



Unified Manager

SANtricity 11.9

NetApp
December 16, 2024

Índice

- Gerenciamento de vários arrays com o Unified Manager 7 1
 - Interface principal 1
 - Storage arrays 4
 - Importação de definições 12
 - Grupos de array 20
 - Atualizações 22
 - Espelhamento 29
 - Certificados 46
 - Gerenciamento de acesso 55

Gerenciamento de vários arrays com o Unified Manager 7

Interface principal

Visão geral da interface do Unified Manager


O Unified Manager é uma interface baseada na Web que permite gerenciar vários storage arrays em uma única visualização.

Página principal

Quando você faz login no Unified Manager, a página principal é aberta para **Gerenciar - todos**. Nesta página, você pode rolar por uma lista de matrizes de armazenamento descobertas na sua rede, ver o seu status e executar operações em uma única matriz ou em um grupo de matrizes.

Barra lateral de navegação

Você pode acessar os recursos e funções do Unified Manager na barra lateral de navegação.

Área	Descrição
Gerenciar	Descubra matrizes de armazenamento na sua rede, inicie o Gestor de sistema SANtricity para uma matriz, importe definições de uma matriz para várias matrizes e gere grupos de matrizes. Marque as caixas de seleção ao lado dos nomes dos arrays para executar operações neles, como importar configurações e criar grupos de matrizes. As elipses no final de cada linha fornecem um menu em linha para operações em um único array, como renomeá-lo.
Operações	Visualize o progresso das operações em lote, como importar configurações de um array para outro.  Algumas operações não estão disponíveis quando um storage array tem um status não ideal.
Gerenciamento de certificados	Gerencie certificados para autenticar entre navegadores e clientes.
Gerenciamento de acesso	Estabeleça a autenticação de usuário para a interface do Unified Manager.
Suporte	Veja opções de suporte técnico, recursos e Contatos.

Definições de interface e ajuda

No canto superior direito da interface, você pode acessar a Ajuda e outra documentação. Você também pode acessar opções de administração, que estão disponíveis na lista suspensa ao lado do nome de login.

Logins de usuário e senhas

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

Para obter mais informações sobre usuários e senhas, consulte:

- ["Defina a proteção de senha de administrador"](#)
- ["Altere a senha de administrador"](#)
- ["Alterar senhas para perfis de usuário locais"](#)

Navegadores suportados

O Unified Manager pode ser acessado de vários tipos de navegadores.

Os seguintes navegadores e versões são suportados.

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



O Proxy de Serviços Web deve estar instalado e disponível para o navegador.

Defina a proteção de senha de administrador

Você deve configurar o Unified Manager com uma senha de administrador para protegê-lo contra acesso não autorizado.

Senha de administrador e perfis de usuário

Ao iniciar o Unified Manager pela primeira vez, você será solicitado a definir uma senha de administrador. Qualquer usuário que tenha a senha de administrador pode fazer alterações de configuração nos storages.

Além da senha de administrador, a interface do Unified Manager inclui perfis de usuário pré-configurados com uma ou mais funções mapeadas para eles. Para obter mais informações, ["Como o Gerenciamento de Acesso funciona"](#) consulte .

Os usuários e mapeamentos não podem ser alterados. Apenas as senhas podem ser modificadas. Para alterar senhas, consulte:

- ["Altere a senha de administrador"](#)
- ["Alterar senhas para perfis de usuário locais"](#)

Tempos limite da sessão

O software solicita a senha apenas uma vez durante uma única sessão de gerenciamento. Uma sessão expira após 30 minutos de inatividade por padrão, e nesse momento, você deve digitar a senha novamente. Se outro utilizador aceder ao software a partir de outro cliente de gestão e alterar a palavra-passe enquanto a sessão estiver em curso, ser-lhe-á pedida uma palavra-passe da próxima vez que tentar uma operação de configuração ou uma operação de visualização.

Por razões de segurança, você pode tentar inserir uma senha apenas cinco vezes antes que o software entre em um estado de "bloqueio". Neste estado, o software rejeita tentativas subsequentes de senha. Tem de esperar 10 minutos para repor o estado "normal" antes de tentar introduzir novamente uma palavra-passe.

Você pode ajustar os tempos limite da sessão ou desativar completamente os tempos limite da sessão. Para obter mais informações, "[Gerenciar tempos limite de sessão](#)" consulte .

Altere a senha de administrador

Você pode alterar a senha de administrador usada para acessar o Unified Manager.

Antes de começar

- Você deve estar logado como administrador local, o que inclui permissões de administrador raiz.
- Você deve saber a senha de administrador atual.

Sobre esta tarefa

Tenha em mente estas diretrizes ao escolher uma senha:

- As senhas diferenciam maiúsculas de minúsculas.
- Os espaços de saída não são removidos das senhas quando são definidos. Tenha cuidado para incluir espaços se eles foram incluídos na senha.
- Para maior segurança, use pelo menos 15 caracteres alfanuméricos e altere a senha com frequência.

Passos

1. Selecione **Definições > Gestão de Acesso**.
2. Selecione a guia **funções de usuário local**.
3. Selecione o usuário **admin** na tabela.

O botão alterar senha fica disponível.

4. Selecione **alterar palavra-passe**.

A caixa de diálogo alterar senha será exibida.

5. Se não estiver definido um comprimento mínimo de palavra-passe para palavras-passe de utilizador local, selecione a caixa de verificação para exigir que o utilizador introduza uma palavra-passe para aceder ao sistema.
6. Introduza a nova palavra-passe nos dois campos.
7. Introduza a palavra-passe do administrador local para confirmar esta operação e, em seguida, clique em **alterar**.

Gerenciar tempos limite de sessão

É possível configurar tempos limite para o Unified Manager para que os usuários de sessões inativas sejam desconetados após um tempo especificado.

Sobre esta tarefa

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



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

Passos

1. Na barra de menus, selecione a seta suspensa ao lado do nome de login do usuário.
2. Selecione **Ativar/Desativar tempo limite da sessão**.

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

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

O tempo limite mínimo que você pode definir é de 15 minutos.



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

4. Clique em **Salvar**.

Storage arrays

Descrição geral da descoberta

Para gerenciar recursos de armazenamento, primeiro você deve descobrir os storages de armazenamento na rede.

Como faço para descobrir arrays?

Use a página Adicionar/descobrir para localizar e adicionar os storages de armazenamento que você deseja gerenciar na rede da sua organização. Você pode descobrir vários arrays ou descobrir um único array. Para fazer isso, você insere endereços IP de rede e, em seguida, o Unified Manager tenta conexões individuais para cada endereço IP nesse intervalo.

Saiba mais:

- ["Considerações para descobrir arrays"](#)
- ["Descubra vários storages de armazenamento"](#)
- ["Descubra um único array"](#)

Como faço para gerenciar arrays?

Depois de descobrir arrays, vá para a página **Gerenciar - todos**. Nesta página, você pode rolar por uma lista de matrizes de armazenamento descobertas na sua rede, ver o seu status e executar operações em uma única matriz ou em um grupo de matrizes.

Se você quiser gerenciar um único array, selecione-o e abra o System Manager.

Saiba mais:

- ["Considerações para acessar o System Manager"](#)
- ["Gerenciar um storage array individual"](#)
- ["Ver o status do storage array"](#)

Conceitos

Considerações para descobrir arrays

Antes que o Unified Manager possa exibir e gerenciar recursos de storage, ele deve descobrir os storages que você deseja gerenciar na rede da organização. Você pode descobrir vários arrays ou descobrir um único array.

Descobrendo vários storages de armazenamento

Se você optar por descobrir vários arrays, insira um intervalo de endereços IP de rede e, em seguida, o Unified Manager tentará conexões individuais para cada endereço IP nesse intervalo. Qualquer matriz de armazenamento alcançada com sucesso aparece na página descobrir e pode ser adicionada ao seu domínio de gerenciamento.

Descobrendo um único storage array

Se você optar por descobrir um único array, insira o endereço IP único de um dos controladores no storage array e, em seguida, o storage array individual será adicionado.



O Unified Manager detecta e exibe apenas o único endereço IP ou endereço IP dentro de um intervalo atribuído a um controlador. Se houver controladores alternativos ou endereços IP atribuídos a esses controladores que estejam fora desse único endereço IP ou intervalo de endereços IP, o Unified Manager não os detectará ou exibirá. No entanto, depois de adicionar a matriz de armazenamento, todos os endereços IP associados serão descobertos e exibidos na visualização Gerenciar.

Credenciais do usuário

Como parte do processo de descoberta, você deve fornecer a senha de administrador para cada storage que deseja adicionar.

Certificados de serviços da Web

Como parte do processo de descoberta, o Unified Manager verifica se os storage arrays descobertos estão usando certificados de uma fonte confiável. O Unified Manager usa dois tipos de autenticação baseada em certificado para todas as conexões que estabelece com o navegador:

- **Certificados confiáveis**

Para storages descobertos pelo Unified Manager, talvez seja necessário instalar certificados confiáveis adicionais fornecidos pela Autoridade de certificação.

Use o botão **Import** para importar esses certificados. Se você já tiver conectado a esse array antes, um ou ambos os certificados do controlador expiram, revogam ou faltam um certificado raiz ou um certificado intermediário em sua cadeia de certificados. Você deve substituir o certificado expirado ou revogado ou adicionar o certificado raiz ou o certificado intermediário em falta antes de gerenciar o storage array.

• Certificados autoassinados

Certificados autoassinados também podem ser usados. Se o administrador tentar descobrir matrizes sem importar certificados assinados, o Unified Manager exibirá uma caixa de diálogo de erro que permite que o administrador aceite o certificado autoassinado. O certificado autoassinado do storage array será marcado como confiável e o storage array será adicionado ao Unified Manager.

Se você não confiar nas conexões com o storage array, selecione **Cancelar** e valide a estratégia de certificado de segurança do storage antes de adicionar o storage array ao Unified Manager.

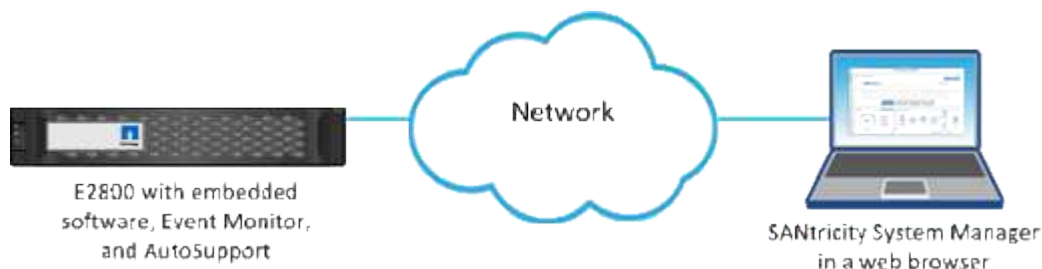
Considerações para acessar o System Manager

Selecione um ou mais storages e use a opção Iniciar para abrir o System Manager quando quiser configurar e gerenciar storages.

O System Manager é uma aplicação incorporada nos controladores, que está ligada à rede através de uma porta de gestão Ethernet. Ele inclui todas as funções baseadas em array.

Para acessar o System Manager, você deve ter:

- Um dos modelos de array listados aqui: "[Visão geral do hardware e-Series](#)"
- Uma conexão fora da banda a um cliente de gerenciamento de rede com um navegador da Web.



Descubra arrays

Descubra vários storages de armazenamento

Você descobre várias matrizes para detectar todas as matrizes de armazenamento na sub-rede onde reside o servidor de gestão e para adicionar automaticamente as matrizes descobertas ao seu domínio de gestão.

Antes de começar

- Você deve estar conectado com um perfil de usuário que inclua permissões de Administrador de Segurança.
- A matriz de armazenamento deve ser corretamente configurada e configurada.

- As senhas do storage array devem ser configuradas usando o bloco Gerenciamento de Acesso do System Manager.
- Para resolver certificados não confiáveis, você deve ter arquivos de certificado confiáveis de uma autoridade de certificação (CA) e os arquivos de certificado estão disponíveis no sistema local.

Descobrir arrays é um procedimento de várias etapas.

Etapa 1: Insira o endereço de rede

Introduza um intervalo de endereços de rede para pesquisar na sub-rede local. Qualquer matriz de armazenamento alcançada com sucesso aparece na página descobrir e pode ser adicionada ao seu domínio de gerenciamento.

Se você precisar parar a operação de descoberta por qualquer motivo, clique em **Stop Discovery**.

Passos

1. Na página Gerenciar, selecione **Adicionar/descobrir**.

A caixa de diálogo Adicionar/descobrir é exibida.

2. Selecione o botão de opção **Discover all storage arrays within a network range**.
3. Introduza o endereço de rede inicial e o endereço de rede final para procurar na sub-rede local e, em seguida, clique em **Iniciar descoberta**.

O processo de descoberta é iniciado. Este processo de descoberta pode levar vários minutos para ser concluído. A tabela na página descobrir é preenchida à medida que os storages são descobertos.



Se não forem detetados arrays gerenciáveis, verifique se os storages de armazenamento estão conectados corretamente à sua rede e se seus endereços atribuídos estão dentro do alcance. Clique em **New Discovery Parameters** (novos parâmetros de descoberta) para voltar à página Add/Discover (Adicionar/descobrir).

4. Reveja a lista de matrizes de armazenamento descobertas.
5. Marque a caixa de seleção ao lado de qualquer matriz de armazenamento que você deseja adicionar ao seu domínio de gerenciamento e clique em **Avançar**.

O Unified Manager executa uma verificação de credenciais em cada array que você está adicionando ao domínio de gerenciamento. Talvez seja necessário resolver quaisquer certificados autoassinados e certificados não confiáveis associados a essa matriz.

6. Clique em **Next** (seguinte) para avançar para a próxima etapa do assistente.

Etapa 2: Resolva certificados autoassinados durante a descoberta

Como parte do processo de descoberta, o sistema verifica se os storages de armazenamento estão usando certificados por uma fonte confiável.

Passos

1. Execute um dos seguintes procedimentos:
 - Se você confiar nas conexões com os storages de armazenamento descobertos, continue para a próxima placa no assistente. Os certificados autoassinados serão marcados como confiáveis e os storages de armazenamento serão adicionados ao Unified Manager.

- Se você não confiar nas conexões com os storages de armazenamento, selecione **Cancelar** e valide a estratégia de certificado de segurança de cada storage antes de adicionar qualquer um deles ao Unified Manager.

2. Clique em **Next** (seguinte) para avançar para a próxima etapa do assistente.

Etapa 3: Resolva certificados não confiáveis durante a descoberta

Certificados não confiáveis ocorrem quando um storage array tenta estabelecer uma conexão segura com o Unified Manager, mas a conexão não consegue confirmar como segura. Durante o processo de descoberta de matriz, você pode resolver certificados não confiáveis importando um certificado de autoridade de certificação (CA) (ou certificado assinado pela CA) emitido por um terceiro confiável.

Talvez seja necessário instalar certificados de CA confiáveis adicionais se alguma das seguintes opções for verdadeira:

- Recentemente, você adicionou uma matriz de armazenamento.
- Um ou ambos os certificados expiram.
- Um ou ambos os certificados são revogados.
- Um ou ambos os certificados estão faltando um certificado raiz ou intermediário.

Passos

1. Marque a caixa de seleção ao lado de qualquer storage para o qual você deseja resolver certificados não confiáveis e selecione o botão **Importar**.

Abre-se uma caixa de diálogo para importar os ficheiros de certificado fidedignos.

2. Clique em **Procurar** para selecionar os arquivos de certificado para os storages de armazenamento.

Os nomes dos arquivos são exibidos na caixa de diálogo.

3. Clique em **Importar**.

Os arquivos são carregados e validados.



Qualquer storage array com problemas de certificado não confiáveis que não sejam resolvidos não será adicionado ao Unified Manager.

4. Clique em **Next** (seguinte) para avançar para a próxima etapa do assistente.

Passo 4: Forneça senhas

Você deve inserir as senhas dos storages de armazenamento que deseja adicionar ao seu domínio de gerenciamento.

Passos

1. Introduza a palavra-passe para cada matriz de armazenamento que pretende adicionar ao Unified Manager.
2. **Opcional:** associar matrizes de armazenamento a um grupo: Na lista pendente, selecione o grupo pretendido a associar com as matrizes de armazenamento selecionadas.
3. Clique em **Finish**.

Depois de terminar

Os storages de armazenamento são adicionados ao domínio de gerenciamento e associados ao grupo selecionado (se especificado).



Pode levar alguns minutos para que o Unified Manager se conecte aos storage arrays especificados.

Descubra um único array

Use a opção Add/Discover Single Storage Array (Adicionar/descobrir matriz de armazenamento única) para descobrir e adicionar manualmente uma única matriz de armazenamento à rede da sua organização.

Antes de começar

- A matriz de armazenamento deve ser corretamente configurada e configurada.
- As senhas do storage array devem ser configuradas usando o bloco Gerenciamento de Acesso do System Manager.

Passos

1. Na página Gerenciar, selecione **Adicionar/descobrir**.

A caixa de diálogo Adicionar/descobrir é exibida.

2. Selecione o botão de opção **Discover a single storage array**.
3. Insira o endereço IP de um dos controladores na matriz de armazenamento e clique em **Start Discovery**.

Pode levar alguns minutos para que o Unified Manager se conecte ao storage array especificado.



A mensagem Storage Array Not Accessible (Matriz de armazenamento não acessível) é exibida quando a conexão com o endereço IP do controlador especificado não for bem-sucedida.

4. Se solicitado, resolva quaisquer certificados autoassinados.

Como parte do processo de descoberta, o sistema verifica se os storages descobertos estão usando certificados por uma fonte confiável. Se não conseguir localizar um certificado digital para uma matriz de armazenamento, ele solicitará que você resolva o certificado que não está assinado por uma autoridade de certificação (CA) reconhecida adicionando uma exceção de segurança.

5. Se solicitado, resolva quaisquer certificados não confiáveis.

Certificados não confiáveis ocorrem quando um storage array tenta estabelecer uma conexão segura com o Unified Manager, mas a conexão não consegue confirmar como segura. Resolva certificados não confiáveis importando um certificado de autoridade de certificação (CA) emitido por um terceiro confiável.

6. Clique em **seguinte**.
7. **Opcional:** associar a matriz de armazenamento descoberta a um grupo: Na lista suspensa, selecione o grupo desejado a ser associado à matriz de armazenamento.

O grupo "All" (todos) é selecionado por predefinição.

8. Insira a senha de administrador do storage que você deseja adicionar ao domínio de gerenciamento e

clique em **OK**.

Depois de terminar

O storage array é adicionado ao Unified Manager e, se especificado, também é adicionado ao grupo selecionado.

Se a coleta automática de dados de suporte estiver ativada, os dados de suporte serão coletados automaticamente para um storage array que você adicionar.

Gerenciar arrays

Ver o status do storage array

O Unified Manager exibe o status de cada storage array descoberto.

Vá para a página **Gerenciar - todos**. Nesta página, você pode visualizar o status da conexão entre o Proxy de Serviços Web e esse storage array.

Os indicadores de status são descritos na tabela a seguir.

Estado	Indica
Ideal	O storage array está em um estado ideal. Não há problemas de certificado e a senha é válida.
Palavra-passe inválida	Foi fornecida uma palavra-passe inválida da matriz de armazenamento.
Certificado não fidedigno	Uma ou mais conexões com o storage não são confiáveis porque o certificado HTTPS é autoassinado e não foi importado, ou o certificado é assinado pela CA e os certificados raiz e intermediário da CA não foram importados.
Precisa de atenção	Há um problema com o storage array que requer a sua intervenção para corrigi-lo.
Bloqueio	O storage array está em um estado bloqueado.
Desconhecido	O storage array nunca foi contatado. Isso pode acontecer quando o Web Services Proxy está sendo iniciado e ainda não entrou em Contato com o storage array, ou o storage está offline e nunca foi contatado desde que o Web Services Proxy foi iniciado.
Offline	O Web Services Proxy já havia contatado o storage array, mas agora perdeu toda a conexão com ele.

Gerenciar um storage array individual

Você pode usar a opção Iniciar para abrir o System Manager baseado em navegador para um ou mais arrays de storage quando quiser executar operações de gerenciamento.

Passos

1. Na página Gerenciar, selecione um ou mais arrays de armazenamento que você deseja gerenciar.
2. Clique em **Launch**.

O sistema abre uma nova janela e exibe a página de login do System Manager.

3. Digite seu nome de usuário e senha e clique em **Log in**.

Altere as senhas do storage array

Você pode atualizar as senhas usadas para visualizar e acessar matrizes de armazenamento no Unified Manager.

Antes de começar

- Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de armazenamento.
- Você deve saber a senha atual para a matriz de armazenamento, que é definida no System Manager.

Sobre esta tarefa

Nesta tarefa, insira a senha atual de um storage array para que você possa acessá-lo no Unified Manager. Isso pode ser necessário se a senha do array tiver sido alterada no System Manager e, agora, ela também deve ser alterada no Unified Manager.

Passos

1. Na página Gerenciar, selecione um ou mais arrays de armazenamento.
2. Selecione **tarefas incomuns > fornecer senhas de storage de armazenamento**.
3. Insira a senha ou as senhas de cada matriz de armazenamento e clique em **Salvar**.

Remova os storage arrays do SANtricity Unified Manager

Você pode remover um ou mais arrays de storage se não quiser mais gerenciá-lo do Unified Manager.

Sobre esta tarefa

Não é possível acessar nenhum dos storages de armazenamento que você remover. Você pode, no entanto, estabelecer uma conexão com qualquer um dos storages removidos apontando um navegador diretamente para seu endereço IP ou nome de host.

A remoção de um storage array não afeta o storage array ou seus dados de forma alguma. Se uma matriz de armazenamento for removida acidentalmente, ela pode ser adicionada novamente.

Passos

1. Selecione a página **Gerenciar**.
2. Selecione um ou mais storages que você deseja remover.
3. Selecione **tarefas incomuns > Remove storage array**.

O storage array é removido de todas as visualizações no Gerenciador Unificado do SANtricity.

Importação de definições

Descrição geral das definições de importação

O recurso Importar configurações permite que você execute uma operação em lote para importar as configurações de uma matriz para várias matrizes. Esse recurso economiza tempo quando você precisa configurar vários arrays na rede.

Que definições podem ser importadas?

Você pode importar métodos de alerta, configurações do AutoSupport, configurações dos Serviços de diretório, configurações de armazenamento (como grupos de volumes e pools) e configurações do sistema (como balanceamento de carga automático).

Saiba mais:

- ["Como as Configurações de importação funcionam"](#)
- ["Requisitos para replicação de configurações de storage"](#)

Como faço para executar uma importação em lote?

Em uma matriz de armazenamento a ser usada como fonte, abra o System Manager e configure as configurações desejadas. Em seguida, no Unified Manager, vá para a página Gerenciar e importe as configurações para um ou mais arrays.

Saiba mais:

- ["Importar definições de alerta"](#)
- ["Importar definições do AutoSupport"](#)
- ["Importar definições dos serviços de diretório"](#)
- ["Importar definições de configuração de armazenamento"](#)
- ["Importar definições do sistema"](#)

Conceitos

Como as Configurações de importação funcionam

Você pode usar o Unified Manager para importar configurações de um storage array para vários storage arrays. O recurso Importar configurações é uma operação em lote que economiza tempo quando você precisa configurar vários arrays na rede.

Definições disponíveis para importação

As configurações a seguir podem ser importadas para vários storages:

- **Alertas** — métodos de alertas para enviar eventos importantes para administradores, usando e-mail, um servidor syslog ou um servidor SNMP.
- **AutoSupport** — um recurso que monitora a integridade de um storage array e envia envios automáticos para o suporte técnico.

- **Serviços de diretório** — Um método de autenticação de usuário gerenciado por meio de um servidor LDAP (Lightweight Directory Access Protocol) e serviço de diretório, como o Active Directory da Microsoft.
- **Configuração de armazenamento** — Configurações relacionadas ao seguinte:
 - Volumes (somente volumes espessos e não-repositórios)
 - Grupos de volume e pools
 - Atribuições de unidades hot spare
- **Configurações do sistema** — Configurações relacionadas ao seguinte:
 - Definições de digitalização de multimídia para um volume
 - Definições SSD
 - Balanceamento de carga automático (não inclui relatórios de conectividade de host)

Fluxo de trabalho de configuração

Para importar configurações, siga este fluxo de trabalho:

1. Em uma matriz de armazenamento a ser usada como origem, configure as configurações usando o System Manager.
2. Nos storages a serem usados como destinos, faça backup de sua configuração usando o System Manager.
3. No Unified Manager, vá para a página **Manage** e importe as configurações.
4. Na página **operações**, revise os resultados da operação Importar configurações.

Requisitos para replicação de configurações de storage

Antes de importar uma configuração de armazenamento de um storage array para outro, revise os requisitos e as diretrizes.

Compartimentos

- Os compartimentos em que os controladores residem devem ser idênticos nos arrays de origem e destino.
- As IDs de gaveta devem ser idênticas nos arrays de origem e destino.
- Os compartimentos de expansão devem ser preenchidos nos mesmos slots com os mesmos tipos de unidade (se a unidade for usada na configuração, o local das unidades não utilizadas não importa).

Controladores

- O tipo de controlador pode ser diferente entre os arrays de origem e destino (por exemplo, importando de um E2800 para um E5700), mas o tipo de gabinete RBOD deve ser idêntico.
- As HICs, incluindo os recursos DA DO host, devem ser idênticas entre os arrays de origem e destino.
- A importação de uma configuração duplex para simplex não é suportada; no entanto, a importação de simplex para duplex é permitida.
- As definições FDE não estão incluídas no processo de importação.

Estado

- Os arrays de destino devem estar no status ideal.

- O array de origem não precisa estar no status ideal.

Armazenamento

- A capacidade da unidade pode variar entre os arrays de origem e destino, desde que a capacidade de volume no destino seja maior do que a origem. (Um array de destino pode ter unidades de capacidade mais novas e maiores que não seriam totalmente configuradas em volumes pela operação de replicação.)
- Volumes de pool de discos de 64 TB ou maiores no array de origem impedirão o processo de importação nos destinos.
- Os volumes finos não estão incluídos no processo de importação.

Use importações de lote

Importar definições de alerta

Você pode importar configurações de alerta de um storage array para outros storage arrays. Esta operação em lote economiza tempo quando você precisa configurar vários arrays na rede.

Antes de começar

- Os alertas são configurados no System Manager para a matriz de armazenamento que você deseja usar como fonte (**Configurações > Alertas**).
- A configuração existente para os storages de armazenamento de destino é feita com backup no System Manager (**Configurações > sistema > Salvar configuração da matriz de armazenamento**).

Sobre esta tarefa

Você pode selecionar alertas de e-mail, SNMP ou syslog para a operação de importação. As definições importadas incluem:

- **Alertas por e-mail** — Um endereço de servidor de e-mail e os endereços de e-mail dos destinatários do alerta.
- **Alertas Syslog** — Um endereço de servidor syslog e uma porta UDP.
- **Alertas SNMP** — Um nome de comunidade e endereço IP para o servidor SNMP.

Passos

1. Na página Gerenciar, clique em **Importar configurações**.

O assistente Importar configurações é aberto.

2. Na caixa de diálogo Selecionar configurações, selecione **Email alerts**, **SNMP alerts** ou **Syslog alerts** e, em seguida, clique em **Next**.

Abre-se uma caixa de diálogo para selecionar a matriz de origem.

3. Na caixa de diálogo Selecionar fonte, selecione a matriz com as configurações que deseja importar e clique em **Avançar**.
4. Na caixa de diálogo Selecionar destinos, selecione um ou mais arrays para receber as novas configurações.



Matrizes de armazenamento com firmware abaixo de 8,50 não estão disponíveis para seleção. Além disso, uma matriz não aparece nesta caixa de diálogo se o Unified Manager não puder se comunicar com essa matriz (por exemplo, se estiver offline ou se tiver problemas de certificado, senha ou rede).

5. Clique em **Finish**.

A página operações exibe os resultados da operação de importação. Se a operação falhar, você pode clicar em sua linha para ver mais informações.

Resultados

Os storages de armazenamento de destino agora estão configurados para enviar alertas aos administradores por e-mail, SNMP ou syslog.

Importar definições do AutoSupport

Você pode importar uma configuração do AutoSupport de um storage array para outros storage arrays. Esta operação em lote economiza tempo quando você precisa configurar vários arrays na rede.

Antes de começar

- O AutoSupport é configurado no Gerenciador de sistema para o storage array que você deseja usar como origem (**suporte > Centro de suporte**).
- A configuração existente para os storages de armazenamento de destino é feita com backup no System Manager (**Configurações > sistema > Salvar configuração da matriz de armazenamento**).

Sobre esta tarefa

As configurações importadas incluem os recursos separados (Basic AutoSupport, AutoSupport OnDemand e Remote Diagnostics), a janela de manutenção, o método de entrega e o agendamento de envio.

Passos

1. Na página Gerenciar, clique em **Importar configurações**.

O assistente Importar configurações é aberto.

2. Na caixa de diálogo Selecionar configurações, selecione **AutoSupport** e clique em **Avançar**.

Abre-se uma caixa de diálogo para selecionar a matriz de origem.

3. Na caixa de diálogo Selecionar fonte, selecione a matriz com as configurações que deseja importar e clique em **Avançar**.

4. Na caixa de diálogo Selecionar destinos, selecione um ou mais arrays para receber as novas configurações.



Matrizes de armazenamento com firmware abaixo de 8,50 não estão disponíveis para seleção. Além disso, uma matriz não aparece nesta caixa de diálogo se o Unified Manager não puder se comunicar com essa matriz (por exemplo, se estiver offline ou se tiver problemas de certificado, senha ou rede).

5. Clique em **Finish**.

A página operações exibe os resultados da operação de importação. Se a operação falhar, você pode clicar em sua linha para ver mais informações.

Resultados

Os storages de armazenamento de destino agora são configurados com as mesmas configurações de AutoSupport que o array de origem.

Importar definições dos serviços de diretório

Você pode importar uma configuração de serviços de diretório de um storage array para outros storage arrays. Esta operação em lote economiza tempo quando você precisa configurar vários arrays na rede.

Antes de começar

- Os serviços de diretório são configurados no System Manager para a matriz de armazenamento que você deseja usar como fonte (**Configurações > Gerenciamento de Acesso**).
- A configuração existente para os storages de armazenamento de destino é feita com backup no System Manager (**Configurações > sistema > Salvar configuração da matriz de armazenamento**).

Sobre esta tarefa

As configurações importadas incluem o nome de domínio e URL de um servidor LDAP (Lightweight Directory Access Protocol), juntamente com os mapeamentos para os grupos de usuários do servidor LDAP para as funções predefinidas do storage array.

Passos

1. Na página Gerenciar, clique em **Importar configurações**.

O assistente Importar configurações é aberto.

2. Na caixa de diálogo Selecionar configurações, selecione **Serviços de diretório** e clique em **Avançar**.

Abre-se uma caixa de diálogo para selecionar a matriz de origem.

3. Na caixa de diálogo Selecionar fonte, selecione a matriz com as configurações que deseja importar e clique em **Avançar**.

4. Na caixa de diálogo Selecionar destinos, selecione um ou mais arrays para receber as novas configurações.



Matrizes de armazenamento com firmware abaixo de 8,50 não estão disponíveis para seleção. Além disso, uma matriz não aparece nesta caixa de diálogo se o Unified Manager não puder se comunicar com essa matriz (por exemplo, se estiver offline ou se tiver problemas de certificado, senha ou rede).

5. Clique em **Finish**.

A página operações exibe os resultados da operação de importação. Se a operação falhar, você pode clicar em sua linha para ver mais informações.

Resultados

Os storages de armazenamento de destino agora são configurados com os mesmos serviços de diretório que o array de origem.

Importar definições do sistema

Você pode importar a configuração do sistema de um storage array para outros storage arrays. Esta operação em lote economiza tempo quando você precisa configurar vários arrays na rede.

Antes de começar

- As configurações do sistema são configuradas no System Manager para a matriz de armazenamento que você deseja usar como origem.
- A configuração existente para os storages de armazenamento de destino é feita com backup no System Manager (**Configurações > sistema > Salvar configuração da matriz de armazenamento**).

Sobre esta tarefa

As definições importadas incluem definições de digitalização de multimídia para um volume, definições de SSD para controladores e balanceamento de carga automático (não inclui relatórios de conectividade do anfitrião).

Passos

1. Na página Gerenciar, clique em **Importar configurações**.

O assistente Importar configurações é aberto.

2. Na caixa de diálogo Selecionar configurações, selecione **sistema** e clique em **Avançar**.

Abre-se uma caixa de diálogo para selecionar a matriz de origem.

3. Na caixa de diálogo Selecionar fonte, selecione a matriz com as configurações que deseja importar e clique em **Avançar**.

4. Na caixa de diálogo Selecionar destinos, selecione um ou mais arrays para receber as novas configurações.



Matrizes de armazenamento com firmware abaixo de 8,50 não estão disponíveis para seleção. Além disso, uma matriz não aparece nesta caixa de diálogo se o Unified Manager não puder se comunicar com essa matriz (por exemplo, se estiver offline ou se tiver problemas de certificado, senha ou rede).

5. Clique em **Finish**.

A página operações exibe os resultados da operação de importação. Se a operação falhar, você pode clicar em sua linha para ver mais informações.

Resultados

Os storages de armazenamento de destino agora são configurados com as mesmas configurações do sistema que o array de origem.

Importar definições de configuração de armazenamento

Você pode importar a configuração de armazenamento de um storage array para outros storage arrays. Esta operação em lote economiza tempo quando você precisa configurar vários arrays na rede.

Antes de começar

- O armazenamento é configurado no Gerenciador de sistema do SANtricity para o storage array que você deseja usar como origem.
- A configuração existente para os storages de armazenamento de destino é feita com backup no System Manager (**Configurações > sistema > Salvar configuração da matriz de armazenamento**).
- Os arrays de origem e destino devem atender a estes requisitos:
 - As gavetas em que os controladores residem devem ser idênticas.
 - As IDs de gaveta devem ser idênticas.
 - Os compartimentos de expansão devem ser preenchidos nos mesmos slots com os mesmos tipos de unidades.
 - O tipo de compartimento RBOD deve ser idêntico.
 - As HICs, incluindo os recursos de Garantia de dados do host, devem ser idênticas.
 - Os arrays de destino devem estar no status ideal.
 - A capacidade de volume no array de destino é maior do que a capacidade do array de origem.
- Você entende as seguintes restrições:
 - A importação de uma configuração duplex para simplex não é suportada; no entanto, a importação de simplex para duplex é permitida.
 - Volumes de pool de discos de 64 TB ou maiores no array de origem impedirão o processo de importação nos destinos.
 - Os volumes finos não estão incluídos no processo de importação.

Sobre esta tarefa

As configurações importadas incluem volumes configurados (somente volumes espessos e não-repositórios), grupos de volumes, pools e atribuições de unidades hot spare.

Passos

1. Na página Gerenciar, clique em **Importar configurações**.

O assistente Importar configurações é aberto.

2. Na caixa de diálogo Selecionar configurações, selecione **Configuração de armazenamento** e clique em **Avançar**.

Abre-se uma caixa de diálogo para selecionar a matriz de origem.

3. Na caixa de diálogo Selecionar fonte, selecione a matriz com as configurações que deseja importar e clique em **Avançar**.
4. Na caixa de diálogo Selecionar destinos, selecione um ou mais arrays para receber as novas configurações.



Matrizes de armazenamento com firmware abaixo de 8,50 não estão disponíveis para seleção. Além disso, uma matriz não aparece nesta caixa de diálogo se o Unified Manager não puder se comunicar com essa matriz (por exemplo, se estiver offline ou se tiver problemas de certificado, senha ou rede).

5. Clique em **Finish**.

A página operações exibe os resultados da operação de importação. Se a operação falhar, você pode clicar em sua linha para ver mais informações.

Resultados

Os storage arrays de destino agora são configurados com a mesma configuração de armazenamento que o array de origem.

FAQs

Que definições serão importadas?

O recurso Importar configurações é uma operação em lote que carrega configurações de uma matriz de armazenamento para várias matrizes de armazenamento. As configurações importadas durante essa operação dependem de como o storage de armazenamento de origem é configurado no System Manager.

As seguintes configurações podem ser importadas para vários storages de armazenamento:

- **Alertas por e-mail** — as configurações incluem um endereço de servidor de e-mail e os endereços de e-mail dos destinatários do alerta.
- **Alertas Syslog** — as configurações incluem um endereço de servidor syslog e uma porta UDP.
- **Alertas SNMP** — as configurações incluem um nome de comunidade e endereço IP para o servidor SNMP.
- **AutoSupport** — as configurações incluem os recursos separados (AutoSupport Básico, OnDemand do AutoSupport e Diagnóstico remoto), a janela de manutenção, o método de entrega e o cronograma de envio.
- **Serviços de diretório** — a configuração inclui o nome de domínio e URL de um servidor LDAP (Lightweight Directory Access Protocol), juntamente com os mapeamentos para os grupos de usuários do servidor LDAP para as funções predefinidas do storage array.
- **Configuração de armazenamento** — as configurações incluem volumes (somente volumes espessos e somente não-repositórios), grupos de volumes, pools e atribuições de unidades hot spare.
- * Configurações do sistema* — as configurações incluem configurações de varredura de Mídia para um volume, cache SSD para controladores e balanceamento de carga automático (não inclui relatórios de conectividade do host).

Por que não vejo todos os meus arrays de armazenamento?

Durante a operação Importar configurações, alguns dos storages de armazenamento podem não estar disponíveis na caixa de diálogo seleção de destino.

Os storage arrays podem não aparecer pelos seguintes motivos:

- A versão do firmware é inferior a 8,50.
- A matriz de armazenamento está offline.
- O sistema não pode se comunicar com esse array (por exemplo, o array tem problemas de certificado, senha ou rede).

Grupos de array

Visão geral dos grupos

Na página Gerenciar grupos, você pode criar um conjunto de grupos de storage para facilitar o gerenciamento.

O que são grupos de matriz?

Você pode gerenciar sua infraestrutura física e virtualizada agrupando um conjunto de storage arrays. Você pode querer agrupar storages para facilitar a execução de tarefas de monitoramento ou geração de relatórios.

Existem dois tipos de grupos:

- **All group** — o grupo All é o grupo padrão e inclui todos os storages de armazenamento descobertos em sua organização. O grupo todos pode ser acessado a partir da vista principal.
- **Grupo criado pelo usuário** — Um grupo criado pelo usuário inclui os storages que você seleciona manualmente para adicionar a esse grupo. Os grupos criados pelo utilizador podem ser acedidos a partir da vista principal.

Como configuro grupos?

Na página Gerenciar grupos, você pode criar um grupo e adicionar matrizes a esse grupo.

Saiba mais:

- ["Configurar o grupo de storage array"](#)

Configurar o grupo de storage array

Você cria grupos de armazenamento e adiciona matrizes de armazenamento aos grupos.

A configuração de grupos é um procedimento de duas etapas.

Passo 1: Criar grupo

Primeiro você cria um grupo. O grupo de armazenamento define quais unidades fornecem o armazenamento que compõe o volume.

Passos

1. Na página Gerenciar, selecione **Gerenciar grupos** > **criar grupo de matriz de armazenamento**.
2. No campo **Nome**, digite um nome para o novo grupo.
3. Selecione as matrizes de armazenamento que pretende adicionar ao novo grupo.
4. Clique em **criar**.

Etapa 2: Adicionar storage array ao grupo

Você pode adicionar um ou mais arrays de armazenamento a um grupo criado pelo usuário.

Passos

1. Na exibição principal, selecione **Gerenciar** e, em seguida, selecione o grupo ao qual você deseja adicionar matrizes de armazenamento.
2. Selecione **Gerenciar grupos > Adicionar matrizes de armazenamento ao grupo**.
3. Selecione as matrizes de armazenamento que pretende adicionar ao grupo.
4. Clique em **Add**.

Remova os storages de armazenamento do grupo

Você pode remover um ou mais arrays de armazenamento gerenciados de um grupo se não quiser mais gerenciá-los de um grupo de armazenamento específico.

Sobre esta tarefa

A remoção de matrizes de armazenamento de um grupo não afeta a matriz de armazenamento ou os seus dados de forma alguma. Se o storage array for gerenciado pelo System Manager, você ainda poderá gerenciá-lo usando o navegador. Se um storage array for removido acidentalmente de um grupo, ele poderá ser adicionado novamente.

Passos

1. Na página Gerenciar, selecione **Gerenciar grupos > Remover matrizes de armazenamento do grupo**.
2. Na lista suspensa, selecione o grupo que contém os storages de armazenamento que deseja remover e clique na caixa de seleção ao lado de cada storage array que você deseja remover do grupo.
3. Clique em **Remover**.

Eliminar grupo de matrizes de armazenamento

Você pode remover um ou mais grupos de storage que não são mais necessários.

Sobre esta tarefa

Esta operação exclui apenas o grupo de matrizes de armazenamento. Os storage arrays associados ao grupo excluído permanecem acessíveis por meio da exibição Gerenciar tudo ou qualquer outro grupo ao qual está associado.

Passos

1. Na página Gerenciar, selecione **Gerenciar grupos > Excluir grupo de matrizes de armazenamento**.
2. Selecione um ou mais grupos de matrizes de armazenamento que pretende eliminar.
3. Clique em **Excluir**.

Renomeie o grupo de storage array

Você pode alterar o nome de um grupo de storage array quando o nome atual não for mais significativo ou aplicável.

Sobre esta tarefa

Tenha em mente estas diretrizes.

- Um nome pode consistir em letras, números e os caracteres especiais sublinhado (_), hífen (-) e libra (no). Se você escolher outros caracteres, uma mensagem de erro será exibida. Você é solicitado a escolher outro nome.
- Limite o nome para 30 caracteres. Todos os espaços à esquerda e à direita no nome são eliminados.
- Use um nome único e significativo que seja fácil de entender e lembrar.
- Evite nomes arbitrários ou nomes que rapidamente perderem seu significado no futuro.

Passos

1. Na exibição principal, selecione **Gerenciar** e, em seguida, selecione o grupo de storage que deseja renomear.
2. Selecione **Gerenciar grupos > Renomear storage array group**.
3. No campo **Nome do grupo**, digite um novo nome para o grupo.
4. Clique em **Renomear**.

Atualizações

Visão geral do Centro de atualizações

No Centro de Atualização, você pode gerenciar atualizações de software SANtricity os e NVSRAM para vários storages de armazenamento.

Como funcionam as atualizações?

Transfira o software SO mais recente e, em seguida, atualize um ou mais arrays.

Atualizar fluxo de trabalho

As etapas a seguir fornecem um fluxo de trabalho de alto nível para a realização de atualizações de software.

1. Você faz o download do arquivo de software mais recente do SANtricity os no site de suporte (um link está disponível no Unified Manager na página suporte). Salve o arquivo no sistema host de gerenciamento (o host onde você acessa o Unified Manager em um navegador) e, em seguida, descompacte o arquivo.
2. No Gerenciador Unificado, você carrega o arquivo de software do SANtricity os e o arquivo NVSRAM no repositório (uma área do servidor proxy de serviços da Web onde os arquivos são armazenados). Pode adicionar ficheiros a partir do **Centro de Atualização > Atualizar software SANtricity os** ou a partir do **Centro de Atualização > gerir repositório de software**.
3. Depois que os arquivos são carregados no repositório, você pode selecionar o arquivo a ser usado na atualização. Na página Atualizar o software SANtricity os (**Centro de atualização > Atualizar software SANtricity os**), selecione o ficheiro de software SANtricity os e o ficheiro NVSRAM. Depois de selecionar um ficheiro de software, é apresentada nesta página uma lista de matrizes de armazenamento compatíveis. Em seguida, selecione as matrizes de armazenamento que pretende atualizar com o novo software. (Não é possível selecionar matrizes incompatíveis.)
4. Em seguida, você pode iniciar uma transferência e ativação imediata de software, ou você pode optar por preparar os arquivos para ativação posteriormente. Durante o processo de atualização, o Unified Manager executa as seguintes tarefas:
 - a. Executa uma verificação de integridade nos storage arrays para determinar se existem condições que

possam impedir a conclusão da atualização. Se algum array falhar na verificação de integridade, você pode pular esse array específico e continuar a atualização para os outros, ou você pode parar todo o processo e solucionar problemas dos arrays que não passaram.

- b. Transfere os arquivos de atualização para cada controlador.
- c. Reinicializa os controladores e ativa o novo software SANtricity os, um controlador de cada vez. Durante a ativação, o arquivo SANtricity os existente é substituído pelo novo arquivo.



Você também pode especificar que o software está ativado posteriormente.

Atualização imediata ou faseada

Você pode ativar a atualização imediatamente ou colocá-la em fase posterior. Você pode optar por ativar mais tarde por estes motivos:

- **Hora do dia** — a ativação do software pode demorar muito tempo, então você pode querer esperar até que as cargas de e/S sejam mais leves. Dependendo da carga de e/S e do tamanho do cache, uma atualização da controladora normalmente pode levar entre 15 a 25 minutos para ser concluída. Os controladores reiniciam e fazem failover durante a ativação para que o desempenho possa ser menor do que o normal até que a atualização seja concluída.
- * Tipo de pacote* — você pode querer testar o novo software e firmware em uma matriz de armazenamento antes de atualizar os arquivos em outras matrizes de armazenamento.

Para ativar o software em estágio, vá para o **suporte > Centro de atualização** e clique em **Ativar** na área rotulada SANtricity os Controller Software upgrade.

Verificação de integridade

Uma verificação de integridade é executada como parte do processo de atualização, mas você também pode executar uma verificação de integridade separadamente antes de começar (vá para o **Centro de Atualização > Verificação de integridade pré-atualização**).

A verificação de integridade avalia todos os componentes do sistema de storage para garantir que a atualização possa prosseguir. As seguintes condições podem impedir a atualização:

- Unidades atribuídas com falha
- Peças sobressalentes quentes em uso
- Grupos de volumes incompletos
- Operações exclusivas em execução
- Volumes em falta
- Controlador em estado não ótimo
- Número excessivo de eventos de log
- Falha na validação da base de dados de configuração
- Unidades com versões antigas do DACstore

O que eu preciso saber antes de atualizar?

Antes de atualizar vários storages de armazenamento, revise as principais considerações como parte do Planejamento.

Versões atuais

Você pode exibir as versões atuais do software SANtricity os na página Gerenciar do Gerenciador Unificado para cada storage array descoberto. A versão é mostrada na coluna Software do SANtricity os. As informações de firmware e NVSRAM da controladora estão disponíveis em uma caixa de diálogo pop-up quando você clica na versão do SANtricity os em cada linha.

Outros componentes que exigem atualização

Como parte do processo de atualização, você também pode precisar atualizar o driver multipath/failover do host ou o driver HBA para que o host possa interagir com os controladores corretamente.

Para obter informações sobre compatibilidade, consulte o "[Matriz de interoperabilidade do NetApp](#)". Consulte também os procedimentos nos Guias expressos do seu sistema operativo. Os guias expressos estão disponíveis no "[Documentação do e-Series e do SANtricity](#)".

Controladores duplos

Se um storage array contiver dois controladores e você tiver um driver multipath instalado, o storage array poderá continuar processando e/S durante a atualização. Durante a atualização, ocorre o seguinte processo:

1. O controlador A faz failover de todos os LUNs para o controlador B.
2. A atualização ocorre no controlador A..
3. O controlador A recupera os LUNs e todos os LUNs do controlador B.
4. A atualização ocorre no controlador B.

Após a conclusão da atualização, talvez seja necessário redistribuir manualmente os volumes entre as controladoras para garantir que os volumes voltem para a controladora proprietária correta.

Atualizar software e firmware

Execute a verificação de integridade pré-atualização

Uma verificação de integridade é executada como parte do processo de atualização, mas você também pode executar uma verificação de integridade separadamente antes de começar. A verificação de integridade avalia os componentes do storage array para garantir que a atualização possa prosseguir.

Passos

1. Na visualização principal, selecione **Manage** e, em seguida, selecione menu:Upgrade Center [Pre-Upgrade Health Check] (Verificação de integridade pré-atualização).

A caixa de diálogo Verificação do estado de pré-atualização abre-se e lista todos os sistemas de armazenamento descobertos.

2. Se necessário, filtre ou classifique os sistemas de storage na lista para que você possa visualizar todos os sistemas que não estão no estado ideal atualmente.
3. Marque as caixas de seleção dos sistemas de armazenamento que você deseja executar na verificação de integridade.
4. Clique em **Iniciar**.

O progresso é mostrado na caixa de diálogo enquanto a verificação de integridade é executada.

5. Quando a verificação de integridade for concluída, você pode clicar nas elipses (...) à direita de cada linha para exibir mais informações e executar outras tarefas.



Se algum array falhar na verificação de integridade, você pode pular esse array específico e continuar a atualização para os outros, ou você pode parar todo o processo e solucionar problemas dos arrays que não passaram.

Atualize o SANtricity os

Atualize um ou mais storages de armazenamento com o software mais recente e NVSRAM para garantir que você tenha todos os recursos e correções de bugs mais recentes. A NVSRAM da controladora é um arquivo de controladora que especifica as configurações padrão para os controladores.

Antes de começar

- Os arquivos mais recentes do SANtricity os estão disponíveis no sistema host em que o proxy de serviços da Web do SANtricity e o Gerenciador Unificado estão em execução.
- Você sabe se deseja ativar a atualização de software agora ou mais tarde.

Você pode optar por ativar mais tarde por estes motivos:

- **Hora do dia** — a ativação do software pode demorar muito tempo, então você pode querer esperar até que as cargas de e/S sejam mais leves. Os controladores fazem failover durante a ativação, portanto, o desempenho pode ser menor do que o normal até que a atualização seja concluída.
- * Tipo de pacote* — você pode querer testar o novo software do sistema operacional em uma matriz de armazenamento antes de atualizar os arquivos em outras matrizes de armazenamento.



Os sistemas devem estar executando o SANtricity os 11.70.5 para atualizar para 11,80.x ou posterior.

Sobre esta tarefa

Mais uma vez



Risco de perda de dados ou risco de danos à matriz de armazenamento - não faça alterações na matriz de armazenamento enquanto a atualização estiver ocorrendo. Mantenha o poder do storage array.

Passos

1. Se o storage array contiver apenas uma controladora ou um driver multipath não estiver em uso, interrompa a atividade de e/S no storage array para evitar erros de aplicativos. Se o seu storage array tiver duas controladoras e você tiver um driver multipath instalado, não será necessário interromper a atividade de e/S.
2. Na exibição principal, selecione **Gerenciar** e, em seguida, selecione um ou mais storages que você deseja atualizar.
3. Selecione **Centro de Atualização** > **Atualizar software SANtricity os**.

A página Atualizar software SANtricity os é exibida.

4. Transfira o mais recente pacote de software do SANtricity os a partir do site de suporte da NetApp para a

sua máquina local.

- a. Clique em **Adicionar novo arquivo ao repositório de software**.
- b. Clique no link para encontrar os mais recentes **Downloads do SANtricity os**.
- c. Clique no link **Download Latest Release**.
- d. Siga as instruções restantes para transferir o ficheiro SANtricity os e o ficheiro NVSRAM para a sua máquina local.



O firmware assinado digitalmente é necessário na versão 8,42 e superior. Se tentar transferir firmware não assinado, é apresentado um erro e a transferência é cancelada.

5. Selecione o arquivo de software do sistema operacional e o arquivo NVSRAM que você deseja usar para atualizar os controladores:

- a. Na lista suspensa **Selecione um arquivo de software do SANtricity os**, selecione o arquivo do sistema operacional que você baixou para sua máquina local.

Se houver vários arquivos disponíveis, os arquivos serão classificados da data mais recente para a data mais antiga.



O repositório de software lista todos os arquivos de software associados ao Web Services Proxy. Se você não vir o arquivo que deseja usar, clique no link **Adicionar novo arquivo ao repositório de software**, para navegar até o local onde reside o arquivo do sistema operacional que você deseja adicionar.

- a. Na lista suspensa **Selecione um arquivo NVSRAM**, selecione o arquivo do controlador que deseja usar.

Se houver vários arquivos, os arquivos serão classificados da data mais recente para a data mais antiga.

6. Na tabela Matriz de armazenamento compatível, reveja os storages de armazenamento compatíveis com o arquivo de software do sistema operacional selecionado e selecione os storages que você deseja atualizar.

- As matrizes de armazenamento selecionadas na vista gerir e compatíveis com o ficheiro de firmware selecionado são selecionadas por predefinição na tabela Matriz de armazenamento compatível.
- As matrizes de armazenamento que não podem ser atualizadas com o ficheiro de firmware selecionado não são selecionáveis na tabela Matriz de armazenamento compatível, conforme indicado pelo estado **incompatível**.

7. **Opcional:** para transferir o arquivo de software para os storages de armazenamento sem ativá-los, marque a caixa de seleção **Transfira o software do sistema operacional para os storages, marque-o como encenado e ative posteriormente**.

8. Clique em **Iniciar**.

9. Dependendo se você escolheu ativar agora ou mais tarde, execute um dos seguintes procedimentos:

- Digite **TRANSFER** para confirmar que deseja transferir as versões propostas de software do sistema operacional nos arrays que você selecionou para atualizar e clique em **Transferir**.

Para ativar o software transferido, selecione **Centro de Atualização > Activate Staged os Software**.

- Digite **UPGRADE** para confirmar que deseja transferir e ativar as versões propostas de software do

sistema operacional nos arrays que você selecionou para atualizar e clique em **Upgrade**.

O sistema transfere o ficheiro de software para cada matriz de armazenamento selecionada para atualizar e, em seguida, ativa esse ficheiro iniciando uma reinicialização.

As seguintes ações ocorrem durante a operação de atualização:

- Uma verificação de integridade de pré-atualização é executada como parte do processo de atualização. A verificação de integridade da pré-atualização avalia todos os componentes do storage array para garantir que a atualização possa prosseguir.
 - Se qualquer verificação de integridade falhar em um storage array, a atualização será interrompida. Você pode clicar nas reticências (...) e selecionar **Salvar Registro** para revisar os erros. Você também pode optar por substituir o erro de verificação de integridade e clicar em **continuar** para continuar com a atualização.
 - Você pode cancelar a operação de atualização após a verificação de integridade da pré-atualização.
10. **Opcional:** uma vez concluída a atualização, você pode ver uma lista do que foi atualizado para uma matriz de armazenamento específica clicando nas reticências (...) e selecionando **Salvar Log**.

O arquivo é salvo na pasta Downloads do navegador com o nome `upgrade_log-<date>.json`.

Ativar o software SO faseado

Você pode optar por ativar o arquivo de software imediatamente ou esperar até um momento mais conveniente. Este procedimento pressupõe que optou por ativar o ficheiro de software posteriormente.

Sobre esta tarefa

Você pode transferir os arquivos de firmware sem ativá-los. Você pode optar por ativar mais tarde por estes motivos:

- **Hora do dia** — a ativação do software pode demorar muito tempo, então você pode querer esperar até que as cargas de e/S sejam mais leves. Os controladores reiniciam e fazem failover durante a ativação para que o desempenho possa ser menor do que o normal até que a atualização seja concluída.
- *** Tipo de pacote*** — você pode querer testar o novo software e firmware em uma matriz de armazenamento antes de atualizar os arquivos em outras matrizes de armazenamento.



Não é possível parar o processo de ativação depois de iniciado.

Passos

1. Na vista principal, selecione **Manage** (gerir). Se necessário, clique na coluna Status para classificar, na parte superior da página, todos os storages de armazenamento com o status "Atualização do sistema operacional (aguardando ativação)".
2. Selecione uma ou mais matrizes de armazenamento para as quais pretende ativar o software e, em seguida, selecione o **Centro de Atualização > Ativar software de SO faseado**.

As seguintes ações ocorrem durante a operação de atualização:

- Uma verificação de integridade pré-atualização é executada como parte do processo de ativação. A verificação de integridade da pré-atualização avalia todos os componentes do storage array para garantir que a ativação possa continuar.

- Se qualquer verificação de integridade falhar em um storage array, a ativação será interrompida. Você pode clicar nas reticências (...) e selecionar **Salvar Registro** para revisar os erros. Você também pode optar por substituir o erro de verificação de integridade e clicar em **continuar** para continuar com a ativação.
 - Pode cancelar a operação de ativação após a verificação do estado de pré-atualização. Após a conclusão bem-sucedida da verificação de integridade da pré-atualização, ocorre a ativação. O tempo de ativação depende da configuração do storage array e dos componentes que você está ativando.
3. **Opcional:** após a conclusão da ativação, você pode ver uma lista do que foi ativado para uma matriz de armazenamento específica clicando nas reticências (...) e selecionando **Salvar Log**.

O arquivo é salvo na pasta Downloads do navegador com o nome `activate_log-<date>.json`.

Gerenciar o repositório de software

O repositório de software lista todos os arquivos de software associados ao Web Services Proxy.

Se você não vir o arquivo que deseja usar, use a opção Gerenciar Repositório de software para importar um ou mais arquivos do SANtricity os para o sistema host onde o Proxy de serviços da Web e o Gerenciador Unificado estão sendo executados. Você também pode optar por excluir um ou mais arquivos do SANtricity os disponíveis no repositório de software.

Antes de começar

Se você estiver adicionando arquivos do SANtricity os, verifique se os arquivos do sistema operacional estão disponíveis no sistema local.

Passos

1. No modo de exibição principal, selecione **Manage** e, em seguida, selecione **Centro de Atualização > Manage Software Repository**.

A caixa de diálogo Gerenciar Repositório de Software é exibida.

2. Execute uma das seguintes ações:

Opção	Faça isso
Importar	<ol style="list-style-type: none"> a. Clique em Importar. b. Clique em Procurar e navegue até o local onde residem os arquivos do sistema operacional que você deseja adicionar. Os arquivos DO SO têm um nome de arquivo semelhante <code>N2800-830000-000.dlp</code> ao . c. Selecione um ou mais arquivos do sistema operacional que você deseja adicionar e clique em Importar.
Eliminar	<ol style="list-style-type: none"> a. Selecione um ou mais arquivos do SO que você deseja remover do repositório de software. b. Clique em Excluir.

Resultados

Se você selecionou importar, o(s) arquivo(s) será(ão) carregado(s) e validado(s). Se você selecionou excluir, os arquivos serão removidos do repositório de software.

Limpar o software de SO faseado

Você pode remover o software de sistema operacional em estágios para garantir que uma versão pendente não seja ativada inadvertidamente posteriormente. A remoção do software do SO em estágio não afeta a versão atual que está sendo executada nos storages de armazenamento.

Passos

1. Na visualização principal, selecione **Manage** e, em seguida, selecione **Centro de Atualização > Clear Staged os Software**.

A caixa de diálogo Clear Staged os Software abre e lista todos os sistemas de armazenamento descobertos com software pendente ou NVSRAM.

2. Se necessário, filtre ou classifique os sistemas de storage na lista para que você possa visualizar todos os sistemas que tenham feito o software em estágios.
3. Marque as caixas de seleção dos sistemas de armazenamento com software pendente que você deseja desmarcar.
4. Clique em **Limpar**.

O estado da operação é apresentado na caixa de diálogo.

Espelhamento

Visão geral do espelhamento

Use os recursos de espelhamento para replicar dados entre um storage array local e um storage array remoto, seja de forma assíncrona ou síncrona.



O espelhamento síncrono não está disponível no sistema de storage EF600 ou EF300.

O que é espelhamento?

As aplicações SANtricity incluem dois tipos de espelhamento: Assíncrono e síncrono. O espelhamento assíncrono copia volumes de dados sob demanda ou de acordo com o cronograma, o que minimiza ou evita o tempo de inatividade que pode resultar de corrupção ou perda de dados. O espelhamento síncrono replica volumes de dados em tempo real para garantir disponibilidade contínua.

Saiba mais:

- ["Como o espelhamento funciona"](#)
- ["Terminologia de espelhamento"](#)

Como faço para configurar o espelhamento?

Você configura o espelhamento assíncrono ou síncrono no Unified Manager e, em seguida, usa o System Manager para gerenciar sincronizações.

Saiba mais:

- ["Fluxo de trabalho de configuração de espelhamento"](#)
- ["Requisitos para uso do espelhamento"](#)
- ["Crie um par espelhado assíncrono"](#)
- ["Crie par espelhado síncrono"](#)

Conceitos

Como o espelhamento funciona

O Unified Manager inclui opções de configuração para os recursos de espelhamento do SANtricity, que permitem que os administradores repliquem dados entre dois storage arrays para proteção de dados.



O espelhamento síncrono não está disponível no sistema de storage EF600 ou EF300.

Tipos de espelhamento

As aplicações SANtricity incluem dois tipos de espelhamento: Assíncrono e síncrono.

O espelhamento assíncrono copia volumes de dados sob demanda ou de acordo com o cronograma, o que minimiza ou evita o tempo de inatividade que pode resultar de corrupção ou perda de dados. O espelhamento assíncrono captura o estado do volume primário em um determinado momento no tempo e copia apenas os dados que foram alterados desde a última captura de imagem. O site principal pode ser atualizado imediatamente e o site secundário pode ser atualizado como a largura de banda permite. As informações são armazenadas em cache e enviadas posteriormente, à medida que os recursos de rede ficam disponíveis. Esse tipo de espelhamento é ideal para processos periódicos, como backup e arquivamento.

O espelhamento síncrono replica volumes de dados em tempo real para garantir disponibilidade contínua. O objetivo é alcançar um objetivo de ponto de restauração (RPO) sem perda de dados ao ter uma cópia dos dados importantes disponível se um desastre ocorrer em um dos dois storage arrays. A cópia é idêntica aos dados de produção a cada momento, porque cada vez que uma gravação é feita no volume primário, uma gravação é feita no volume secundário. O host não recebe uma confirmação de que a gravação foi bem-sucedida até que o volume secundário seja atualizado com as alterações feitas no volume primário. Esse tipo de espelhamento é ideal para fins de continuidade dos negócios, como recuperação de desastres.

Diferenças entre tipos de espelhamento

A tabela a seguir descreve as principais diferenças entre os dois tipos de espelhamento.

Atributo	Assíncrono	Síncrono
Método de replicação	Point-in-time — o espelhamento é feito sob demanda ou automaticamente de acordo com uma programação definida pelo usuário.	Contínuo — o espelhamento é executado automaticamente continuamente, copiando dados de cada gravação de host.
Distância	Suporta longas distâncias entre arrays. Normalmente, a distância é limitada apenas pelas capacidades da rede e da tecnologia de extensão de canal.	Restrito a distâncias mais curtas entre arrays. Normalmente, a distância deve estar a cerca de 10 km (6,2 milhas) do storage array local para atender aos requisitos de latência e desempenho do aplicativo.
Método de comunicação	Uma rede IP ou Fibre Channel padrão.	Apenas rede Fibre Channel.
Tipos de volume	Padrão ou fino.	Apenas padrão.

Fluxo de trabalho de configuração de espelhamento

Você configura o espelhamento assíncrono ou síncrono no Unified Manager e, em seguida, usa o System Manager para gerenciar sincronizações.

Fluxo de trabalho de espelhamento assíncrono

O espelhamento assíncrono envolve o seguinte fluxo de trabalho:

1. Execute a configuração inicial no Unified Manager:
 - a. Selecione a matriz de armazenamento local como a origem para a transferência de dados.
 - b. Crie ou selecione um grupo de consistência de espelho existente, que é um contentor para o volume primário no array local e o volume secundário no array remoto. Os volumes primário e secundário são referidos como o "par espelhado". Se você estiver criando o grupo de consistência de espelho pela primeira vez, especifique se deseja executar sincronizações manuais ou agendadas.
 - c. Selecione um volume primário no storage array local e, em seguida, determine sua capacidade reservada. A capacidade reservada é a capacidade física alocada a ser usada para a operação de cópia.
 - d. Selecione um storage array remoto como o destino da transferência, um volume secundário e, em seguida, determine sua capacidade reservada.
 - e. Inicie a transferência de dados inicial do volume primário para o volume secundário. Dependendo do tamanho do volume, esta transferência inicial pode demorar várias horas.
2. Verifique o progresso da sincronização inicial:
 - a. No Unified Manager, inicie o System Manager para o array local.
 - b. No System Manager, visualize o status da operação de espelhamento. Quando o espelhamento estiver concluído, o status do par espelhado é "ótimo".

3. Opcionalmente, você pode reagendar ou realizar manualmente transferências de dados subsequentes no System Manager. Somente blocos novos e alterados são transferidos do volume primário para o volume secundário.



Como a replicação assíncrona é periódica, o sistema pode consolidar os blocos alterados e conservar a largura de banda da rede. Há impacto mínimo na taxa de transferência de gravação e na latência de gravação.

Fluxo de trabalho de espelhamento síncrono

O espelhamento síncrono envolve o seguinte fluxo de trabalho:

1. Execute a configuração inicial no Unified Manager:
 - a. Selecione uma matriz de armazenamento local como a origem para a transferência de dados.
 - b. Selecione um volume primário no storage array local.
 - c. Selecione uma matriz de armazenamento remota como destino para a transferência de dados e, em seguida, selecione um volume secundário.
 - d. Selecione as prioridades de sincronização e ressincronização.
 - e. Inicie a transferência de dados inicial do volume primário para o volume secundário. Dependendo do tamanho do volume, esta transferência inicial pode demorar várias horas.
2. Verifique o progresso da sincronização inicial:
 - a. No Unified Manager, inicie o System Manager para o array local.
 - b. No System Manager, visualize o status da operação de espelhamento. Quando o espelhamento estiver concluído, o status do par espelhado é "ótimo". Os dois arrays tentam permanecer sincronizados através de operações normais. Somente blocos novos e alterados são transferidos do volume primário para o volume secundário.
3. Opcionalmente, você pode alterar as configurações de sincronização no System Manager.



Como a replicação síncrona é contínua, o link de replicação entre os dois locais precisa fornecer recursos de largura de banda suficientes.

Terminologia de espelhamento

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

Prazo	Descrição
Storage array local	O storage array local é o storage array em que você está agindo.
Grupo de consistência do espelho	Um grupo de consistência de espelho é um recipiente para um ou mais pares espelhados. Para operações de espelhamento assíncrono, você precisa criar um grupo de consistência de espelhamento. Todos os pares espelhados em um grupo são ressincronizados simultaneamente, preservando assim um ponto de recuperação consistente. O espelhamento síncrono não usa grupos de consistência de espelho.

Prazo	Descrição
Par espelhado	<p>Um par espelhado é composto por dois volumes, um volume primário e um volume secundário.</p> <p>No espelhamento assíncrono, um par espelhado sempre pertence a um grupo de consistência de espelho. As operações de gravação são executadas primeiro no volume primário e, em seguida, replicadas no volume secundário. Cada par espelhado em um grupo de consistência de espelho compartilha as mesmas configurações de sincronização.</p>
Volume primário	O volume primário de um par espelhado é o volume de origem a ser espelhado.
Storage array remoto	O storage array remoto geralmente é designado como local secundário, que geralmente contém uma réplica dos dados em uma configuração de espelhamento.
Capacidade reservada	<p>A capacidade reservada é a capacidade alocada física usada para qualquer operação de serviço de cópia e objeto de storage. Não é diretamente legível pelo host.</p> <p>Esses volumes são necessários para que o controlador possa salvar persistentemente as informações necessárias para manter o espelhamento em um estado operacional. Eles contêm informações como Registros delta e dados copy-on-write.</p>
Volume secundário	O volume secundário de um par espelhado geralmente está localizado em um local secundário e contém uma réplica dos dados.
Sincronização	A sincronização ocorre na sincronização inicial entre o storage array local e o storage array remoto. A sincronização também ocorre quando os volumes primário e secundário ficam não sincronizados após uma interrupção da comunicação. Quando o link de comunicação está funcionando novamente, todos os dados não replicados são sincronizados com o storage array do volume secundário.

Requisitos para uso do espelhamento

Se você planeja configurar o espelhamento, tenha em mente os seguintes requisitos.

Unified Manager

- O serviço Web Services Proxy deve estar em execução.
- O Unified Manager deve estar em execução em seu host local por meio de uma conexão HTTPS.
- O Unified Manager deve mostrar certificados SSL válidos para a matriz de armazenamento. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando o Unified Manager e navegando para o **certificado** > **Gerenciamento de certificados**.

Storage arrays



O espelhamento síncrono não está disponível no storage array EF600 ou EF300.

- Você precisa ter dois storage arrays.
- Cada storage array deve ter duas controladoras.
- Os dois storage arrays devem ser descobertos no Unified Manager.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conectado à rede.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)
- Você deve saber a senha para os storages de armazenamento local e remoto.
- Você precisa ter capacidade livre suficiente no storage array remoto para criar um volume secundário igual ou maior que o volume principal que deseja espelhar.
- O espelhamento assíncrono é compatível com controladoras com portas de host Fibre Channel (FC) ou iSCSI, enquanto o espelhamento síncrono é compatível somente com controladoras com portas de host FC.

Requisitos de conectividade

O espelhamento por meio de uma interface FC (assíncrona ou síncrona) requer o seguinte:

- Cada controladora do storage array dedica sua porta de host FC de maior número às operações de espelhamento.
- Se o controlador tiver portas FC de base e portas FC da placa de interface do host (HIC), a porta numerada mais alta estará em um HIC. Qualquer host conectado à porta dedicada é desconectado e nenhuma solicitação de login do host é aceita. As solicitações de e/S nessa porta são aceitas somente de controladores que participam de operações de espelhamento.
- As portas de espelhamento dedicadas devem ser conectadas a um ambiente de malha FC que suporte as interfaces do serviço de diretório e serviço de nomes. Em particular, FC-AL e ponto a ponto não são compatíveis como opções de conectividade entre as controladoras que estão participando de relacionamentos espelhados.

O espelhamento através de uma interface iSCSI (apenas assíncrona) requer o seguinte:

- Ao contrário do FC, o iSCSI não requer uma porta dedicada. Quando o espelhamento assíncrono é usado em ambientes iSCSI, não é necessário dedicar nenhuma das portas iSCSI de front-end do storage array para uso com espelhamento assíncrono. Essas portas são compartilhadas para tráfego de espelhamento assíncrono e conexões de e/S de host para array.
- O controlador mantém uma lista de sistemas de armazenamento remoto com os quais o iniciador iSCSI tenta estabelecer uma sessão. A primeira porta que estabelece com êxito uma conexão iSCSI é usada para toda a comunicação subsequente com esse storage de armazenamento remoto. Se a comunicação falhar, uma nova sessão é tentada usando todas as portas disponíveis.
- As portas iSCSI são configuradas no nível da matriz, porta a porta. A comunicação entre controladores para mensagens de configuração e transferência de dados usa as configurações globais, incluindo configurações para:
 - VLAN: Os sistemas locais e remotos devem ter a mesma configuração de VLAN para se comunicar
 - Porta de escuta iSCSI

- Jumbo Frames
- Prioridade Ethernet



A comunicação do intercontrolador iSCSI deve usar uma porta de conexão de host e não a porta Ethernet de gerenciamento.

Candidatos a volume espelhado

- O nível RAID, os parâmetros de armazenamento em cache e o tamanho do segmento podem ser diferentes nos volumes primário e secundário de um par espelhado.



Para controladores EF600 e EF300, os volumes primário e secundário de um par espelhado assíncrono devem corresponder ao mesmo protocolo, nível da bandeja, tamanho do segmento, tipo de segurança e nível RAID. Pares espelhados assíncronos não elegíveis não aparecerão na lista de volumes disponíveis.

- O volume secundário deve ser pelo menos tão grande quanto o volume primário.
- Um volume pode participar de apenas um relacionamento de espelho.
- Para um par espelhado síncrono, os volumes primário e secundário devem ser volumes padrão. Não podem ser volumes finos ou volumes instantâneos.
- Para o espelhamento síncrono, há limites para o número de volumes compatíveis com um determinado storage array. Certifique-se de que o número de volumes configurados na matriz de armazenamento seja inferior ao limite suportado. Quando o espelhamento síncrono está ativo, os dois volumes de capacidade reservada criados contam para o limite de volume.
- Para o espelhamento assíncrono, o volume primário e o volume secundário devem ter os mesmos recursos de Segurança da Unidade.
 - Se o volume primário for compatível com FIPS, o volume secundário deve ser capaz de FIPS.
 - Se o volume principal for compatível com FDE, o volume secundário tem de ser capaz de FDE.
 - Se o volume principal não estiver usando o Drive Security, o volume secundário não deve estar usando o Drive Security.

Capacidade reservada

Espelhamento assíncrono:

- Um volume de capacidade reservada é necessário para um volume primário e para um volume secundário em um par espelhado para Registrar informações de gravação para recuperar de reinicializações do controlador e outras interrupções temporárias.
- Como o volume principal e o volume secundário em um par espelhado exigem capacidade reservada adicional, você precisa garantir que tenha capacidade livre disponível em ambos os storage arrays na relação espelhada.

Espelhamento síncrono:

- A capacidade reservada é necessária para um volume primário e para um volume secundário para 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 o volume principal e o volume secundário em um par espelhado exigem capacidade

reservada, você precisa garantir que tenha capacidade livre suficiente disponível em ambos os storage arrays que participam do relacionamento de espelhamento síncrono.

Recurso de segurança da unidade

- Se você estiver usando unidades com capacidade de segurança, o volume primário e o volume secundário devem ter configurações de segurança compatíveis. Esta restrição não é imposta; portanto, você deve verificá-la por conta própria.
- Se você estiver usando unidades com capacidade segura, o volume primário e o volume secundário deverão usar o mesmo tipo de unidade. Esta restrição não é imposta; portanto, você deve verificá-la por conta própria.
- Se estiver a utilizar o Data Assurance (DA), o volume primário e o volume secundário têm de ter as mesmas definições DE DA.

Configurar o espelhamento

Crie um par espelhado assíncrono

Para configurar o espelhamento assíncrono, você cria um par espelhado que inclui um volume primário no array local e um volume secundário no array remoto.

Antes de começar

Antes de criar um par espelhado, atenda aos seguintes requisitos do Unified Manager:

- O serviço Web Services Proxy deve estar em execução.
- O Unified Manager deve estar em execução em seu host local por meio de uma conexão HTTPS.
- O Unified Manager deve mostrar certificados SSL válidos para a matriz de armazenamento. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando o Unified Manager e navegando para o **certificado** > **Gerenciamento de certificados**.

Certifique-se também de atender aos seguintes requisitos para storage arrays e volumes:

- Cada storage array deve ter duas controladoras.
- Os dois storage arrays devem ser descobertos no Unified Manager.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conectado à rede.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)
- Você deve saber a senha para os storages de armazenamento local e remoto.
- Você precisa ter capacidade livre suficiente no storage array remoto para criar um volume secundário igual ou maior que o volume principal que deseja espelhar.
- Seus storage arrays locais e remotos são conectados por meio de uma malha Fibre Channel ou de uma interface iSCSI.
- Você criou os volumes primário e secundário que deseja usar na relação de espelhamento assíncrono.
- O volume secundário deve ser pelo menos tão grande quanto o volume primário.

Sobre esta tarefa

O processo para criar um par espelhado assíncrono é um procedimento de várias etapas.

Passo 1: Crie ou selecione um grupo de consistência de espelho

Nesta etapa, você cria um novo grupo de consistência de espelho ou seleciona um existente. Um grupo de consistência de espelho é um contendor para os volumes primário e secundário (o par espelhado) e especifica o método de ressincronização desejado (manual ou automático) para todos os pares no grupo.

Passos

1. Na página **Gerenciar**, selecione a matriz de armazenamento local que você deseja usar para a origem.
2. Selecione **ações > Create Asynchronous Mirrored Pair** (criar par espelhado assíncrono).

O assistente criar par espelhado assíncrono é aberto.

3. Selecione um grupo de consistência de espelho existente ou crie um novo.

Para selecionar um grupo existente, certifique-se de que **um grupo de consistência de espelho existente** está selecionado e selecione o grupo na tabela. Um grupo de consistência pode incluir vários pares espelhados.

Para criar um novo grupo, faça o seguinte:

- a. Selecione **Um novo grupo de consistência de espelho** e, em seguida, clique em **seguinte**.
- b. Insira um nome exclusivo que melhor descreva os dados nos volumes que serão espelhados entre os dois arrays de armazenamento. Um nome só pode consistir em letras, números e os caracteres especiais sublinhado (_), traço (-) e sinal de hash (#). Um nome não pode exceder 30 caracteres e não pode conter espaços.
- c. Selecione a matriz de armazenamento remoto na qual você deseja estabelecer uma relação de espelhamento com a matriz de armazenamento local.



Se a matriz de armazenamento remota estiver protegida por palavra-passe, o sistema solicitará uma palavra-passe.

- d. Escolha se deseja sincronizar os pares espelhados manualmente ou automaticamente:
 - **Manual** — Selecione essa opção para iniciar manualmente a sincronização de todos os pares espelhados nesse grupo. Observe que quando você deseja executar uma ressincronização mais tarde, você deve iniciar o System Manager para o storage array primário e, em seguida, ir para **armazenamento > Espelhamento assíncrono**, selecione o grupo na guia **Espelhar grupos** e selecione **mais > manualmente ressincronizar**.
 - **Automático** — Selecione o intervalo desejado em **minutos**, **horas** ou **dias**, desde o início da atualização anterior até o início da próxima atualização. Por exemplo, se o intervalo de sincronização for definido em 30 minutos e o processo de sincronização começar às 4:00 horas, o próximo processo será iniciado às 4:30 horas
- e. Selecione as definições de alerta pretendidas:
 - Para sincronizações manuais, especifique o limite (definido pela porcentagem da capacidade restante) para quando receber alertas.
 - Para sincronizações automáticas, você pode definir três métodos de alerta: Quando a sincronização não tiver sido concluída em um período específico de tempo, quando os dados do ponto de recuperação no array remoto forem mais antigos que um limite de tempo específico e quando a capacidade reservada estiver próxima a um limite específico (definido pela porcentagem da capacidade restante).

4. Selecione **seguinte** e vá para [Passo 2: Selecione o volume principal](#).

Se você definiu um novo grupo de consistência de espelho, o Unified Manager criará primeiro o grupo de consistência de espelho no storage array local e, em seguida, criará o grupo de consistência de espelho no storage array remoto. Você pode visualizar e gerenciar o grupo de consistência de espelho iniciando o System Manager para cada array.



Se o Unified Manager criar com êxito o grupo de consistência de espelho no storage array local, mas não conseguir criá-lo no storage array remoto, ele excluirá automaticamente o grupo de consistência de espelho do storage array local. Se ocorrer um erro enquanto o Unified Manager estiver tentando excluir o grupo de consistência de espelho, você deverá excluí-lo manualmente.

Passo 2: Selecione o volume principal

Nesta etapa, você seleciona o volume principal a ser usado na relação de espelhamento e aloca capacidade reservada. Quando você seleciona um volume primário no storage array local, o sistema exibe uma lista de todos os volumes elegíveis para esse par espelhado. Quaisquer volumes que não sejam elegíveis para serem usados não são exibidos nessa lista.

Todos os volumes adicionados ao grupo de consistência de espelho no storage array local terão a função principal na relação de espelhamento.

Passos

1. Na lista de volumes elegíveis, selecione um volume que pretende utilizar como volume principal e, em seguida, clique em **seguinte** para atribuir a capacidade reservada.
2. Na lista de candidatos elegíveis, selecione capacidade reservada para o volume primário.

Tenha em mente as seguintes diretrizes:

- A configuração padrão para capacidade reservada é de 20% da capacidade do volume base e, geralmente, essa capacidade é suficiente. Se você alterar a porcentagem, clique em **Atualizar candidatos**.
 - A capacidade necessária varia, dependendo da frequência e do tamanho das gravações de e/S no volume principal e por quanto tempo você precisa manter a capacidade.
 - Em geral, escolha uma capacidade maior para a capacidade reservada se uma ou ambas as condições existirem:
 - Você pretende manter o par espelhado por um longo período de tempo.
 - Uma grande porcentagem de blocos de dados mudará no volume primário devido à intensa atividade de e/S. Use dados históricos de desempenho ou outros utilitários do sistema operacional para ajudá-lo a determinar a atividade típica de e/S para o volume principal.
3. Selecione **seguinte** e vá para [Passo 3: Selecione o volume secundário](#).

Passo 3: Selecione o volume secundário

Nesta etapa, você seleciona o volume secundário a ser usado na relação de espelhamento e aloca sua capacidade reservada. Quando você seleciona um volume secundário no storage array remoto, o sistema exibe uma lista de todos os volumes elegíveis para esse par espelhado. Quaisquer volumes que não sejam elegíveis para serem usados não são exibidos nessa lista.

Todos os volumes adicionados ao grupo de consistência de espelho no storage array de armazenamento remoto terão a função secundária na relação de espelhamento.

Passos

1. Na lista de volumes elegíveis, selecione um volume que você deseja usar como volume secundário no par espelhado e clique em **Next** para alocar a capacidade reservada.
2. Na lista de candidatos elegíveis, selecione capacidade reservada para o volume secundário.

Tenha em mente as seguintes diretrizes:

- A configuração padrão para capacidade reservada é de 20% da capacidade do volume base e, geralmente, essa capacidade é suficiente. Se você alterar a porcentagem, clique em **Atualizar candidatos**.
 - A capacidade necessária varia, dependendo da frequência e do tamanho das gravações de e/S no volume principal e por quanto tempo você precisa manter a capacidade.
 - Em geral, escolha uma capacidade maior para a capacidade reservada se uma ou ambas as condições existirem:
 - Você pretende manter o par espelhado por um longo período de tempo.
 - Uma grande porcentagem de blocos de dados mudará no volume primário devido à intensa atividade de e/S. Use dados históricos de desempenho ou outros utilitários do sistema operacional para ajudá-lo a determinar a atividade típica de e/S para o volume principal.
3. Selecione **Finish** para concluir a sequência de espelhamento assíncrono.

Resultados

O Unified Manager realiza as seguintes ações:

- Inicia a sincronização inicial entre a matriz de armazenamento local e a matriz de armazenamento remoto.
- Cria a capacidade reservada para o par espelhado no storage array local e no storage array remoto.



Se o volume espelhado for um volume fino, apenas os blocos provisionados (capacidade alocada em vez de capacidade reportada) serão transferidos para o volume secundário durante a sincronização inicial. Isso reduz a quantidade de dados que devem ser transferidos para concluir a sincronização inicial.

Crie par espelhado síncrono

Para configurar o espelhamento síncrono, você cria um par espelhado que inclui um volume primário no array local e um volume secundário no array remoto.



Este recurso não está disponível no sistema de armazenamento EF600 ou EF300.

Antes de começar

Antes de criar um par espelhado, atenda aos seguintes requisitos do Unified Manager:

- O serviço Web Services Proxy deve estar em execução.
- O Unified Manager deve estar em execução em seu host local por meio de uma conexão HTTPS.
- O Unified Manager deve mostrar certificados SSL válidos para a matriz de armazenamento. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando o Unified Manager e navegando para o **certificado** > **Gerenciamento de certificados**.

Certifique-se também de atender aos seguintes requisitos para storage arrays e volumes:

- Os dois storage arrays que você planeja usar para espelhamento são descobertos no Unified Manager.
- Cada storage array deve ter duas controladoras.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conectado à rede.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)
- Você deve saber a senha para os storages de armazenamento local e remoto.
- Seus storage arrays locais e remotos são conectados por meio de uma malha Fibre Channel.
- Você criou os volumes primário e secundário que deseja usar na relação de espelhamento síncrono.
- O volume primário deve ser um volume padrão. Não pode ser um volume fino ou um volume instantâneo.
- O volume secundário deve ser um volume padrão. Não pode ser um volume fino ou um volume instantâneo.
- O volume secundário deve ser pelo menos tão grande quanto o volume primário.

Sobre esta tarefa

O processo para criar pares espelhados síncronos é um procedimento de várias etapas.

Passo 1: Selecione o volume principal

Nesta etapa, você seleciona o volume primário a ser usado na relação de espelhamento síncrono. Quando você seleciona um volume primário no storage array local, o sistema exibe uma lista de todos os volumes elegíveis para esse par espelhado. Quaisquer volumes que não sejam elegíveis para serem usados não são exibidos nessa lista. O volume selecionado mantém a função principal na relação de espelhamento.

Passos

1. Na página **Gerenciar**, selecione a matriz de armazenamento local que você deseja usar para a origem.
2. Selecione **ações > Create Synchronous Mirrored Pair** (criar par espelhado síncrono).

O assistente criar par espelhado síncrono é aberto.

3. Na lista de volumes elegíveis, selecione um volume que você deseja usar como o volume principal no espelho.
4. Selecione **seguinte** e vá para [Passo 2: Selecione o volume secundário](#).

Passo 2: Selecione o volume secundário

Nesta etapa, você seleciona o volume secundário a ser usado na relação de espelhamento. Quando você seleciona um volume secundário no storage array remoto, o sistema exibe uma lista de todos os volumes elegíveis para esse par espelhado. Quaisquer volumes que não sejam elegíveis para serem usados não são exibidos nessa lista. O volume selecionado manterá a função secundária na relação de espelho.

Passos

1. Selecione a matriz de armazenamento remoto na qual você deseja estabelecer uma relação de espelhamento com a matriz de armazenamento local.



Se a matriz de armazenamento remota estiver protegida por palavra-passe, o sistema solicitará uma palavra-passe.

- Os storage arrays são listados pelo nome do storage array. Se você não nomeou um storage array, ele será listado como "sem nome".
 - Se o storage array que você deseja usar não estiver na lista, verifique se ele foi descoberto no Unified Manager.
2. Na lista de volumes elegíveis, selecione um volume que pretende utilizar como volume secundário no espelho.



Se um volume secundário for escolhido com uma capacidade maior que o volume primário, a capacidade utilizável será restrita ao tamanho do volume primário.

3. Clique em **seguinte** e vá para [Passo 3: Selecione as configurações de sincronização](#).

Passo 3: Selecione as configurações de sincronização

Nesta etapa, você seleciona as configurações que determinam como os dados são sincronizados após uma interrupção de comunicação. Você pode definir a prioridade na qual o proprietário do controlador do volume primário ressincroniza os dados com o volume secundário após uma interrupção de comunicação. Você também deve selecionar a política de ressincronização, manual ou automática.

Passos

1. Utilize a barra deslizante para definir a prioridade de sincronização.

A prioridade de sincronização determina quanto dos recursos do sistema são usados para concluir a sincronização inicial e a operação de ressincronização após uma interrupção de comunicação em comparação com as solicitações de e/S de serviço.

A prioridade definida nesta caixa de diálogo aplica-se tanto ao volume primário como ao volume secundário. Você pode modificar a taxa no volume primário posteriormente acessando o System Manager e selecionando **armazenamento > Espelhamento síncrono > mais > Editar configurações**.

Existem cinco taxas de prioridade de sincronização:

- Mais baixo
- Baixo
- Média
- Alta
- Mais alto

Se a prioridade de sincronização estiver definida para a taxa mais baixa, a atividade de e/S será priorizada e a operação de ressincronização demorará mais tempo. Se a prioridade de sincronização estiver definida para a taxa mais alta, a operação de ressincronização será priorizada, mas a atividade de e/S para o storage array pode ser afetada.

2. Escolha se deseja ressincronizar os pares espelhados na matriz de armazenamento remoto manualmente ou automaticamente.
- **Manual** (a opção recomendada) — Selecione essa opção para exigir que a sincronização seja reiniciada manualmente após a comunicação ser restaurada para um par espelhado. Essa opção oferece a melhor oportunidade para recuperar dados.
 - **Automático** — Selecione esta opção para iniciar a ressincronização automaticamente após a comunicação ser restaurada para um par espelhado.

Para retomar manualmente a sincronização, vá para System Manager e selecione **armazenamento > Espelhamento síncrono**, realce o par espelhado na tabela e selecione **Resume** em **More**.

3. Clique em **Finish** para concluir a sequência de espelhamento síncrono.

Resultados

Quando o espelhamento é ativado, o sistema executa as seguintes ações:

- Inicia a sincronização inicial entre a matriz de armazenamento local e a matriz de armazenamento remoto.
- Define a prioridade de sincronização e a política de ressincronização.
- Reserva a porta com o número mais alto do HIC do controlador para transmissão de dados espelhados.

As solicitações de e/S recebidas nesta porta são aceitas somente pelo proprietário do controlador preferido remoto do volume secundário no par espelhado. (São permitidas reservas no volume primário.)

- Cria dois volumes de capacidade reservados, um para cada controlador, que são usados para Registrar informações de gravação para recuperar de reinicializações do controlador e outras interrupções temporárias.

A capacidade de cada volume é de 128 MiB. No entanto, se os volumes forem colocados em um pool, 4 GiB serão reservados para cada volume.

Depois de terminar

Vá para System Manager e selecione **Home > View Operations in Progress** (Visualizar operações em andamento) para ver o progresso da operação de espelhamento síncrono. Esta operação pode ser demorada e pode afetar o desempenho do sistema.

FAQs

O que eu preciso saber antes de criar um grupo de consistência de espelho?

Siga estas diretrizes antes de criar um grupo de consistência espelhada.

Atender aos seguintes requisitos do Unified Manager:

- O serviço Web Services Proxy deve estar em execução.
- O Unified Manager deve estar em execução em seu host local por meio de uma conexão HTTPS.
- O Unified Manager deve mostrar certificados SSL válidos para a matriz de armazenamento. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando o Unified Manager e navegando para o **certificado > Gerenciamento de certificados**.

Certifique-se também de atender aos seguintes requisitos para matrizes de armazenamento:

- Os dois storage arrays devem ser descobertos no Unified Manager.
- Cada storage array deve ter duas controladoras.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conetado à rede.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)

- Você deve saber a senha para os storages de armazenamento local e remoto.
- Seus storage arrays locais e remotos são conectados por meio de uma malha Fibre Channel ou de uma interface iSCSI.



O espelhamento síncrono não está disponível no sistema de storage EF600 ou EF300.

O que eu preciso saber antes de criar um par espelhado?

Antes de criar um par espelhado, siga estas diretrizes.

- Você precisa ter dois storage arrays.
- Cada storage array deve ter duas controladoras.
- Os dois storage arrays devem ser descobertos no Unified Manager.
- Cada controlador no array primário e no array secundário deve ter uma porta de gerenciamento Ethernet configurada e estar conectado à rede.
- As matrizes de armazenamento têm uma versão mínima de firmware de 7,84. (Cada um deles pode executar diferentes versões do sistema operacional.)
- Você deve saber a senha para os storages de armazenamento local e remoto.
- Você precisa ter capacidade livre suficiente no storage array remoto para criar um volume secundário igual ou maior que o volume principal que deseja espelhar.
- O espelhamento assíncrono é compatível com controladoras com portas de host Fibre Channel (FC) ou iSCSI, enquanto o espelhamento síncrono é compatível somente com controladoras com portas de host FC.



O espelhamento síncrono não está disponível no sistema de storage EF600 ou EF300.

Por que eu alteraria essa porcentagem?

A capacidade reservada costuma ser de 20% do volume base para operações de espelhamento assíncrono. Normalmente, essa capacidade é suficiente.

A capacidade necessária varia, dependendo da frequência e tamanho das gravações de e/S no volume base e quanto tempo você pretende usar a operação de serviço de cópia do objeto de armazenamento. Em geral, escolha uma porcentagem maior para a capacidade reservada se uma ou ambas as condições existirem:

- Se a vida útil de uma operação de serviço de cópia de um objeto de armazenamento específico será muito longa.
- Se uma grande porcentagem de blocos de dados mudar no volume base devido à intensa atividade de e/S. Use dados históricos de desempenho ou outros utilitários do sistema operacional para ajudá-lo a determinar a atividade típica de e/S para o volume base.

Por que vejo mais de um candidato à capacidade reservada?

Se houver mais de um volume em um pool ou grupo de volumes que atenda ao valor percentual de capacidade selecionado para o objeto de armazenamento, você verá vários candidatos.

Você pode atualizar a lista de candidatos recomendados alterando a porcentagem de espaço físico da

unidade que deseja reservar no volume base para operações de serviço de cópia. Os melhores candidatos são exibidos com base na sua seleção.

Por que não vejo todos os meus volumes?

Ao selecionar um volume primário para um par espelhado, uma lista mostra todos os volumes elegíveis.

Quaisquer volumes que não sejam elegíveis para serem usados não são exibidos nessa lista. Os volumes podem não ser elegíveis por qualquer um dos seguintes motivos:

- O volume não é ideal.
- O volume já está participando de uma relação de espelhamento.
- Para o espelhamento síncrono, os volumes primário e secundário em um par espelhado devem ser volumes padrão. Não podem ser volumes finos ou volumes instantâneos.
- Para o espelhamento assíncrono, os thin volumes devem ter a expansão automática ativada.



Para controladores EF600 e EF300, os volumes primário e secundário de um par espelhado assíncrono devem corresponder ao mesmo protocolo, nível da bandeja, tamanho do segmento, tipo de segurança e nível RAID. Pares espelhados assíncronos não elegíveis não aparecerão na lista de volumes disponíveis.

Por que não vejo todos os volumes no storage array remoto?

Quando você está selecionando um volume secundário no storage array remoto, uma lista mostra todos os volumes elegíveis para esse par espelhado.

Quaisquer volumes que não sejam elegíveis para serem usados, não serão exibidos nessa lista. Os volumes não podem ser elegíveis por qualquer um dos seguintes motivos:

- O volume é um volume não padrão, como um volume instantâneo.
- O volume não é ideal.
- O volume já está participando de uma relação de espelhamento.
- Para espelhamento assíncrono, os atributos de volume fino entre o volume primário e o volume secundário não correspondem.
- Se estiver a utilizar o Data Assurance (DA), o volume primário e o volume secundário têm de ter as mesmas definições DE DA.
 - Se o volume primário for DA ativado, o volume secundário tem de ser DA ativado.
 - Se o volume primário não estiver ativado DA, o volume secundário não deve ser ativado DA.
- Para o espelhamento assíncrono, o volume primário e o volume secundário devem ter os mesmos recursos de Segurança da Unidade.
 - Se o volume primário for compatível com FIPS, o volume secundário deve ser capaz de FIPS.
 - Se o volume principal for compatível com FDE, o volume secundário tem de ser capaz de FDE.
 - Se o volume principal não estiver usando o Drive Security, o volume secundário não deve estar usando o Drive Security.

Qual o impacto que a prioridade de sincronização tem nas taxas de sincronização?

A prioridade de sincronização define quanto tempo de processamento é alocado para atividades de sincronização em relação ao desempenho do sistema.

O proprietário do controlador do volume primário executa esta operação em segundo plano. Ao mesmo tempo, o proprietário do controlador processa gravações de e/S locais no volume principal e gravações remotas associadas no volume secundário. Como a ressincronização desvia os recursos de processamento do controlador da atividade de e/S, a ressincronização pode ter um impacto no desempenho do aplicativo host.

Mantenha essas diretrizes em mente para ajudá-lo a determinar quanto tempo uma prioridade de sincronização pode levar e como as prioridades de sincronização podem afetar o desempenho do sistema.

Estas tarifas prioritárias estão disponíveis:

- Mais baixo
- Baixo
- Média
- Alta
- Mais alto

A taxa de prioridade mais baixa suporta o desempenho do sistema, mas a ressincronização leva mais tempo. A taxa de prioridade mais alta é compatível com a ressincronização, mas o desempenho do sistema pode estar comprometido.

Estas orientações aproximam aproximadamente as diferenças entre as prioridades.

Taxa de prioridade para sincronização completa	Tempo decorrido em comparação com a taxa de sincronização mais elevada
Mais baixo	Aproximadamente oito vezes, desde que na taxa de prioridade mais alta.
Baixo	Aproximadamente seis vezes, desde que na taxa de prioridade mais alta.
Média	Aproximadamente três vezes e meia, desde que com a taxa de prioridade mais alta.
Alta	Aproximadamente o dobro do tempo na taxa de prioridade mais alta.

As cargas de tamanho de volume e taxa de e/S do host afetam as comparações de tempo de sincronização.

Por que é recomendável usar uma política de sincronização manual?

A ressincronização manual é recomendada porque permite gerenciar o processo de ressincronização de uma forma que forneça a melhor oportunidade para recuperar dados.

Se você usar uma política de resincronização automática e ocorrerem problemas de comunicação intermitente durante a resincronização, os dados no volume secundário poderão ser corrompidos temporariamente. Quando a resincronização é concluída, os dados são corrigidos.

Certificados

Descrição geral dos certificados

O Gerenciamento de certificados permite criar solicitações de assinatura de certificado (CSRs), importar certificados e gerenciar certificados existentes.

O que são certificados?

Certificados são arquivos digitais que identificam entidades online, como sites e servidores, para comunicações seguras na internet. Existem dois tipos de certificados: Um certificado *assinado* é validado por uma autoridade de certificação (CA) e um certificado *autoassinado* é validado pelo proprietário da entidade em vez de um terceiro.

Saiba mais:

- ["Como os certificados funcionam"](#)
- ["Terminologia do certificado"](#)

Como faço para configurar certificados?

No Gerenciamento de certificados, você pode configurar certificados para a estação de gerenciamento que hospeda o Unified Manager e também importar certificados para os controladores nos arrays.

Saiba mais:

- ["Use certificados assinados pela CA para o sistema de gerenciamento"](#)
- ["Importar certificados para matrizes"](#)

Conceitos

Como os certificados funcionam

Certificados são arquivos digitais que identificam entidades online, como sites e servidores, para comunicações seguras na internet.

Certificados assinados

Os certificados garantem que as comunicações da Web sejam transmitidas de forma encriptada, privada e inalterada, apenas entre o servidor e o cliente especificados. Com o Unified Manager, você pode gerenciar certificados para o navegador em um sistema de gerenciamento de host e as controladoras nos storage arrays descobertos.

Um certificado pode ser assinado por uma autoridade confiável ou pode ser autoassinado. "Assinatura" significa simplesmente que alguém validou a identidade do proprietário e determinou que seus dispositivos podem ser confiáveis. As matrizes de armazenamento são fornecidas com um certificado auto-assinado gerado automaticamente em cada controlador. Você pode continuar usando os certificados autoassinados ou obter certificados assinados pela CA para uma conexão mais segura entre os controladores e os sistemas

host.



Embora os certificados assinados pela CA forneçam melhor proteção de segurança (por exemplo, evitando ataques man-in-the-middle), eles também exigem taxas que podem ser caras se você tiver uma rede grande. Em contraste, os certificados autoassinados são menos seguros, mas são gratuitos. Portanto, os certificados autoassinados são mais usados para ambientes de teste internos, não em ambientes de produção.

Um certificado assinado é validado por uma autoridade de certificação (CA), que é uma organização de terceiros confiável. Os certificados assinados incluem detalhes sobre o proprietário da entidade (normalmente, um servidor ou site), data de emissão e expiração do certificado, domínios válidos para a entidade e uma assinatura digital composta por letras e números.

Quando você abre um navegador e insere um endereço da Web, o sistema executa um processo de verificação de certificados em segundo plano para determinar se você está se conectando a um site que inclui um certificado válido assinado pela CA. Geralmente, um site protegido com um certificado assinado inclui um ícone de cadeado e uma designação https no endereço. Se você tentar se conectar a um site que não contenha um certificado assinado pela CA, o navegador exibirá um aviso de que o site não está seguro.

A CA toma medidas para verificar sua identidade durante o processo de inscrição. Eles podem enviar um e-mail para sua empresa registrada, verificar seu endereço comercial e executar uma verificação HTTP ou DNS. Quando o processo de aplicação estiver concluído, a CA envia arquivos digitais para serem carregados em um sistema de gerenciamento de host. Normalmente, esses arquivos incluem uma cadeia de confiança, como segue:

- **Root** — na parte superior da hierarquia está o certificado raiz, que contém uma chave privada usada para assinar outros certificados. A raiz identifica uma organização de CA específica. Se você usar a mesma CA para todos os dispositivos de rede, precisará de apenas um certificado raiz.
- **Intermediate** — ramificação fora da raiz são os certificados intermediários. A CA emite um ou mais certificados intermediários para atuar como intermediários entre uma raiz protegida e certificados de servidor.
- **Servidor** — na parte inferior da cadeia está o certificado do servidor, que identifica sua entidade específica, como um site ou outro dispositivo. Cada controlador em um storage array requer um certificado de servidor separado.

Certificados autoassinados

Cada controladora no storage inclui um certificado pré-instalado e autoassinado. Um certificado autoassinado é semelhante a um certificado assinado pela CA, exceto que ele é validado pelo proprietário da entidade em vez de um terceiro. Como um certificado assinado pela CA, um certificado autoassinado contém sua própria chave privada e também garante que os dados sejam criptografados e enviados por uma conexão HTTPS entre um servidor e um cliente.

Os certificados autoassinados não são "confiáveis" pelos navegadores. Cada vez que você tenta se 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 que você prossiga para o site; ao fazê-lo, você está essencialmente aceitando o certificado auto-assinado.

Certificados para Unified Manager

A interface do Unified Manager é instalada com o Web Services Proxy em um sistema host. Quando você abre um navegador e tenta se conectar ao Unified Manager, o navegador tenta verificar se o host é uma fonte confiável verificando se há um certificado digital. Se o navegador não localizar um certificado assinado pela CA para o servidor, ele abrirá uma mensagem de aviso. A partir daí, você pode continuar para o site para

aceitar o certificado autoassinado para essa sessão. Ou, você pode obter certificados digitais assinados de uma CA para que você não veja mais a mensagem de aviso.

Certificados para controladores

Durante uma sessão do Unified Manager, você pode ver mensagens de segurança adicionais quando tentar acessar um controlador que não tenha um certificado assinado pela CA. Nesse caso, você pode confiar permanentemente no certificado autoassinado ou importar os certificados assinados pela CA para os controladores para que o servidor Proxy de Serviços da Web possa autenticar solicitações de clientes recebidas desses controladores.

Terminologia do certificado

Os termos a seguir se aplicam ao gerenciamento de certificados.

Prazo	Descrição
CA	Uma autoridade de certificação (CA) é uma entidade confiável que emite documentos eletrônicos, chamados certificados digitais, para segurança na Internet. Esses certificados identificam proprietários de sites, o que permite conexões seguras entre clientes e servidores.
CSR	Uma solicitação de assinatura de certificado (CSR) é uma mensagem enviada de um requerente para uma autoridade de certificação (CA). O CSR valida as informações que a CA precisa para emitir um certificado.
Certificado	Um certificado identifica o proprietário de um site para fins de segurança, o que impede que atacantes personifiquem o site. O certificado contém informações sobre o proprietário do site e a identidade da entidade confiável que certifica (assina) essas informações.
Cadeia de certificados	Uma hierarquia de arquivos que adiciona uma camada de segurança aos certificados. Normalmente, a cadeia inclui um certificado raiz na parte superior da hierarquia, um ou mais certificados intermediários e os certificados de servidor que identificam as entidades.
Certificado intermédio	Um ou mais certificados intermediários ramificam da raiz na cadeia de certificados. A CA emite um ou mais certificados intermediários para atuar como intermediários entre uma raiz protegida e certificados de servidor.
Armazenamento de chaves	Um keystore é um repositório no seu sistema de gerenciamento de host que contém chaves privadas, juntamente com suas chaves públicas e certificados correspondentes. Essas chaves e certificados identificam suas próprias entidades, como os controladores.
Certificado raiz	O certificado raiz está no topo da hierarquia na cadeia de certificados e contém uma chave privada usada para assinar outros certificados. A raiz identifica uma organização de CA específica. Se você usar a mesma CA para todos os dispositivos de rede, precisará de apenas um certificado raiz.

Prazo	Descrição
Certificado assinado	Um certificado validado por uma autoridade de certificação (CA). Este arquivo de dados contém uma chave privada e garante que os dados sejam enviados de forma criptografada entre um servidor e um cliente através de uma conexão HTTPS. Além disso, um certificado assinado inclui detalhes sobre o proprietário da entidade (normalmente, um servidor ou site) e uma assinatura digital composta por letras e números. Um certificado assinado usa uma cadeia de confiança e, portanto, é mais frequentemente usado em ambientes de produção. Também referido como um "certificado assinado pela CA" ou um "certificado de gestão".
Certificado auto-assinado	Um certificado autoassinado é validado pelo proprietário da entidade. Este arquivo de dados contém uma chave privada e garante que os dados sejam enviados de forma criptografada entre um servidor e um cliente através de uma conexão HTTPS. Também inclui uma assinatura digital composta por letras e números. Um certificado autoassinado não usa a mesma cadeia de confiança que um certificado assinado pela CA e, portanto, é mais frequentemente usado em ambientes de teste. Também referido como um certificado "pré-instalado".
Certificado do servidor	O certificado do servidor está na parte inferior da cadeia de certificados. Ele identifica sua entidade específica, como um site ou outro dispositivo. Cada controlador em um sistema de storage requer um certificado de servidor separado.
Loja de confiança	Um repositório de confiança é um repositório que contém certificados de terceiros confiáveis, como CAs.

Use certificados assinados pela CA para o sistema de gerenciamento

Você pode obter e importar certificados assinados pela CA para acesso seguro ao sistema de gerenciamento que hospeda o Unified Manager.

Antes de começar

Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.

Sobre esta tarefa

O uso de certificados assinados pela CA é um procedimento de três etapas.

Passo 1: Complete um arquivo CSR

Primeiro, é necessário gerar um arquivo de solicitação de assinatura de certificado (CSR), que identifique sua organização e o sistema host onde o Proxy de Serviços Web e o Unified Manager estão instalados.



Como alternativa, você pode gerar um arquivo CSR usando uma ferramenta como OpenSSL e pular para [Passo 2: Envie o arquivo CSR](#).

Passos

1. Selecione **Gerenciamento de certificados**.

2. Na guia Gerenciamento, selecione **Complete CSR**.
3. Insira as seguintes informações e clique em **Next**:
 - **Organização** — o nome completo e legal de sua empresa ou organização. Inclua sufixos, como Inc. Ou Corp.
 - * Unidade organizacional (opcional) * — a divisão da sua organização que está a lidar com o certificado.
 - **Cidade/localidade** — a cidade onde o seu sistema de acolhimento ou negócio está localizado.
 - **Estado/região (opcional)** — o estado ou a região onde o seu sistema anfitrião ou negócio está localizado.
 - **Código ISO do país** — o código ISO de dois dígitos do seu país (Organização Internacional para Padronização), como os EUA.
4. Insira as seguintes informações sobre o sistema host onde o Proxy de Serviços Web está instalado:
 - **Nome comum** — o endereço IP ou o nome DNS do sistema host onde o Proxy de Serviços Web está instalado. Verifique se esse endereço está correto; ele deve corresponder exatamente ao que você digita para acessar o Unified Manager no navegador. Não inclua http:// ou https://. O nome DNS não pode começar com um curinga.
 - **Endereços IP alternativos** — se o nome comum for um endereço IP, você pode opcionalmente inserir quaisquer endereços IP adicionais ou aliases para o sistema host. Para várias entradas, use um formato delimitado por vírgulas.
 - **Nomes DNS alternativos** — se o nome comum for um nome DNS, insira quaisquer nomes DNS adicionais para o sistema host. Para várias entradas, use um formato delimitado por vírgulas. Se não houver nomes DNS alternativos, mas você inseriu um nome DNS no primeiro campo, copie esse nome aqui. O nome DNS não pode começar com um curinga.
5. Certifique-se de que as informações do host estão corretas. Se não estiver, os certificados retornados da CA falharão quando você tentar importá-los.
6. Clique em **Finish**.
7. Vá para [Passo 2: Envie o arquivo CSR](#).

Passo 2: Envie o arquivo CSR

Depois de criar um arquivo de solicitação de assinatura de certificado (CSR), você o enviará a uma Autoridade de Certificação (CA) para receber certificados de gerenciamento assinados para o sistema que hospeda o Unified Manager e o Proxy de Serviços da Web.



Os sistemas e-Series exigem o formato PEM (codificação ASCII Base64) para certificados assinados, que inclui os seguintes tipos de arquivo: .pem, .crt, .cer ou .key.

Passos

1. Localize o ficheiro CSR transferido.

A localização da pasta do download depende do seu navegador.

2. Envie o arquivo CSR para uma CA (por exemplo, VeriSign ou DigiCert) e solicite certificados assinados no formato PEM.



Depois de enviar um arquivo CSR para a CA, NÃO regenere outro arquivo CSR.

Sempre que você gera um CSR, o sistema cria um par de chaves privadas e públicas. A chave pública faz parte da CSR, enquanto a chave privada é mantida no keystore do sistema. Quando você recebe os certificados assinados e os importa, o sistema garante que as chaves privadas e públicas sejam o par original. Se as chaves não corresponderem, os certificados assinados não funcionarão e você deverá solicitar novos certificados à CA.

3. Quando a CA retornar os certificados assinados, vá para [Passo 3: Importar certificados de gestão](#).

Passo 3: Importar certificados de gestão

Depois de receber certificados assinados da Autoridade de Certificação (CA), importe os certificados para o sistema host onde a interface Web Services Proxy e Unified Manager estão instalados.

Antes de começar

- Você recebeu certificados assinados da CA. Esses arquivos incluem o certificado raiz, um ou mais certificados intermediários e o certificado do servidor.
- Se a CA forneceu um arquivo de certificado encadeado (por exemplo, um arquivo .p7b), você deve descompactar o arquivo encadeado em arquivos individuais: O certificado raiz, um ou mais certificados intermediários e o certificado do servidor. Você pode usar o utilitário Windows `certmgr` para descompactar os arquivos (clique com o botão direito do Mouse e selecione **todas as tarefas** > **Exportar**). A codificação base-64 é recomendada. Quando as exportações estiverem concluídas, um arquivo CER é exibido para cada arquivo de certificado na cadeia.
- Você copiou os arquivos de certificado para o sistema host onde o Proxy de Serviços Web está sendo executado.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Na guia Gerenciamento, selecione **Importar**.

Abre-se uma caixa de diálogo para importar os ficheiros de certificado.

3. Clique em **Procurar** para selecionar primeiro os arquivos de certificado raiz e intermediário e, em seguida, selecione o certificado do servidor. Se você gerou o CSR a partir de uma ferramenta externa, você também deve importar o arquivo de chave privada que foi criado juntamente com o CSR.

Os nomes de arquivo são exibidos na caixa de diálogo.

4. Clique em **Importar**.

Resultados

Os arquivos são carregados e validados. As informações do certificado são exibidas na página Gerenciamento de certificados.

Repor certificados de gestão

Você pode reverter o certificado de gerenciamento para o estado original, autoassinado de fábrica.

Antes de começar

Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança.

Caso contrário, as funções do certificado não aparecem.

Sobre esta tarefa

Esta tarefa exclui o certificado de gerenciamento atual do sistema host onde o Proxy de serviços da Web e o Unified Manager estão instalados. Depois que o certificado é redefinido, o sistema host reverte para usando o certificado autoassinado.

Passos

1. Selecione **Definições > certificados**.
2. Selecione a guia **Array Management** e, em seguida, selecione **Reset**.

Uma caixa de diálogo confirmar certificado de gerenciamento de redefinição é aberta.

3. Digite `reset` o campo e clique em **Reset**.

Após a atualização do navegador, o navegador pode bloquear o acesso ao site de destino e informar que o site está usando HTTP Strict Transport Security. Essa condição surge quando você volta para certificados autoassinados. Para limpar a condição que está bloqueando o acesso ao destino, você deve limpar os dados de navegação do navegador.

Resultados

O sistema reverte para o uso do certificado autoassinado do servidor. Como resultado, o sistema solicita aos usuários que aceitem manualmente o certificado autoassinado para suas sessões.

Use certificados de matriz

Importar certificados para matrizes

Se necessário, você pode importar certificados para os storages de armazenamento para que eles possam se autenticar com o sistema que hospeda o Unified Manager. Os certificados podem ser assinados por uma autoridade de certificação (CA) ou podem ser autoassinados.

Antes de começar

- Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.
- Se você estiver importando certificados confiáveis, os certificados devem ser importados para os controladores de storage usando o System Manager.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione a guia **Trusted**.

Esta página mostra todos os certificados reportados para os storages de armazenamento.

3. Selecione um **Importar > certificados** para importar um certificado de CA ou **Importar > certificados de matriz de armazenamento autoassinados** para importar um certificado autoassinado.

Para limitar a exibição, você pode usar o campo de filtragem **Mostrar certificados que são...** ou pode classificar as linhas de certificado clicando em um dos cabeçalhos de coluna.

4. Na caixa de diálogo, selecione o certificado e clique em **Importar**.

O certificado é carregado e validado.

Excluir certificados confiáveis

Você pode excluir um ou mais certificados que não são mais necessários, como um certificado expirado.

Antes de começar

Importe o novo certificado antes de excluir o antigo.



Esteja ciente de que a exclusão de um certificado raiz ou intermediário pode afetar vários storages, já que esses storages podem compartilhar os mesmos arquivos de certificado.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione a guia **Trusted**.
3. Selecione um ou mais certificados na tabela e clique em **Excluir**.



A função **Delete** não está disponível para certificados pré-instalados.

A caixa de diálogo confirmar Excluir certificado confiável é aberta.

4. Confirme a exclusão e clique em **Excluir**.

O certificado é removido da tabela.

Resolver certificados não confiáveis

Certificados não confiáveis ocorrem quando um storage array tenta estabelecer uma conexão segura com o Unified Manager, mas a conexão não consegue confirmar como segura.

Na página certificado, você pode resolver certificados não confiáveis importando um certificado autoassinado da matriz de armazenamento ou importando um certificado de autoridade de certificação (CA) emitido por um terceiro confiável.

Antes de começar

- Você deve estar conectado com um perfil de usuário que inclua permissões de Administrador de Segurança.
- Se você pretende importar um certificado assinado pela CA:
 - Você gerou uma solicitação de assinatura de certificado (arquivo .CSR) para cada controlador na matriz de armazenamento e a enviou para a CA.
 - A CA retornou arquivos de certificado confiáveis.
 - Os ficheiros de certificado estão disponíveis no sistema local.

Sobre esta tarefa

Talvez seja necessário instalar certificados de CA confiáveis adicionais se alguma das seguintes opções for verdadeira:

- Recentemente, você adicionou uma matriz de armazenamento.
- Um ou ambos os certificados expiram.
- Um ou ambos os certificados são revogados.
- Um ou ambos os certificados estão faltando um certificado raiz ou intermediário.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione a guia **Trusted**.

Esta página mostra todos os certificados reportados para os storages de armazenamento.

3. Selecione um **Importar > certificados** para importar um certificado de CA ou **Importar > certificados de matriz de armazenamento autoassinados** para importar um certificado autoassinado.

Para limitar a exibição, você pode usar o campo de filtragem **Mostrar certificados que são...** ou pode classificar as linhas de certificado clicando em um dos cabeçalhos de coluna.

4. Na caixa de diálogo, selecione o certificado e clique em **Importar**.

O certificado é carregado e validado.

Gerenciar certificados

Ver certificados

Você pode ver informações resumidas de um certificado, que inclui a organização usando o certificado, a autoridade que emitiu o certificado, o período de validade e as impressões digitais (identificadores exclusivos).

Antes de começar

Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções do certificado não aparecem.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione um dos seguintes separadores:
 - **Gerenciamento** — mostra o certificado para o sistema que hospeda o Proxy de Serviços Web. Um certificado de gerenciamento pode ser autoassinado ou aprovado por uma autoridade de certificação (CA). Ele permite acesso seguro ao Unified Manager.
 - **Trusted** — mostra os certificados que o Unified Manager pode acessar para matrizes de armazenamento e outros servidores remotos, como um servidor LDAP. Os certificados podem ser emitidos a partir de uma autoridade de certificação (CA) ou podem ser autoassinados.
3. Para ver mais informações sobre um certificado, selecione sua linha, selecione as elipses no final da linha e clique em **Exibir** ou **Exportar**.

Exportar certificados

Você pode exportar um certificado para exibir seus detalhes completos.

Antes de começar

Para abrir o ficheiro exportado, tem de ter uma aplicação de visualizador de certificados.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione um dos seguintes separadores:
 - **Gerenciamento** — mostra o certificado para o sistema que hospeda o Proxy de Serviços Web. Um certificado de gerenciamento pode ser autoassinado ou aprovado por uma autoridade de certificação (CA). Ele permite acesso seguro ao Unified Manager.
 - **Trusted** — mostra os certificados que o Unified Manager pode acessar para matrizes de armazenamento e outros servidores remotos, como um servidor LDAP. Os certificados podem ser emitidos a partir de uma autoridade de certificação (CA) ou podem ser autoassinados.
3. Selecione um certificado na página e, em seguida, clique nas elipses no final da linha.
4. Clique em **Exportar** e salve o arquivo de certificado.
5. Abra o arquivo no aplicativo visualizador de certificados.

Gerenciamento de acesso

Visão geral do Gerenciamento de Acesso

O Access Management é um método de configuração da autenticação de usuário no Unified Manager.

Quais métodos de autenticação estão disponíveis?

Estão disponíveis os seguintes métodos de autenticação:

- **Funções de usuário local** — a autenticação é gerenciada por meio de recursos RBAC (controle de acesso baseado em função). As funções de usuário local incluem perfis de usuário predefinidos e funções com permissões de acesso específicas.
- **Serviços de diretório** — a autenticação é gerenciada por meio de um servidor LDAP (Lightweight Directory Access Protocol) e serviço de diretório, como o Active Directory da Microsoft.
- **SAML** — a autenticação é gerenciada por meio de um Provedor de identidade (IDP) usando SAML 2,0.

Saiba mais:

- ["Como o Gerenciamento de Acesso funciona"](#)
- ["Terminologia de Gerenciamento de Acesso"](#)
- ["Permissões para funções mapeadas"](#)
- ["SAML"](#)

Como faço para configurar o Gerenciamento de Acesso?

O software SANtricity está pré-configurado para utilizar funções de utilizador locais. Se pretender utilizar o LDAP, pode configurá-lo na página Gestão de acessos.

Saiba mais:

- ["Gerenciamento de acesso com funções de usuário local"](#)
- ["Gerenciamento de acesso com serviços de diretório"](#)
- ["Configurar SAML"](#)

Conceitos

Como o Gerenciamento de Acesso funciona

Use o Gerenciamento de acesso para estabelecer a autenticação de usuário no Unified Manager.

Fluxo de trabalho de configuração

A configuração do Access Management funciona da seguinte forma:

1. Um administrador faz login no Unified Manager com um perfil de usuário que inclui permissões de administrador de segurança.



Para iniciar sessão pela primeira vez, o nome de utilizador `admin` é apresentado automaticamente e não pode ser alterado. O `admin` utilizador tem acesso total a todas as funções do sistema. A palavra-passe tem de ser definida no início de sessão pela primeira vez.

2. O administrador navega para acessar o Gerenciamento na interface do usuário, que inclui funções de usuário locais pré-configuradas. Essas funções são uma implementação dos recursos RBAC (controle de acesso baseado em função).
3. O administrador configura um ou mais dos seguintes métodos de autenticação:
 - *** Funções de usuário local*** — a autenticação é gerenciada por meio de recursos RBAC. As funções de usuário local incluem usuários predefinidos e funções com permissões de acesso específicas. Os administradores podem usar essas funções de usuário local como o único método de autenticação ou usá-las em combinação com um serviço de diretório. Nenhuma configuração é necessária, além de definir senhas para usuários.
 - **Serviços de diretório** — a autenticação é gerenciada por meio de um servidor LDAP (Lightweight Directory Access Protocol) e serviço de diretório, como o ativo Directory da Microsoft. Um administrador se conecta ao servidor LDAP e, em seguida, mapeia os usuários LDAP para as funções de usuário local.
 - **SAML** — a autenticação é gerenciada por meio de um Provedor de identidade (IDP) usando a Security Assertion Markup Language (SAML) 2,0. Um administrador estabelece a comunicação entre o sistema IDP e o storage array e, em seguida, mapeia os usuários IDP para as funções de usuário local incorporadas no storage array.
4. O administrador fornece aos usuários credenciais de login para o Unified Manager.
5. Os usuários fazem login no sistema inserindo suas credenciais. Durante o início de sessão, o sistema executa as seguintes tarefas em segundo plano:

- Autentica o nome de utilizador e a palavra-passe na conta de utilizador.
- Determina as permissões do usuário com base nas funções atribuídas.
- Fornece ao usuário acesso a funções na interface do usuário.
- Exibe o nome do usuário no banner superior.

Funções disponíveis no Unified Manager

O acesso a funções depende das funções atribuídas de um usuário, que incluem o seguinte:

- **Storage admin** — Acesso completo de leitura/gravação a objetos de armazenamento nas matrizes, mas sem acesso à configuração de segurança.
- **Security admin** — Acesso à configuração de segurança em Gerenciamento de Acesso e Gerenciamento de certificados.
- **Support admin** — Acesso a todos os recursos de hardware em matrizes de armazenamento, dados de falha e eventos mel. Sem acesso a objetos de armazenamento ou à configuração de segurança.
- **Monitor** — Acesso somente leitura a todos os objetos de armazenamento, mas sem acesso à configuração de segurança.

Uma função indisponível está a cinzento ou não é apresentada na interface do utilizador.

Terminologia de Gerenciamento de Acesso

Saiba como os termos do Gerenciamento de Acesso se aplicam ao Unified Manager.

Prazo	Descrição
Active Directory	O Active Directory (AD) é um serviço de diretório da Microsoft que usa LDAP para redes de domínio do Windows.
Encadernação	As operações de vinculação são usadas para autenticar clientes no servidor de diretórios. A vinculação geralmente requer credenciais de conta e senha, mas alguns servidores permitem operações anônimas de vinculação.
CA	Uma autoridade de certificação (CA) é uma entidade confiável que emite documentos eletrônicos, chamados certificados digitais, para segurança na Internet. Esses certificados identificam proprietários de sites, o que permite conexões seguras entre clientes e servidores.
Certificado	Um certificado identifica o proprietário de um site para fins de segurança, o que impede que atacantes personifiquem o site. O certificado contém informações sobre o proprietário do site e a identidade da entidade confiável que certifica (assina) essas informações.
LDAP	O LDAP (Lightweight Directory Access Protocol) é um protocolo de aplicação para aceder e manter serviços de informação de diretório distribuído. Este protocolo permite que vários aplicativos e serviços diferentes se conectem ao servidor LDAP para validar usuários.

Prazo	Descrição
RBAC	O controle de acesso baseado em função (RBAC) é um método de regular o acesso a recursos de computador ou rede com base nas funções de usuários individuais. O Unified Manager inclui funções predefinidas.
SAML	Security Assertion Markup Language (SAML) é um padrão baseado em XML para autenticação e autorização entre duas entidades. O SAML permite a autenticação multifator, na qual os usuários devem fornecer dois ou mais itens para provar sua identidade (por exemplo, uma senha e uma impressão digital). O recurso SAML incorporado do storage array é compatível com SAML2,0 para afirmação, autenticação e autorização de identidade.
SSO	Logon único (SSO) é um serviço de autenticação que permite que um conjunto de credenciais de login acesse vários aplicativos.
Proxy de serviços Web	O Web Services Proxy, que fornece acesso através de mecanismos HTTPS padrão, permite que os administradores configurem serviços de gerenciamento para matrizes de armazenamento. O proxy pode ser instalado em hosts Windows ou Linux. A interface do Unified Manager está disponível com o Web Services Proxy.

Permissões para funções mapeadas

Os recursos RBAC (controle de acesso baseado em função) incluem usuários predefinidos com uma ou mais funções mapeadas para eles. Cada função inclui permissões para acessar tarefas no Unified Manager.

As funções fornecem acesso do usuário a tarefas, como segue:

- **Storage admin** — Acesso completo de leitura/gravação a objetos de armazenamento nas matrizes, mas sem acesso à configuração de segurança.
- **Security admin** — Acesso à configuração de segurança em Gerenciamento de Acesso e Gerenciamento de certificados.
- **Support admin** — Acesso a todos os recursos de hardware em matrizes de armazenamento, dados de falha e eventos mel. Sem acesso a objetos de armazenamento ou à configuração de segurança.
- **Monitor** — Acesso somente leitura a todos os objetos de armazenamento, mas sem acesso à configuração de segurança.

Se um usuário não tiver permissões para uma determinada função, essa função não estará disponível para seleção ou não será exibida na interface do usuário.

Gerenciamento de acesso com funções de usuário local

Os administradores podem usar os recursos RBAC (controle de acesso baseado em função) aplicados no Unified Manager. Esses recursos são chamados de "funções de usuário local".

Fluxo de trabalho de configuração

As funções de utilizador local são pré-configuradas no sistema. Para usar funções de usuário local para autenticação, os administradores podem fazer o seguinte:

1. Um administrador faz login no Unified Manager com um perfil de usuário que inclui permissões de administrador de segurança.



O `admin` utilizador tem acesso total a todas as funções do sistema.

2. Um administrador analisa os perfis de usuário, que são predefinidos e não podem ser modificados.
3. Opcionalmente, o administrador atribui novas senhas para cada perfil de usuário.
4. Os usuários fazem login no sistema com suas credenciais atribuídas.

Gerenciamento

Ao usar apenas funções de usuário local para autenticação, os administradores podem executar as seguintes tarefas de gerenciamento:

- Alterar senhas.
- Defina um comprimento mínimo para senhas.
- Permitir que os usuários façam login sem senhas.

Gerenciamento de acesso com serviços de diretório

Os administradores podem usar um servidor LDAP (Lightweight Directory Access Protocol) e um serviço de diretório, como o Active Directory da Microsoft.

Fluxo de trabalho de configuração

Se um servidor LDAP e um serviço de diretório são usados na rede, a configuração funciona da seguinte forma:

1. Um administrador faz login no Unified Manager com um perfil de usuário que inclui permissões de administrador de segurança.



O `admin` utilizador tem acesso total a todas as funções do sistema.

2. O administrador insere as configurações do servidor LDAP. As configurações incluem o nome do domínio, URL e informações da conta Bind.
3. Se o servidor LDAP usar um protocolo seguro (LDAPS), o administrador carrega uma cadeia de certificados de autoridade de certificação (CA) para autenticação entre o servidor LDAP e o sistema host onde o proxy de serviços da Web está instalado.
4. Depois de estabelecer a ligação ao servidor, o administrador mapeia os grupos de utilizadores para as funções de utilizador locais. Essas funções são predefinidas e não podem ser modificadas.
5. O administrador testa a conexão entre o servidor LDAP e o Proxy de serviços da Web.
6. Os usuários fazem login no sistema com suas credenciais LDAP/Directory Services atribuídas.

Gerenciamento

Ao usar serviços de diretório para autenticação, os administradores podem executar as seguintes tarefas de gerenciamento:

- Adicione um servidor de diretório.
- Editar definições do servidor de diretório.
- Mapeie usuários LDAP para funções de usuário locais.
- Remova um servidor de diretório.
- Alterar senhas.
- Defina um comprimento mínimo para senhas.
- Permitir que os usuários façam login sem senhas.

Gerenciamento de acesso com SAML

Para Gerenciamento de Acesso, os administradores podem usar os recursos de Security Assertion Markup Language (SAML) 2,0 incorporados no array.

Fluxo de trabalho de configuração

A configuração SAML funciona da seguinte forma:

1. Um administrador faz login no Unified Manager com um perfil de usuário que inclui permissões de administrador de segurança.



O `admin` utilizador tem acesso total a todas as funções do System Manager.

2. O administrador vai para a guia **SAML** em Gerenciamento de Acesso.
3. Um administrador configura as comunicações com o Provedor de identidade (IDP). Um IDP é um sistema externo usado para solicitar credenciais de um usuário e determinar se o usuário foi autenticado com êxito. Para configurar as comunicações com o storage array, o administrador baixa o arquivo de metadados IDP do sistema IDP e, em seguida, usa o Unified Manager para carregar o arquivo para o storage array.
4. Um administrador estabelece uma relação de confiança entre o Fornecedor de Serviços e o IDP. Um Fornecedor de Serviços controla a autorização do utilizador; neste caso, o controlador na matriz de armazenamento atua como o Fornecedor de Serviços. Para configurar as comunicações, o administrador usa o Unified Manager para exportar um arquivo de metadados do provedor de serviços para o controlador. A partir do sistema IDP, o administrador então importa o arquivo de metadados para o IDP.



Os administradores também devem certificar-se de que o IDP suporta a capacidade de retornar um ID de nome na autenticação.

5. O administrador mapeia as funções do storage array para atributos de usuário definidos no IDP. Para fazer isso, o administrador usa o Unified Manager para criar os mapeamentos.
6. O administrador testa o login SSO para o URL do IDP. Este teste garante que a matriz de armazenamento e o IDP possam se comunicar.



Uma vez que o SAML está ativado, você *não pode* desabilitá-lo através da interface do usuário, nem pode editar as configurações de IDP. Se você precisar desativar ou editar a configuração SAML, entre em Contato com o suporte técnico para obter assistência.

7. No Unified Manager, o administrador habilita o SAML para o storage array.
8. Os usuários fazem login no sistema com suas credenciais SSO.

Gerenciamento

Ao usar o SAML para autenticação, os administradores podem executar as seguintes tarefas de gerenciamento:

- Modificar ou criar novos mapeamentos de função
- Exportar ficheiros do fornecedor de serviços

Restrições de acesso

Quando o SAML está ativado, os usuários não podem descobrir ou gerenciar o armazenamento desse array a partir da interface herdada do Storage Manager.

Além disso, os seguintes clientes não podem acessar os serviços e recursos do storage array:

- Janela de gerenciamento empresarial (EMW)
- Interface de linha de comando (CLI)
- Clientes de Software Developer Kits (SDK)
- Clientes na banda
- Clientes API REST de Autenticação básica HTTP
- Faça login usando o endpoint padrão da API REST

Use funções de usuário local

Ver funções de utilizador locais

Na guia funções do usuário local, você pode exibir os mapeamentos dos usuários para as funções padrão. Esses mapeamentos fazem parte do RBAC (controles de acesso baseados em função) aplicado no Proxy de serviços da Web para Unified Manager.

Antes de começar

Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.

Sobre esta tarefa

Os usuários e mapeamentos não podem ser alterados. Apenas as senhas podem ser modificadas.

Passos

1. Selecione **Gerenciamento de Acesso**.
2. Selecione a guia **funções de usuário local**.

Os usuários são mostrados na tabela:

- **Admin** — Super administrador que tem acesso a todas as funções do sistema. Este usuário inclui todas as funções.
- **Storage** — o administrador responsável por todo o provisionamento de armazenamento. Esse usuário inclui as seguintes funções: Administrador de storage, administrador de suporte e monitor.
- **Segurança** — o usuário responsável pela configuração de segurança, incluindo Gerenciamento de Acesso e Gerenciamento de certificados. Este usuário inclui as seguintes funções: Admin de segurança e Monitor.
- **Suporte** — o usuário responsável por recursos de hardware, dados de falha e atualizações de firmware. Este usuário inclui as seguintes funções: Admin de suporte e Monitor.
- **Monitor** — Um usuário com acesso somente leitura ao sistema. Este utilizador inclui apenas a função Monitor.
- **rw** (leitura/gravação) — este usuário inclui as seguintes funções: Administrador de armazenamento, administrador de suporte e monitor.
- **Ro** (somente leitura) — este usuário inclui somente a função Monitor.

Alterar senhas para perfis de usuário locais

Você pode alterar as senhas de usuário para cada usuário no Gerenciamento de acesso.

Antes de começar

- Você deve estar logado como administrador local, o que inclui permissões de administrador raiz.
- Você deve saber a senha do administrador local.

Sobre esta tarefa

Tenha em mente estas diretrizes ao escolher uma senha:

- Quaisquer novas senhas de usuário local devem atender ou exceder a configuração atual para uma senha mínima (em Configurações de visualização/edição).
- As senhas diferenciam maiúsculas de minúsculas.
- Os espaços de saída não são removidos das senhas quando são definidos. Tenha cuidado para incluir espaços se eles foram incluídos na senha.
- Para maior segurança, use pelo menos 15 caracteres alfanuméricos e altere a senha com frequência.

Passos

1. Selecione **Gerenciamento de Acesso**.
2. Selecione a guia **funções de usuário local**.
3. Selecione um usuário na tabela.

O botão alterar senha fica disponível.

4. Selecione **alterar palavra-passe**.

A caixa de diálogo alterar senha será exibida.

5. Se não estiver definido um comprimento mínimo de palavra-passe para palavras-passe de utilizador local, pode selecionar a caixa de verificação para exigir que o utilizador introduza uma palavra-passe para aceder ao sistema.
6. Introduza a nova palavra-passe para o utilizador selecionado nos dois campos.

7. Introduza a palavra-passe do administrador local para confirmar esta operação e, em seguida, clique em **alterar**.

Resultados

Se o usuário estiver conectado no momento, a alteração da senha fará com que a sessão ativa do usuário seja encerrada.

Altere as definições de palavra-passe do utilizador local

Pode definir o comprimento mínimo necessário para todas as palavras-passe de utilizador locais novas ou atualizadas. Também pode permitir que os utilizadores locais acessem ao sistema sem introduzir uma palavra-passe.

Antes de começar

Você deve estar logado como administrador local, o que inclui permissões de administrador raiz.

Sobre esta tarefa

Tenha estas diretrizes em mente ao definir o comprimento mínimo para senhas de usuário local:

- A definição de alterações não afeta as palavras-passe de utilizador locais existentes.
- A definição de comprimento mínimo necessário para palavras-passe de utilizador local tem de ter entre 0 e 30 caracteres.
- Quaisquer novas senhas de usuário local devem atender ou exceder a configuração de comprimento mínimo atual.
- Não defina um comprimento mínimo para a palavra-passe se pretender que os utilizadores locais acessem ao sistema sem introduzir uma palavra-passe.

Passos

1. Selecione **Gerenciamento de Acesso**.
2. Selecione a guia **funções de usuário local**.
3. Selecione **Exibir/Editar configurações**.

A caixa de diálogo Configurações de senha do usuário local é aberta.

4. Execute um dos seguintes procedimentos:
 - Para permitir que os usuários locais acessem o sistema *sem* inserir uma senha, desmarque a caixa de seleção "exigir que todas as senhas de usuário local sejam pelo menos".
 - Para definir um comprimento mínimo de palavra-passe para todas as palavras-passe de utilizador local, selecione a caixa de verificação "exigir que todas as palavras-passe de utilizador local sejam pelo menos" e, em seguida, utilize a caixa de seleção para definir o comprimento mínimo necessário para todas as palavras-passe de utilizador local.

Todas as novas senhas de usuário local devem atender ou exceder a configuração atual.

5. Clique em **Salvar**.

Use os serviços de diretório

Adicionar servidor de diretório

Para configurar a autenticação para o Gerenciamento de Acesso, você estabelece comunicações entre um servidor LDAP e o host que executa o Proxy de Serviços Web para Unified Manager. Em seguida, mapeia os grupos de utilizadores LDAP para as funções de utilizador local.

Antes de começar

- Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- Os grupos de usuários devem ser definidos em seu serviço de diretório.
- As credenciais do servidor LDAP devem estar disponíveis, incluindo o nome de domínio, o URL do servidor e, opcionalmente, o nome de usuário e a senha da conta BIND.
- Para servidores LDAPS que usam um protocolo seguro, a cadeia de certificados do servidor LDAP deve ser instalada na sua máquina local.

Sobre esta tarefa

Adicionar um servidor de diretório é um processo de duas etapas. Primeiro você insere o nome de domínio e URL. Se o servidor usar um protocolo seguro, você também deve carregar um certificado de CA para autenticação se ele for assinado por uma autoridade de assinatura não padrão. Se tiver credenciais para uma conta BIND, também poderá introduzir o nome da conta de utilizador e a palavra-passe. Em seguida, você mapeia os grupos de usuários do servidor LDAP para funções de usuário locais.


Passos

1. Selecione **Gerenciamento de Acesso**.
2. Na guia **Serviços de diretório**, selecione **Adicionar servidor de diretório**.

A caixa de diálogo Adicionar servidor de diretório é aberta.

3. Na guia **Configurações do servidor**, insira as credenciais do servidor LDAP.

Detalhes do campo

Definição	Descrição
Configurações de configuração	Domínio(s)
Introduza o nome de domínio do servidor LDAP. Para vários domínios, insira os domínios em uma lista separada por vírgulas. O nome de domínio é usado no login (<i>username__domain</i>) para especificar em qual servidor de diretório se autenticar.	URL do servidor
Insira o URL para acessar o servidor LDAP na forma <code>ldap[s]://host:*port*de</code> .	Carregar certificado (opcional)
 <p>Este campo aparece apenas se um protocolo LDAPS for especificado no campo URL do servidor acima.</p> <p>Clique em Procurar e selecione um certificado de CA para carregar. Este é o certificado confiável ou cadeia de certificados usada para autenticar o servidor LDAP.</p>	Vincular conta (opcional)

Definição	Descrição
<p>Insira uma conta de usuário somente leitura para consultas de pesquisa no servidor LDAP e para pesquisar nos grupos. Introduza o nome da conta num formato de tipo LDAP. Por exemplo, se o usuário bind for chamado de "bindacct", você poderá inserir um valor como CN=bindacct,CN=Users,DC=cpoc,DC=local.</p>	<p>Vincular senha (opcional)</p>
<div data-bbox="245 898 302 951" data-label="Image"> </div> <p data-bbox="358 772 472 1073">Este campo é exibido quando você insere uma conta BIND.</p> <p data-bbox="212 1125 464 1220">Introduza a palavra-passe para a conta vincular.</p>	<p>Teste a conexão do servidor antes de adicionar</p>

Definição	Descrição
<p>Selecione esta caixa de verificação se pretender certificar-se de que o sistema pode comunicar com a configuração do servidor LDAP introduzida. O teste ocorre depois de clicar em Add na parte inferior da caixa de diálogo.</p> <p>Se esta caixa de verificação estiver selecionada e o teste falhar, a configuração não será adicionada. Você deve resolver o erro ou desmarcar a caixa de seleção para ignorar o teste e adicionar a configuração.</p>	<ul style="list-style-type: none"> • Configurações de privilégio*
Pesquisar DN base	Introduza o contexto LDAP para procurar utilizadores, normalmente na forma <code>CN=Users, DC=cpoc, DC=local de</code> .
Atributo de nome de usuário	Insira o atributo que está vinculado ao ID do usuário para autenticação. Por exemplo <code>sAMAccountName:</code> .
Atributo(s) de grupo	Insira uma lista de atributos de grupo no usuário, que é usada para mapeamento de grupo para função. Por exemplo <code>memberOf, managedObjects:</code> .

4. Clique na guia **Mapeamento de função**.

5. Atribua grupos LDAP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

Detalhes do campo

Definição	Descrição
Mapeamentos	DN do grupo
Especifique o nome distinto do grupo (DN) para o grupo de usuários LDAP a ser mapeado. Expressões regulares são suportadas. Estes caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\) se eles não são parte de um padrão de expressão regular	Funções



A função Monitor é necessária para todos os usuários, incluindo o administrador.

6. Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.
7. Quando terminar com os mapeamentos, clique em **Add**.

O sistema executa uma validação, certificando-se de que a matriz de armazenamento e o servidor LDAP possam se comunicar. Se for apresentada uma mensagem de erro, assinale as credenciais introduzidas na caixa de diálogo e volte a introduzir as informações, se necessário.

Edite as configurações do servidor de diretório e mapeamentos de função

Se você configurou anteriormente um servidor de diretório em Gerenciamento de Acesso, poderá alterar suas configurações a qualquer momento. As configurações incluem as informações de conexão do servidor e os mapeamentos de grupo para função.

Antes de começar

- Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- Um servidor de diretório deve ser definido.

Passos

1. Selecione **Gerenciamento de Acesso**.
2. Selecione a guia **Serviços de diretório**.
3. Se mais de um servidor estiver definido, selecione o servidor que deseja editar na tabela.

4. Selecione **Exibir/Editar configurações**.

A caixa de diálogo Configurações do servidor de diretório é aberta.

5. Na guia **Configurações do servidor**, altere as configurações desejadas.

Detalhes do campo

Definição	Descrição
Configurações de configuração	Domínio(s)
O(s) nome(s) de domínio do(s) servidor(es) LDAP. Para vários domínios, insira os domínios em uma lista separada por vírgulas. O nome de domínio é usado no login (<i>username__domain</i>) para especificar em qual servidor de diretório se autenticar.	URL do servidor
O URL para acessar o servidor LDAP na forma <code>ldap[s]://host:port de</code> .	Vincular conta (opcional)
A conta de usuário somente leitura para consultas de pesquisa no servidor LDAP e para pesquisa dentro dos grupos.	Vincular senha (opcional)
A senha para a conta vincular. (Este campo é exibido quando uma conta BIND é inserida.)	Teste a conexão do servidor antes de salvar

Definição	Descrição
Verifica se o sistema pode comunicar com a configuração do servidor LDAP. O teste ocorre depois de clicar em Salvar . Se esta caixa de verificação estiver selecionada e o teste falhar, a configuração não será alterada. Você deve resolver o erro ou desmarcar a caixa de seleção para ignorar o teste e reeditar a configuração.	<ul style="list-style-type: none"> • Configurações de privilégio*
Pesquisar DN base	O contexto LDAP para procurar usuários, normalmente na forma CN=Users, DC=cpoc, DC=local de .
Atributo de nome de usuário	O atributo que está vinculado ao ID do usuário para autenticação. Por exemplo sAMAccountName: .
Atributo(s) de grupo	Uma lista de atributos de grupo no usuário, que é usada para mapeamento de grupo para função. Por exemplo memberOf, managedObjects: .

6. Na guia **Mapeamento de função**, altere o mapeamento desejado.

Detalhes do campo

Definição	Descrição
Mapeamentos	DN do grupo
O nome de domínio para o grupo de utilizadores LDAP a ser mapeado. Expressões regulares são suportadas. Esses caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular: O que é que é que não é possível	Funções



A função Monitor é necessária para todos os usuários, incluindo o administrador.

- Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.
- Clique em **Salvar**.

Resultados

Depois de concluir esta tarefa, todas as sessões ativas do utilizador são encerradas. Apenas a sessão de utilizador atual é mantida.

Remova o servidor de diretório

Para interromper a conexão entre um servidor de diretório e o Proxy de serviços da Web, você pode remover as informações do servidor da página Gerenciamento de acesso. Talvez você queira executar essa tarefa se tiver configurado um novo servidor e, em seguida, desejar remover o antigo.

Antes de começar

Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.

Sobre esta tarefa

Depois de concluir esta tarefa, todas as sessões ativas do utilizador são encerradas. Apenas a sessão de utilizador atual é mantida.

Passos

1. Selecione **Gerenciamento de Acesso**.
2. Selecione a guia **Serviços de diretório**.
3. Na lista, selecione o servidor de diretório que deseja excluir.
4. Clique em **Remover**.

A caixa de diálogo Remover servidor de diretório é aberta.

5. Digite `remove` o campo e clique em **Remover**.

As configurações do servidor de diretório, as configurações de privilégio e os mapeamentos de função são removidos. Os usuários não podem mais fazer login com credenciais deste servidor.

Use SAML

Configurar SAML

Para configurar a autenticação para o Access Management, você pode usar os recursos de Security Assertion Markup Language (SAML) incorporados no storage array. Esta configuração estabelece uma conexão entre um Provedor de identidade e o Provedor de armazenamento.

Antes de começar

- Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- Você deve saber o endereço IP ou o nome de domínio do controlador na matriz de armazenamento.
- Um administrador de IDP configurou um sistema de IDP.
- Um administrador de IDP garantiu que o IDP suporta a capacidade de retornar um ID de nome na autenticação.
- Um administrador garantiu que o servidor IDP e o relógio do controlador são sincronizados (através de um servidor NTP ou ajustando as definições do relógio do controlador).
- Um arquivo de metadados IDP é baixado do sistema IDP e está disponível no sistema local usado para acessar o Unified Manager.

Sobre esta tarefa

Um Provedor de identidade (IDP) é um sistema externo usado para solicitar credenciais de um usuário e para determinar se esse usuário foi autenticado com êxito. O IDP pode ser configurado para fornecer autenticação multifator e usar qualquer banco de dados de usuários, como o ativo Directory. Sua equipe de segurança é responsável por manter o IDP. Um provedor de serviços (SP) é um sistema que controla a autenticação e o acesso do usuário. Quando o Gerenciamento de Acesso é configurado com SAML, o storage array atua como o provedor de serviços para solicitar autenticação do provedor de identidade. Para estabelecer uma conexão entre o IDP e o storage array, você compartilha arquivos de metadados entre essas duas entidades. Em seguida, você mapeia as entidades de usuário IDP para as funções de storage array. E, finalmente, você testa os logins de conexão e SSO antes de ativar o SAML.



SAML e Serviços de diretório. Se você ativar o SAML quando os Serviços de diretório estiverem configurados como o método de autenticação, o SAML substituirá os Serviços de diretório no Unified Manager. Se você desabilitar o SAML mais tarde, a configuração dos Serviços de diretório retornará à configuração anterior.



Edição e desativação. Uma vez que o SAML está ativado, você *não pode* desabilitá-lo através da interface do usuário, nem pode editar as configurações de IDP. Se você precisar desativar ou editar a configuração SAML, entre em Contato com o suporte técnico para obter assistência.

Configurar a autenticação SAML é um procedimento de várias etapas.

Passo 1: Faça o upload do arquivo de metadados IDP

Para fornecer ao storage array informações de conexão IDP, você importa metadados IDP para o Unified Manager. O sistema de IDP precisa desses metadados para redirecionar as solicitações de autenticação para o URL correto e para validar as respostas recebidas.

Passos

1. Selecione **Definições > Gestão de Acesso**.
2. Selecione a guia **SAML**.

A página exibe uma visão geral das etapas de configuração.

3. Clique no link **Import Identity Provider (IDP) file**.

A caixa de diálogo Importar arquivo do provedor de identidade será aberta.

4. Clique em **Procurar** para selecionar e carregar o ficheiro de metadados IDP copiado para o sistema local.

Depois de selecionar o ficheiro, é apresentado o ID da entidade IDP.

5. Clique em **Importar**.

Passo 2: Exportar arquivos do provedor de serviços

Para estabelecer uma relação de confiança entre o IDP e o storage array, você importa os metadados do provedor de serviços para o IDP. O IDP precisa desses metadados para estabelecer uma relação de confiança com o controlador e processar solicitações de autorização. O arquivo inclui informações como o nome de domínio do controlador ou endereço IP, para que o IDP possa se comunicar com os provedores de serviços.

Passos

1. Clique no link **Exportar arquivos do provedor de serviços**.

A caixa de diálogo Exportar ficheiros do fornecedor de serviços abre-se.

2. Introduza o endereço IP do controlador ou o nome DNS no campo **Controller A** e, em seguida, clique em **Export** para guardar o ficheiro de metadados no sistema local.

Depois de clicar em **Exportar**, os metadados do fornecedor de serviços são transferidos para o seu sistema local. Anote onde o arquivo é armazenado.

3. No sistema local, localize o arquivo de metadados do provedor de serviços formatado em XML que você exportou.
4. A partir do servidor IDP, importe o arquivo de metadados do provedor de serviços para estabelecer a relação de confiança. Você pode importar o arquivo diretamente ou inserir manualmente as informações do controlador a partir do arquivo.

Passo 3: Mapear funções

Para fornecer aos usuários autorização e acesso ao Unified Manager, é necessário mapear os atributos de usuário e associações a grupos de IDP para as funções predefinidas do storage array.

Antes de começar

- Um administrador de IDP configurou atributos de usuário e associação de grupo no sistema de IDP.
- O arquivo de metadados de IDP é importado para o Unified Manager.
- Um arquivo de metadados do provedor de serviços para o controlador é importado para o sistema IDP para a relação de confiança.

Passos

1. Clique no link para **Mapping Unified Manager Roles**.

A caixa de diálogo Mapeamento de função é aberta.

2. Atribua atributos de usuário e grupos IDP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

Detalhes do campo

Definição	Descrição
Mapeamentos	Atributo do utilizador
Especifique o atributo (por exemplo, "membro de") para o grupo SAML a ser mapeado.	Valor do atributo
Especifique o valor do atributo para o grupo a ser mapeado. Expressões regulares são suportadas. Esses caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\) se eles não forem parte de um padrão de expressão regular	Funções



A função Monitor é necessária para todos os usuários, incluindo o administrador. O Unified Manager não funcionará corretamente para nenhum usuário sem a função Monitor presente.

3. Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.



Mapeamentos de função podem ser modificados depois que o SAML estiver habilitado.

4. Quando terminar com os mapeamentos, clique em **Salvar**.

Passo 4: Teste o login SSO

Para garantir que o sistema IDP e o storage array possam se comunicar, você pode testar opcionalmente um login SSO. Este teste também é realizado durante a etapa final para ativar o SAML.

Antes de começar

- O arquivo de metadados de IDP é importado para o Unified Manager.
- Um arquivo de metadados do provedor de serviços para o controlador é importado para o sistema IDP para a relação de confiança.

Passos

1. Selecione o link **Test SSO Login**.

Abre-se uma caixa de diálogo para introduzir credenciais SSO.

2. Insira credenciais de login para um usuário com permissões de Administrador de Segurança e permissões de Monitor.

Abre-se uma caixa de diálogo enquanto o sistema testa o início de sessão.

3. Procure uma mensagem Teste bem-sucedida. Se o teste for concluído com êxito, vá para a próxima etapa para ativar o SAML.

Se o teste não for concluído com êxito, é apresentada uma mensagem de erro com mais informações. Certifique-se de que:

- O usuário pertence a um grupo com permissões para Administrador de Segurança e Monitor.
- Os metadados carregados para o servidor IDP estão corretos.
- O endereço do controlador nos arquivos de metadados do SP está correto.

Passo 5: Ative o SAML

Sua etapa final é concluir a configuração SAML para autenticação de usuário. Durante esse processo, o sistema também solicita que você teste um login SSO. O processo de teste SSO Login é descrito na etapa anterior.

Antes de começar

- O arquivo de metadados de IDP é importado para o Unified Manager.
- Um arquivo de metadados do provedor de serviços para o controlador é importado para o sistema IDP para a relação de confiança.
- Pelo menos um mapeamento de função Monitor e um Admin de segurança está configurado.



Edição e desativação. Uma vez que o SAML está ativado, você *não pode* desabilitá-lo através da interface do usuário, nem pode editar as configurações de IDP. Se você precisar desativar ou editar a configuração SAML, entre em Contato com o suporte técnico para obter assistência.

Passos

1. Na guia **SAML**, selecione o link **Ativar SAML**.

A caixa de diálogo confirmar ativação SAML é aberta.

2. Digite `enable` e clique em **Ativar**.
3. Insira as credenciais do usuário para um teste de login SSO.

Resultados

Depois que o sistema ativa o SAML, ele termina todas as sessões ativas e começa a autenticar usuários por meio do SAML.

Alterar mapeamentos de função SAML

Se você configurou o SAML para Gerenciamento de Acesso anteriormente, poderá alterar os mapeamentos de função entre os grupos de IDP e as funções predefinidas do storage array.

Antes de começar

- Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- Um administrador de IDP configurou atributos de usuário e associação de grupo no sistema de IDP.
- O SAML está configurado e ativado.

Passos

1. Selecione **Definições > Gestão de Acesso**.
2. Selecione a guia **SAML**.
3. Selecione **Mapeamento de função**.

A caixa de diálogo Mapeamento de função é aberta.

4. Atribua atributos de usuário e grupos IDP às funções predefinidas. Um grupo pode ter várias funções atribuídas.



Tenha cuidado para não remover suas permissões enquanto o SAML estiver ativado ou você perderá o acesso ao Unified Manager.

Detalhes do campo

Definição	Descrição
Mapeamentos	Atributo do utilizador
Especifique o atributo (por exemplo, "membro de") para o grupo SAML a ser mapeado.	Valor do atributo
Especifique o valor do atributo para o grupo a ser mapeado.	Funções



A função Monitor é necessária para todos os usuários, incluindo o administrador. O Unified Manager não funcionará corretamente para nenhum usuário sem a função Monitor presente.

5. Opcionalmente, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.
6. Clique em **Salvar**.

Resultados

Depois de concluir esta tarefa, todas as sessões ativas do utilizador são encerradas. Apenas a sessão de utilizador atual é mantida.

Exporte arquivos do provedor de serviços SAML

Se necessário, você pode exportar metadados do provedor de serviços para o storage array e reimportar o arquivo para o sistema de provedor de identidade (IDP).

Antes de começar

- Você deve estar conectado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- O SAML está configurado e ativado.

Sobre esta tarefa

Nesta tarefa, você exporta metadados do controlador. O IDP precisa desses metadados para estabelecer uma relação de confiança com o controlador e processar solicitações de autenticação. O arquivo inclui informações como o nome de domínio do controlador ou endereço IP que o IDP pode usar para enviar solicitações.

Passos

1. Selecione **Definições > Gestão de Acesso**.
2. Selecione a guia **SAML**.
3. Selecione **Exportar**.

A caixa de diálogo Exportar ficheiros do fornecedor de serviços abre-se.

4. Clique em **Exportar** para salvar o arquivo de metadados no sistema local.



O campo de nome de domínio é somente leitura.

Anote onde o arquivo é armazenado.

5. No sistema local, localize o arquivo de metadados do provedor de serviços formatado em XML que você exportou.
6. No servidor IDP, importe o arquivo de metadados do provedor de serviços. Você pode importar o arquivo diretamente ou inserir manualmente as informações do controlador.
7. Clique em **Fechar**.

FAQs

Por que não consigo fazer login?

Se receber um erro ao tentar iniciar sessão, reveja estas possíveis causas.

Erros de login podem ocorrer por um destes motivos:

- Introduziu um nome de utilizador ou uma palavra-passe incorretos.
- Você não tem Privileges suficiente.
- Tentou iniciar sessão sem sucesso várias vezes, o que acionou o modo de bloqueio. Aguarde 10 minutos para voltar a iniciar sessão.
- A autenticação SAML está ativada. Atualize seu navegador para fazer login.

O que eu preciso saber antes de adicionar um servidor de diretório?

Antes de adicionar um servidor de diretório no Gerenciamento de Acesso, você deve atender a certos requisitos.

- Os grupos de usuários devem ser definidos em seu serviço de diretório.
- As credenciais do servidor LDAP devem estar disponíveis, incluindo o nome de domínio, o URL do servidor e, opcionalmente, o nome de usuário e a senha da conta BIND.
- Para servidores LDAPS que usam um protocolo seguro, a cadeia de certificados do servidor LDAP deve ser instalada na sua máquina local.

O que eu preciso saber sobre mapeamento para funções de storage array?

Antes de mapear grupos para funções, revise as diretrizes.

Os recursos RBAC (controle de acesso baseado em função) incluem as seguintes funções:

- **Storage admin** — Acesso completo de leitura/gravação a objetos de armazenamento nas matrizes, mas sem acesso à configuração de segurança.
- **Security admin** — Acesso à configuração de segurança em Gerenciamento de Acesso e Gerenciamento de certificados.
- **Support admin** — Acesso a todos os recursos de hardware em matrizes de armazenamento, dados de falha e eventos mel. Sem acesso a objetos de armazenamento ou à configuração de segurança.

- **Monitor** — Acesso somente leitura a todos os objetos de armazenamento, mas sem acesso à configuração de segurança.



A função Monitor é necessária para todos os usuários, incluindo o administrador.

Se estiver a utilizar um servidor LDAP (Lightweight Directory Access Protocol) e Serviços de diretório, certifique-se de que:

- Um administrador definiu grupos de usuários no serviço de diretório.
- Você conhece os nomes de domínio de grupo para os grupos de usuários LDAP.

SAML

Se você estiver usando os recursos de Security Assertion Markup Language (SAML) incorporados ao storage array, verifique se:

- Um administrador do Provedor de identidade (IDP) configurou atributos de usuário e associação de grupo no sistema IDP.
- Você conhece os nomes dos membros do grupo.
- Você sabe o valor do atributo para o grupo a ser mapeado. Expressões regulares são suportadas. Esses caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular:

```
\. [ ] { } ( ) < > * + - = ! ? ^ $ |
```

- A função Monitor é necessária para todos os usuários, incluindo o administrador. O Unified Manager não funcionará corretamente para nenhum usuário sem a função Monitor presente.

O que eu preciso saber antes de configurar e ativar o SAML?

Antes de configurar e habilitar os recursos de Security Assertion Markup Language (SAML) para autenticação, certifique-se de atender aos requisitos a seguir e entender as restrições SAML.

Requisitos

Antes de começar, certifique-se de que:

- Um Provedor de identidade (IDP) está configurado na sua rede. Um IDP é um sistema externo usado para solicitar credenciais de um usuário e determinar se o usuário foi autenticado com êxito. Sua equipe de segurança é responsável por manter o IDP.
- Um administrador de IDP configurou atributos de usuário e grupos no sistema de IDP.
- Um administrador de IDP garantiu que o IDP suporta a capacidade de retornar um ID de nome na autenticação.
- Um administrador garantiu que o servidor IDP e o relógio do controlador são sincronizados (através de um servidor NTP ou ajustando as definições do relógio do controlador).
- Um arquivo de metadados IDP é baixado do sistema IDP e está disponível no sistema local usado para acessar o Unified Manager.

- Você sabe o endereço IP ou o nome de domínio do controlador na matriz de armazenamento.

Restrições

Além dos requisitos acima, certifique-se de que compreende as seguintes restrições:

- Uma vez que o SAML está ativado, você *não pode* desabilitá-lo através da interface do usuário, nem pode editar as configurações de IDP. Se você precisar desativar ou editar a configuração SAML, entre em Contato com o suporte técnico para obter assistência. Recomendamos que você teste os logins SSO antes de ativar o SAML na etapa final de configuração. (O sistema também executa um teste de login SSO antes de ativar o SAML.)
- Se você desabilitar o SAML no futuro, o sistema restaurará automaticamente a configuração anterior (funções de usuário local e/ou Serviços de diretório).
- Se os Serviços de diretório estiverem configurados atualmente para autenticação de usuário, o SAML substituirá essa configuração.
- Quando o SAML é configurado, os seguintes clientes não podem acessar os recursos do storage array:
 - Janela de gerenciamento empresarial (EMW)
 - Interface de linha de comando (CLI)
 - Clientes de Software Developer Kits (SDK)
 - Clientes na banda
 - Clientes API REST de Autenticação básica HTTP
 - Faça login usando o endpoint padrão da API REST

Quais são os usuários locais?

Os usuários locais são predefinidos no sistema e incluem permissões específicas.

Os usuários locais incluem:

- **Admin** — Super administrador que tem acesso a todas as funções do sistema. Este usuário inclui todas as funções. A palavra-passe tem de ser definida no início de sessão pela primeira vez.
- **Storage** — o administrador responsável por todo o provisionamento de armazenamento. Esse usuário inclui as seguintes funções: Administrador de storage, administrador de suporte e monitor. Esta conta é desativada até que uma palavra-passe seja definida.
- **Segurança** — o usuário responsável pela configuração de segurança, incluindo Gerenciamento de Acesso e Gerenciamento de certificados. Este usuário inclui as seguintes funções: Admin de segurança e Monitor. Esta conta é desativada até que uma palavra-passe seja definida.
- **Suporte** — o usuário responsável por recursos de hardware, dados de falha e atualizações de firmware. Este usuário inclui as seguintes funções: Admin de suporte e Monitor. Esta conta é desativada até que uma palavra-passe seja definida.
- **Monitor** — Um usuário com acesso somente leitura ao sistema. Este utilizador inclui apenas a função Monitor. Esta conta é desativada até que uma palavra-passe seja definida.
- **rw** (leitura/gravação) — este usuário inclui as seguintes funções: Administrador de armazenamento, administrador de suporte e monitor. Esta conta é desativada até que uma palavra-passe seja definida.
- **Ro** (somente leitura) — este usuário inclui somente a função Monitor. Esta conta é desativada até que uma palavra-passe seja definida.

Informações sobre direitos autorais

Copyright © 2024 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 DESTES DOCUMENTOS. 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 SOBRESSALIENTES; 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 DESTES SOFTWARES, 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.