas não durante a ativação.

   A verificação de integridade pré-atualização começa. Se a verificação de integridade pré-atualização for bem-sucedida, o processo de atualização prossegue para a ativação dos arquivos. Se a verificação de integridade 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 aconselhar você a continuar com a atualização apesar dos erros, selecionando a caixa de seleção **Allow Upgrade**.

   Após a conclusão bem-sucedida da verificação de integridade pré-atualização, a ativação ocorre. O tempo necessário para a ativação depende da configuração do seu array de storage 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 seu navegador com o nome `drive_upgrade_log-timestamp.txt`.

Depois que você terminar

- Verifique se todos os componentes aparecem na página de Hardware.
- Verifique as novas versões de software e firmware consultando a caixa de diálogo Inventário de Software

e Firmware (acesse o **Support › Upgrade Center** e clique no link para **Software and Firmware Inventory**).

- Se você atualizou a NVSRAM do controlador, todas as configurações personalizadas que você aplicou à NVSRAM existente serão perdidas durante o processo de ativação. Você precisa aplicar as configurações personalizadas à NVSRAM novamente após a conclusão do processo de ativação.

Upgrade do firmware da unidade no SANtricity System Manager

Você pode atualizar o firmware das suas unidades para garantir que tenha todos os recursos mais recentes e correções de bugs.

Antes de começar

- Você fez backup dos seus dados usando backup de disco para disco, cópia de volume (para um grupo de volume não afetado pelo upgrade de firmware planejado) ou um espelhamento remoto.
- O array de storage está com status Ótimo.
- Todas as unidades estão com status Ótimo.
- Nenhuma alteração de configuração está em execução no array de storage.
- Se as unidades forem capazes apenas de um upgrade offline, a atividade de E/S em todos os volumes associados às unidades é interrompida.

Passos

1. Selecione o menu: suporte [Upgrade Center].
2. Faça o download dos novos arquivos do site de suporte para o seu cliente de gerenciamento.
3. Em upgrade do firmware da unidade, clique em **Iniciar upgrade**.

   Uma caixa de diálogo aparece, que lista os arquivos de firmware da unidade atualmente em uso.

4. Extraia (descompacte) os arquivos que você baixou do site de Support.
5. Clique em **Procurar** e selecione os novos arquivos de firmware da unidade que você baixou do site de suporte.

   Os arquivos de firmware da unidade têm um nome de arquivo semelhante a `D_HUC101212CSS600_30602291_MS01_2800_0002` com a extensão de `.dlp`.

   Você pode selecionar até quatro arquivos de firmware da unidade, um de cada vez. Se mais de um arquivo de firmware da unidade for compatível com a mesma unidade, você receberá um erro de conflito de arquivos. Decida qual arquivo de firmware da unidade deseja usar para o upgrade e remova o outro.

6. Clique em **Next**.

   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 Firmware Proposto. Se precisar alterar o firmware, clique em **Voltar** para retornar à caixa de diálogo anterior.

7. Selecione o tipo de upgrade que deseja realizar:
   - **Online (padrão)** — Mostra as unidades que suportam um download de firmware *enquanto o array de*

storage está processando E/S. Você não precisa interromper a E/S nos volumes associados que usam essas unidades ao selecionar este método de upgrade. Essas unidades são atualizadas uma de cada vez enquanto o array de storage está processando E/S nessas unidades.

- **Offline (paralelo)** — Mostra as unidades que podem suportar um download de firmware *somente enquanto toda a atividade de E/S estiver interrompida* em quaisquer volumes que utilizam essas unidades. Você deve interromper toda a atividade de E/S em quaisquer volumes que utilizam as unidades que você está atualizando ao selecionar este método de atualização. Unidades que não possuem redundância devem ser processadas como uma operação offline. Este requisito inclui qualquer unidade associada a cache SSD, um grupo de volume RAID 0 ou qualquer pool ou grupo de volume que esteja degradado. A atualização offline (paralela) geralmente é mais rápida do que o método online (padrão).

8. Na primeira coluna da tabela, selecione a(s) unidade(s) que deseja fazer upgrade.
9. Clique em **Iniciar** e confirme que deseja realizar a operação.

   Se precisar interromper a atualização, clique em **Parar**. Quaisquer downloads de firmware em andamento serão concluídos. Quaisquer downloads de firmware que ainda não tenham sido iniciados serão cancelados.

   > Interromper o upgrade do formware 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 seu navegador com o nome `drive_upgrade_log-timestamp.txt`.

11. Se algum dos seguintes erros ocorrer durante o procedimento de upgrade, tome a ação recomendada apropriada.

Erros e ações recomendadas

Se você se deparar com este erro de download de firmware…	Em seguida, faça o seguinte…
Unidades atribuídas com falha	Uma possível causa da falha é que a unidade não possui a assinatura apropriada. Certifique-se de que a unidade afetada seja uma unidade autorizada. Entre em contato com o suporte técnico para mais informações. Ao substituir uma unidade, certifique-se de que a unidade de substituição tenha uma capacidade igual ou superior à da unidade com falha que está sendo substituída. Você pode substituir a unidade com falha enquanto o array de storage está recebendo E/S.
Verificar array de storage	• Certifique-se de que um endereço IP tenha sido atribuído a cada controlador. • Certifique-se de que todos os cabos conectados ao controlador não estão danificados. • Certifique-se de que todos os cabos estejam firmemente conectados.
Unidades hot spare integradas	Essa condição de erro precisa ser corrigida antes que você possa atualizar o firmware. Inicie o System Manager e use o Recovery Guru para resolver o problema.
Grupos de volume incompletos	Se um ou mais grupos de volumes ou pools de discos estiverem incompletos, você deve 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 verificação de mídia/paridade em segundo plano) atualmente em execução em quaisquer grupos de volume	Se uma ou mais operações exclusivas estiverem em andamento, as operações deverão ser concluídas antes que o firmware possa ser atualizado. Use System Manager para monitorar o progresso das operações.
Volumes ausentes	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 do array de storage precisa de atenção. Essa condição deve ser corrigida antes que o firmware possa ser atualizado. Inicie o System Manager e use o Recovery Guru para resolver o problema.

Se você se deparar com este erro de download de firmware…	Em seguida, faça o seguinte…
Informações de partição de armazenamento incompatíveis entre os gráficos de objetos do controlador	Ocorreu um erro ao validar os dados nos controladores. Entre em contato com o suporte técnico para resolver este problema.
A verificação do controlador de banco de dados SPM falha	Ocorreu um erro no banco de dados de mapeamento de partições de armazenamento em um controlador. Entre em contato com o suporte técnico para resolver esse problema.
Validação do banco de dados de configuração (se compatível com a versão do controlador do array de storage)	Ocorreu um erro no banco de dados de configuração de um controlador. Entre em contato com o suporte técnico para resolver este problema.
Verificações relacionadas ao MEL	Contate o suporte técnico para resolver este problema.
Mais de 10 eventos MEL informativos ou críticos de DDE foram relatados nos últimos 7 dias	Contate o suporte técnico para resolver este problema.
Mais de 2 eventos críticos MEL da página 2C foram relatados nos últimos 7 dias	Contate o suporte técnico para resolver este problema.
Mais de 2 eventos MEL críticos de canal de unidade degradado foram relatados nos últimos 7 dias	Contate o suporte técnico para resolver este problema.
Mais de 4 registros críticos de MEL nos últimos 7 dias	Contate o suporte técnico para resolver este problema.

Depois que você terminar

Seu upgrade do formware da unidade foi concluído. Você pode retomar as operações normais.

Saiba mais sobre erros de upgrade de software e firmware do SANtricity

Podem ocorrer erros durante a atualização do software do controlador ou durante o upgrade do firmware da unidade.

Erro de download do firmware	Descrição	Ação recomendada
Unidades atribuídas com falha	Falha ao fazer upgrade de uma unidade atribuída no array de storage.	Uma possível causa da falha é que a unidade não possui a assinatura apropriada. Certifique-se de que a unidade afetada seja uma unidade autorizada. Entre em contato com o suporte técnico para mais informações. Ao substituir uma unidade, certifique-se de que a unidade de substituição tenha uma capacidade igual ou superior à da unidade com falha que está sendo substituída. Você pode substituir a unidade com falha enquanto o array de storage está recebendo E/S.
Unidades hot spare integradas	Se a unidade estiver marcada como hot spare e estiver em uso em um grupo de volume, o processo de upgrade do firmware falhará.	Essa condição de erro precisa ser corrigida antes que você possa atualizar o firmware. Inicie o System Manager e use o Recovery Guru para resolver o problema.
Grupos de volume incompletos	Se alguma unidade que faz parte de um grupo de volume for ignorada, removida ou não responder, ela será considerada um grupo de volume incompleto. Um grupo de volume incompleto impede upgrades de firmware.	Se um ou mais grupos de volumes ou pools de discos estiverem incompletos, você deve 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 verificação de mídia/paridade em segundo plano) atualmente em execução em quaisquer grupos de volume	Não é possível atualizar o firmware se houver alguma operação exclusiva em andamento em um volume.	Se uma ou mais operações exclusivas estiverem em andamento, as operações deverão ser concluídas antes que o firmware possa ser atualizado. Use System Manager para monitorar o progresso das operações.
Volumes ausentes	Não é possível atualizar o firmware se algum volume estiver faltando.	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 download do firmware	Descrição	Ação recomendada
Qualquer controlador em um estado diferente do ideal	Não é possível atualizar o firmware se qualquer um dos controladores estiver em um estado diferente do ótimo.	Um dos controladores do array de storage precisa de atenção. Essa condição deve ser corrigida antes que o firmware possa ser atualizado. Inicie o System Manager e use o Recovery Guru para resolver o problema.
A verificação do controlador de banco de dados SPM falha	Não é possível atualizar o firmware porque o banco de dados de mapeamento das partições de storage está corrompido.	Ocorreu um erro no banco de dados de mapeamento de partições de armazenamento em um controlador. Entre em contato com o suporte técnico para resolver esse problema.
Validação do banco de dados de configuração (se compatível com a versão do controlador do array de storage)	Não é possível atualizar o firmware porque o banco de dados de configuração está corrompido.	Ocorreu um erro no banco de dados de configuração de um controlador. Entre em contato com o suporte técnico para resolver este problema.
Verificações relacionadas ao MEL	Não é possível atualizar o firmware porque o registro de eventos contém erros.	Contate o suporte técnico para resolver este problema.
Mais de 10 eventos MEL informativos ou críticos de DDE foram relatados nos últimos 7 dias	Não é possível atualizar o firmware porque há mais de 10 eventos MEL informativos ou críticos do DDE relatados nos últimos sete dias.	Contate o suporte técnico para resolver este problema.
Mais de 2 eventos críticos MEL da página 2C foram relatados nos últimos 7 dias	Não é possível atualizar o firmware porque há mais de dois eventos críticos MEL de página 2C relatados nos últimos sete dias.	Contate o suporte técnico para resolver este problema.
Mais de 2 eventos MEL críticos de canal de unidade degradado foram relatados nos últimos 7 dias	Não é possível atualizar o firmware porque foram relatados mais de dois eventos MEL críticos de canal de unidade degradada nos últimos sete dias.	Contate o suporte técnico para resolver este problema.
Mais de 4 registros críticos de MEL nos últimos 7 dias	Não é possível atualizar o firmware porque há mais de quatro entradas críticas no log de eventos registradas nos últimos sete dias.	Contate o suporte técnico para resolver este problema.
É necessário um endereço IP de gerenciamento válido.	É necessário um endereço IP de controlador válido para realizar esta operação.	Contate o suporte técnico para resolver este problema.

Erro de download do firmware	Descrição	Ação recomendada
O comando exige que seja fornecido um endereço IP de gerenciamento ativo para cada controlador.	É necessário um endereço IP de controlador para cada controlador associado ao array de storage para esta operação.	Contate o suporte técnico para resolver este problema.
Tipo de arquivo de download não processado retornado.	O arquivo de download especificado não é compatível.	Contate o suporte técnico para resolver este problema.
Ocorreu um erro durante o procedimento de upload de download do firmware.	O download do firmware falhou porque o controlador não consegue processar a solicitação. Verifique se o array de storage está ideal e tente a operação novamente.	Se esse erro ocorrer novamente após verificar se o array de storage está otimizado, 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 o array de storage está ideal e tente novamente a operação.	Se esse erro ocorrer novamente após verificar se o array de storage está otimizado, entre em contato com o suporte técnico para resolver esse problema.
O tempo limite foi atingido enquanto se aguardava o controlador {0} reinicializar.	O software de gerenciamento não consegue se reconectar ao controlador {0} após uma reinicialização. Verifique se existe um caminho de conexão operacional com o array de storage e tente novamente a operação caso ela não tenha sido concluída com sucesso.	Se esse erro ocorrer novamente após verificar se o array de storage está otimizado, 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 dessas condições, talvez seja necessário entrar em contato com o suporte técnico. As informações sobre o download do firmware mais recente do controlador estão disponíveis no array de storage. Essas informações ajudam o suporte técnico a entender as condições de erro que impediram o upgrade e o download do firmware.

AutoSupport FAQ para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

Que dados estou coletando?

O recurso AutoSupport e a funcionalidade de Coleta Manual de Dados de Suporte oferecem maneiras de coletar dados em um pacote de suporte ao cliente para solução de problemas remota e análise de problemas pelo suporte técnico.

O pacote de suporte ao cliente reúne todos os tipos de informações sobre o array de storage em um único

arquivo compactado. As informações coletadas incluem a configuração física, a 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 array de storage.

O que os dados de setores ilegíveis me mostram?

Você pode exibir dados detalhados sobre setores ilegíveis detectados nas unidades do seu array de storage.

O registro de setores ilegíveis mostra o setor ilegível mais recente primeiro. O registro contém as seguintes informações sobre os volumes que contêm os setores ilegíveis. Os campos podem ser classificados.

Campo	Descrição
Volume afetado	Exibe o rótulo do volume. Se um volume ausente contiver setores ilegíveis, o World Wide Identifier será exibido para o volume ausente.
Número da unidade lógica (LUN)	Exibe o LUN do volume. Se o volume não tiver um LUN, a caixa de diálogo mostra NA.
Designado para	Mostra os hosts ou clusters de hosts que têm acesso ao volume. Se o volume não for acessível por um host, cluster de hosts ou mesmo um Default Cluster, a caixa de diálogo mostra 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 detectado.
Endereço de bloco lógico de volume	Exibe o endereço do bloco lógico (LBA) do volume.
Localização da unidade	Mostra a prateleira da unidade, a gaveta (se a sua prateleira da unidade tiver gavetas) e a localização da bay.
Endereço do bloco lógico da unidade	Mostra o LBA da unidade.
Tipo de falha	Exibe um dos seguintes tipos de falha: • **Físico** — Um erro de mídia física. • **Lógico** — Um erro de leitura em outra parte da faixa que causa dados ilegíveis. Por exemplo, um setor ilegível devido a erros de mídia em outra parte do volume. • **Inconsistente** — dados de redundância inconsistentes. • **Garantia de Dados** — Um erro de Data Assurance.

O que é uma health image?

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 detecta determinados erros. Em certos cenários de resolução de problemas, o suporte técnico pode solicitar que você recupere o arquivo de imagem de integridade e o envie para eles.

O que as funcionalidades do AutoSupport fazem?

O recurso AutoSupport é composto por três funcionalidades individuais que você ativa separadamente.

- **Básico AutoSupport** — Permite que seu array de storage colete e envie dados automaticamente para o suporte técnico.
- **AutoSupport OnDemand** — Permite que o suporte técnico solicite a retransmissão de um despacho anterior do AutoSupport quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir do array de storage, não do servidor AutoSupport. O array de storage verifica periodicamente com o servidor AutoSupport se há alguma solicitação de retransmissão pendente e responde de acordo.
- **Diagnóstico Remoto** — Permite que o suporte técnico solicite um novo, atualizado AutoSupport dispatch quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir do array de storage, não do AutoSupport server. O array de storage verifica periodicamente com o AutoSupport server se há novas solicitações pendentes e responde de acordo.

Que tipo de dados é coletado por meio do recurso AutoSupport?

O recurso AutoSupport contém três tipos de despacho padrão: despachos de eventos, despachos agendados e despachos sob demanda e de diagnóstico remoto.

Os dados do AutoSupport não contêm quaisquer dados de usuário.

- **Despachos de eventos**

  Quando ocorrem eventos no sistema que justificam uma notificação proativa ao suporte técnico, o recurso AutoSupport envia automaticamente um despacho acionado por evento.

  - Enviado quando ocorre um evento de suporte no array de storage gerenciado.
  - Inclui uma visão geral abrangente do que estava acontecendo com o array de storage no momento em que o evento ocorreu.
- **Despachos programados**

  O recurso AutoSupport envia automaticamente vários despachos em uma programação regular.

  - **Despachos diários** — Enviados uma vez por dia durante um intervalo de tempo configurável pelo usuário. Inclui os registros de eventos do sistema e dados de desempenho atuais.
  - **Boletins semanais** — Enviados 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 anterior do AutoSupport quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir do array de storage, não do servidor AutoSupport. O array de storage verifica

periodicamente com o servidor AutoSupport se há alguma solicitação de retransmissão pendente e responde de acordo.

- **Diagnóstico Remoto** — Permite que o suporte técnico solicite um novo, atualizado AutoSupport dispatch quando necessário para solucionar um problema. Todas as transmissões são iniciadas a partir do array de storage, não do AutoSupport server. O array de storage verifica periodicamente com o AutoSupport server se há novas solicitações pendentes e responde de acordo.

Como configuro o método de entrega para o recurso AutoSupport?

O recurso AutoSupport suporta os protocolos HTTPS e SMTP para o envio de despachos AutoSupport ao suporte técnico.

Antes de começar

- O recurso AutoSupport deve estar ativado. Você pode verificar se ele está ativado na página AutoSupport.
- Um servidor DNS deve ser instalado e configurado na sua rede. O endereço do servidor DNS deve ser configurado no System Manager (essa tarefa está disponível na página Hardware).

Sobre esta tarefa

Analise os diferentes protocolos:

- **HTTPS** — Permite que você se conecte diretamente ao servidor de suporte técnico de destino usando HTTPS. Se você quiser habilitar AutoSupport OnDemand ou Diagnóstico Remoto, o método de entrega do AutoSupport deve ser definido como HTTPS.
- **E-mail** — Permite usar um servidor de e-mail como método de entrega para o envio de despachos AutoSupport.

> **Diferenças entre os métodos HTTPS e Email**. O método de entrega por Email, que utiliza SMTP, apresenta algumas diferenças importantes em relação ao método de entrega HTTPS. Primeiro, o tamanho dos despachos para o método Email é limitado a 5MB, o que significa que algumas coletas de dados do ASUP não serão despachadas. Segundo, o recurso AutoSupport OnDemand está disponível apenas no método de entrega HTTPS.

Passos

1. Selecione o menu:Suporte [Support Center > AutoSupport] tab.
2. Selecione **Configurar AutoSupport Delivery Method**.

   Uma caixa de diálogo aparece, que lista os métodos de entrega do despacho.

3. Selecione o método de entrega desejado e, em seguida, selecione os parâmetros para esse método de entrega. Faça um dos seguintes procedimentos:
   - Se você selecionou HTTPS, selecione um dos seguintes parâmetros de entrega:
     - **Diretamente** — Este parâmetro de entrega é a seleção padrão. Escolher esta opção permite que você se conecte diretamente ao sistema de suporte técnico de destino usando o protocolo HTTPS.
     - **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 script de autoconfiguração de proxy (PAC)** — Especifique o local de um arquivo de script de autoconfiguração 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 Email, insira as seguintes informações:
  - O endereço do servidor de e-mail como um domínio totalmente qualificado, endereço IPv4 ou endereço IPv6.
  - O endereço de e-mail que aparece no campo De do e-mail de despacho do AutoSupport.
  - **Opcional; caso deseje realizar um teste de configuração.** O endereço de e-mail para onde será enviada uma confirmação quando o sistema AutoSupport receber o despacho de teste.
  - Se desejar criptografar as mensagens, selecione **SMTPS** ou **STARTTLS** para o tipo de criptografia e, em seguida, selecione o número da porta para as mensagens criptografadas. Caso contrário, selecione **None**.
  - Caso necessário, insira um nome de usuário e uma senha para autenticação com o remetente de saída e o servidor de e-mail.

4. Clique em **Testar configuração** para testar a conexão com o servidor de suporte técnico usando os parâmetros de entrega especificados. Se você habilitou o recurso AutoSupport On-Demand, o sistema também testará a conexão para entrega de despacho AutoSupport OnDemand.

   Se o teste de configuração falhar, verifique suas 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?

Ao selecionar 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 no controlador. O recurso Coletar Dados de Configuração salva as mesmas informações que o comando da interface de linha de comando para `save storageArray dbmDatabase`.

O que preciso saber antes de atualizar o software SANtricity OS?

Antes de atualizar o software e firmware do seu controlador, esteja ciente destes itens.

- Você leu o documento e o arquivo `readme.txt` e determinou que deseja fazer a atualização.
- Você sabe se deseja atualizar o firmware do seu IOM.

  Normalmente, você deve atualizar todos os componentes ao mesmo tempo. No entanto, você pode optar por não atualizar o firmware do IOM se não quiser atualizá-lo como parte da atualização do software do controlador SANtricity OS ou se o suporte técnico tiver instruído você a fazer o downgrade do firmware do IOM (você só pode fazer o downgrade do firmware usando a interface de linha de comando).

- Você sabe se deseja atualizar o arquivo NVSRAM do controlador.

  Normalmente, você deve atualizar todos os componentes ao mesmo tempo. No entanto, você pode optar por não atualizar o arquivo NVSRAM do controlador se o seu arquivo tiver sido modificado ou for uma versão personalizada e você não quiser sobrescrevê-lo.

- Você sabe se deseja ativar agora ou mais tarde.

  Os motivos para ativar mais tarde podem incluir:

- **Horário do dia** — A ativação do software e firmware pode demorar bastante, então talvez seja melhor esperar até que as cargas de E/S estejam mais leves. Os controladores fazem failover durante a ativação, portanto o desempenho pode ser inferior ao normal até que a atualização seja concluída.
- **Tipo de pacote** — Você pode querer testar o novo software e firmware em um array de storage antes de atualizar os arquivos em outros arrays de storage.

Esses componentes fazem parte da atualização do software do controlador SANtricity OS:

- **Software de gerenciamento** — System Manager é o software que gerencia o array de storage.
- **Controller firmware** — O firmware do controlador gerencia a E/S entre hosts e volumes.
- **Controller NVSRAM** — O Controller NVSRAM é um arquivo de controlador que especifica as configurações padrão para os controladores.
- **IOM firmware** — O firmware do módulo de E/S (IOM) gerencia a conexão entre um controlador e um compartimento de unidades. Ele também monitora o status dos componentes.
- **Software supervisor** — O software supervisor é a máquina virtual em um controlador na qual o software é executado.

Como parte do processo de upgrade, o driver multipath/failover do host e/ou o driver HBA também podem precisar ser atualizados para que o host possa interagir corretamente com os controladores.

Para determinar se este é o caso, consulte o "NetApp Ferramenta de Matriz de Interoperabilidade".

Se o seu array de storage contiver apenas um controlador ou se você não tiver um driver multipath instalado, interrompa a atividade de E/S para o array de storage para evitar erros de aplicativo. Se o seu array de storage tiver dois controladores e você tiver um driver multipath instalado, não é necessário interromper a atividade de E/S.

Não faça alterações no array de storage enquanto o upgrade estiver em andamento.

O que preciso saber antes de suspender a sincronização automática do IOM?

Suspender a sincronização automática do IOM impede que o firmware do IOM seja atualizado na próxima vez que ocorrer uma atualização do software do controlador SANtricity OS.

Normalmente, o software do controlador e o firmware do IOM são atualizados em conjunto. Você pode suspender a sincronização automática do IOM se tiver uma versão especial do firmware do IOM que deseja preservar em seu gabinete. Caso contrário, você retornará ao firmware do IOM incluído no software do controlador na próxima vez que fizer um upgrade do software do controlador.

Por que a atualização do meu firmware está progredindo tão lentamente?

O progresso da atualização do firmware depende da carga geral do sistema.

Durante um upgrade online do firmware da unidade, se uma transferência de volume ocorrer durante o processo de reconstrução rápida, o sistema inicia uma reconstrução completa no volume que foi transferido. Essa operação pode levar um tempo considerável. O tempo real de reconstrução completa depende de vários fatores, incluindo a quantidade de atividade de E/S ocorrendo durante a operação de reconstrução, o número de unidades no grupo de volume, a configuração de prioridade de reconstrução e o desempenho da unidade.

O que preciso saber antes de atualizar o firmware da unidade?

Antes de atualizar o firmware da unidade, esteja ciente destes itens.

- Como medida de precaução, faça backup dos seus dados usando backup de disco para disco, cópia de volume (para um grupo de volume não afetado pelo upgrade de firmware planejado) ou espelhamento remoto.
- Você pode optar por atualizar apenas algumas unidades para testar o comportamento do novo firmware e garantir que ele está funcionando corretamente. Se o novo firmware estiver funcionando corretamente, atualize as unidades restantes.
- Se você tiver alguma unidade com defeito, conserte-a antes de iniciar o upgrade do firmware.
- Se as unidades puderem realizar uma atualização offline, interrompa a atividade de E/S em todos os volumes associados às unidades. Quando a atividade de E/S é interrompida, nenhuma operação de configuração associada a esses volumes pode ocorrer.
- Não remova nenhuma unidade durante o upgrade do firmware da unidade.
- Não faça nenhuma alteração de configuração no array de storage durante o upgrade do firmware da unidade.

Como escolho qual tipo de upgrade realizar?

Você escolhe o tipo de upgrade a ser realizado na unidade, dependendo do estado do pool ou grupo de volume.

- **Online**

  Se o pool ou grupo de volume suportar redundância e estiver Ótimo, você pode usar o método Online para fazer o upgrade do firmware da unidade. O método Online baixa o firmware *enquanto o array de storage está processando E/S* para os volumes associados que utilizam essas unidades. Você não precisa interromper a E/S para os volumes associados que utilizam 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 volume, seu firmware pode ser atualizado pelo método Online ou Offline. O desempenho do sistema pode ser impactado ao usar o método Online para fazer o upgrade do firmware da unidade.

- **Offline**

  Se o pool ou grupo de volume não suportar redundância (RAID 0) ou estiver degradado, você deve usar o método Offline para upgrade do firmware da unidade. O método Offline fará o upgrade do firmware *somente enquanto toda a atividade de I/O estiver parada* nos volumes associados que utilizam essas unidades. Você deve parar toda a I/O para quaisquer volumes associados que utilizem essas unidades. Se a unidade não estiver atribuída a um pool ou grupo de volume, seu firmware pode ser atualizado pelo método Online ou Offline.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em http://www.netapp.com/TM são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.