SANtricity Unified Manager

SANtricity software

NetApp
March 17, 2026

Índice

Gerenciamento de múltiplos arrays com SANtricity Unified Manager 7

Interface principal

Saiba mais sobre SANtricity Unified Manager

SANtricity Unified Manager é uma interface Web que permite gerenciar vários arrays de storage em uma única visualização.

Página principal

Ao iniciar sessão no Unified Manager, a página principal abre em **Manage - All**. Nessa página, você pode percorrer uma lista de arrays de storage detectados em sua rede, visualizar o status de cada um e realizar operações em um único array ou em um grupo de arrays.

Barra lateral de navegação

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

Área	Descrição
Gerenciar	Descubra arrays de storage em sua rede, inicie SANtricity System Manager para um array, importe configurações de um array para vários arrays e gerencie grupos de arrays. Selecione as caixas de seleção ao lado dos nomes dos arrays para realizar operações neles, como importar configurações e criar grupos de arrays. As reticências no final de cada linha fornecem um menu in-line 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 array de storage está com status não ideal.
Gerenciamento de certificados	Gerencie certificados para autenticar entre navegadores e clientes.
Gerenciamento de acesso	Estabeleça autenticação de usuário para a interface Unified Manager.
Suporte	Veja as opções de suporte técnico, recursos e contatos.

Configurações da interface e ajuda

No canto superior direito da interface, você pode acessar Ajuda e outra documentação. Você também pode acessar opções de administração, que estão disponíveis no menu suspenso ao lado do seu nome de login.

Logins e senhas de usuário

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

Para obter mais informações sobre usuários e senhas, consulte:

- "Defina a proteção por senha de administrador"
- "Alterar a senha do admin"
- "Alterar senhas para perfis de usuário locais"

Navegadores compatíveis com SANtricity Unified Manager

SANtricity Unified Manager pode ser acessado a partir 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.

Saiba mais sobre a proteção por senha de administrador no SANtricity Unified Manager

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

Senha de administrador e perfis de usuário

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

Além da senha de administrador, a interface Unified Manager inclui perfis de usuário pré-configurados com uma ou mais funções atribuídas a eles. Para obter mais informações, consulte "Como funciona o gerenciamento de acessos".

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

- "Alterar a senha do admin"
- "Alterar senhas para perfis de usuário locais"

Tempo limite da sessão

O software solicita a senha apenas uma vez durante uma sessão de gerenciamento. Uma sessão expira após 30 minutos de inatividade por padrão, momento em que você deve inserir a senha novamente. Se outro usuário acessar o software a partir de outro cliente de gerenciamento e alterar a senha enquanto sua sessão estiver em andamento, você será solicitado a inserir a senha na próxima vez que tentar realizar uma operação de configuração ou de visualização.

Por motivos de segurança, você só pode tentar inserir uma senha cinco vezes antes que o software entre em estado de "bloqueio". Nesse estado, o software rejeita tentativas subsequentes de senha. Você deve aguardar 10 minutos para redefinir para o estado "normal" antes de tentar inserir uma senha novamente.

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

Alterar a senha do admin no SANtricity Unified Manager

Você pode alterar a senha de admin usada para acessar SANtricity Unified Manager.

Antes de começar

- Você deve estar conectado como administrador local, o que inclui permissões de Root admin.
- Você deve saber a senha de administrador atual.

Sobre esta tarefa

Mantenha estas diretrizes em mente ao escolher uma senha:

- As senhas diferenciam maiúsculas de minúsculas.
- Os espaços em branco no final das senhas não são removidos durante a sua criação. Certifique-se de incluir os espaços caso eles estejam presentes na senha.
- Para maior segurança, use pelo menos 15 caracteres alfanuméricos e altere a senha com frequência.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **Funções de usuário local**.
3. Selecione o usuário **admin** na tabela.

   O botão Alterar Senha se torna disponível.

4. Selecione **Change Password**.

   A caixa de diálogo Alterar Senha é aberta.

5. Se não houver um comprimento mínimo de senha definido para senhas de usuários locais, selecione a caixa de seleção para exigir que o usuário insira uma senha para acessar o sistema.
6. Digite a nova senha nos dois campos.
7. Digite sua senha de administrador local para confirmar esta operação e clique em **Alterar**.

Gerenciar os tempos limite de sessão no SANtricity Unified Manager

Você pode configurar tempos limite para SANtricity Unified Manager, para que as

sessões inativas dos usuários sejam desconectadas após um tempo especificado.

Sobre esta tarefa

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

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

Passos

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

   A caixa de diálogo Ativar/Desativar Tempo Limite da Sessão é aberta.
3. Use os controles giratórios para aumentar ou diminuir o tempo em minutos.

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

   > Para desativar os tempos limite de sessão, desmarque a caixa de seleção **Definir o tempo de…**.
4. Clique em **Salvar**.

Array de storage

Saiba mais sobre descoberta no SANtricity Unified Manager

Para gerenciar recursos de storage, primeiro você deve descobrir os arrays de storage na rede.

Como faço para descobrir arrays?

Use a página Adicionar/Descobrir para encontrar e adicionar os arrays de storage que deseja gerenciar na rede da sua organização. Você pode descobrir vários arrays ou pode descobrir apenas um array. Para fazer isso, insira os endereços IP da rede e, em seguida, o Unified Manager tentará conexões individuais com cada endereço IP nesse intervalo.

Saiba mais:

- "Considerações para a descoberta de arrays"
- "Descubra vários arrays de storage"
- "Descobrir um único array"

Como faço para gerenciar arrays?

Após descobrir os arrays, acesse a página **Gerenciar - Todos**. Nessa página, você pode percorrer uma lista de arrays de storage descobertos em sua rede, visualizar o status deles e realizar operações em um único

array ou em um grupo de arrays.

Se você deseja gerenciar um único array, pode selecioná-lo e abrir System Manager.

Saiba mais:

- "Considerações para acessar o System Manager"
- "Gerencie um array de storage individual"
- "Visualizar status do array de storage"

Conceitos

Saiba mais sobre como descobrir arrays de storage no SANtricity Unified Manager

Antes que SANtricity Unified Manager possa exibir e gerenciar recursos de storage, ele precisa descobrir os storage arrays que você deseja gerenciar na rede da sua organização. Você pode descobrir vários storage arrays ou pode descobrir apenas um.

Descobrindo múltiplos arrays de storage

Se optar por descobrir vários arrays, insira um intervalo de endereços IP de rede e o Unified Manager tentará conexões individuais com cada endereço IP nesse intervalo. Qualquer array de storage alcançado com sucesso aparecerá na página Discover e poderá ser adicionado ao seu domínio de gerenciamento.

Descobrindo um único array de storage

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

> Unified Manager descobre e exibe apenas o endereço IP único ou o 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 endereço IP único ou intervalo de endereços IP, então o Unified Manager não os descobrirá nem os exibirá. No entanto, depois de adicionar o array de storage, 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 array de storage que deseja adicionar.

Certificados de serviços web

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

- **Certificados confiáveis**

  Para arrays descobertos pelo Unified Manager, pode ser necessário instalar certificados confiáveis adicionais fornecidos pela Certificate Authority.

  Use o botão **Importar** para importar esses certificados. Se você já se conectou a este array antes, um ou

ambos os certificados do controlador estão expirados, revogados ou faltando um certificado raiz ou intermediário em sua cadeia de certificados. Você deve substituir o certificado expirado ou revogado ou adicionar o certificado raiz ou intermediário ausente antes de gerenciar o array de storage.

- **Certificados autoassinados**

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

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

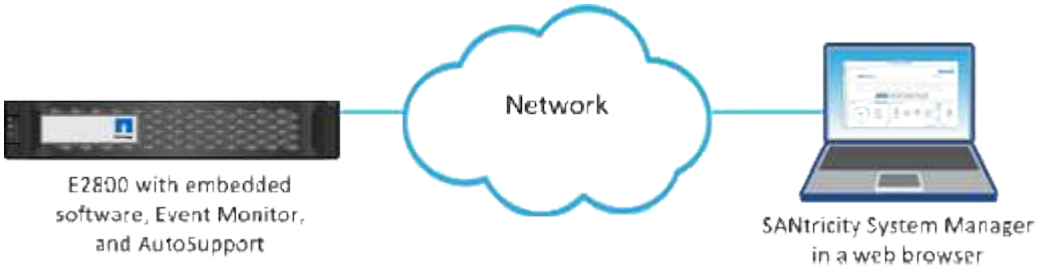
Saiba como acessar o SANtricity System Manager a partir do Unified Manager

Você seleciona um ou mais arrays de storage e usa a opção Launch para abrir SANtricity System Manager quando quiser configurar e gerenciar arrays de storage.

System Manager é um aplicativo integrado nos controladores, que está conectado à rede através de uma porta de gerenciamento Ethernet. Ele inclui todas as funções baseadas em array.

Para acessar System Manager, você deve ter:

- Um dos modelos de array listados aqui: "Visão geral do hardware E-Series"
- Uma conexão fora de banda com um cliente de gerenciamento de rede com um navegador web.



Descobrir arrays

Descubra vários arrays de storage no SANtricity Unified Manager

Você descobre vários arrays para detectar todos os arrays de storage na sub-rede onde reside o servidor de gerenciamento e para adicionar automaticamente os arrays descobertos ao seu domínio de gerenciamento.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security Admin.
- O array de storage deve ser configurado e configurado corretamente.
- As senhas do array de storage devem ser configuradas usando o bloco Access Management do System Manager.
- Para resolver problemas com certificados não confiáveis, você deve ter arquivos de certificado confiáveis de uma Autoridade Certificadora (CA), e os arquivos de certificado devem estar disponíveis em seu

sistema local.

A descoberta de arrays é um procedimento em várias etapas.

Etapa 1: insira o endereço de rede

Você insere um intervalo de endereços de rede para pesquisar na sub-rede local. Qualquer array de storage acessado com sucesso aparece na página Discover e pode ser adicionado ao seu domínio de gerenciamento.

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

Passos

1. Na página Manage, selecione **Add/Discover**.

   A caixa de diálogo Adicionar/Descobrir é exibida.

2. Selecione o botão de opção **Descobrir todos os arrays de storage dentro de um intervalo de rede**.
3. Insira o endereço de rede inicial e o endereço de rede final para pesquisar em sua sub-rede local e clique em **Start Discovery**.

   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 arrays de storage são descobertos.

   Se nenhum array gerenciável for detectado, verifique se os arrays de storage estão conectados corretamente à sua rede e se os endereços atribuídos estão dentro do intervalo. Clique em **New Discovery Parameters** para retornar à página Add/Discover.

4. Revise a lista de arrays de storage descobertos.
5. Selecione a caixa de seleção ao lado de qualquer array de storage que você queira adicionar ao seu domínio de gerenciamento e clique em **Next**.

   Unified Manager realiza uma verificação de credencial em cada array que você adiciona ao domínio de gerenciamento. Pode ser necessário resolver quaisquer certificados autoassinados e certificados não confiáveis associados a esse array.

6. Clique em **Avançar** para prosseguir para a próxima etapa do assistente.

Etapa 2: resolver certificados autoassinados durante a descoberta

Como parte do processo de descoberta, o sistema verifica se os arrays de storage estão usando certificados de uma fonte confiável.

Passos

1. Faça uma das seguintes ações:
   - Se você confiar nas conexões com os arrays de storage descobertos, prossiga para o próximo cartão no assistente. Os certificados autoassinados serão marcados como confiáveis e os arrays de storage serão adicionados ao Unified Manager.
   - Se você não confiar nas conexões com os arrays de storage, selecione **Cancelar** e valide a estratégia de certificado de segurança de cada array de storage antes de adicioná-los ao Unified Manager.
2. Clique em **Avançar** para prosseguir para a próxima etapa do assistente.

Etapa 3: resolver certificados não confiáveis durante a descoberta

Certificados não confiáveis ocorrem quando um array de storage tenta estabelecer uma conexão segura com o Unified Manager, mas a conexão falha ao ser confirmada como segura. Durante o processo de descoberta do array, você pode resolver certificados não confiáveis importando um certificado de autoridade certificadora (CA) (ou certificado assinado por uma CA) emitido por uma terceira parte confiável.

Você pode precisar instalar certificados de CA confiáveis adicionais se alguma das seguintes condições for verdadeira:

- Você adicionou recentemente um array de storage.
- Um ou ambos os certificados expiraram.
- Um ou ambos os certificados estão revogados.
- Um ou ambos os certificados estão sem um certificado raiz ou intermediário.

Passos

1. Selecione a caixa de seleção ao lado de qualquer array de storage para o qual você deseja resolver certificados não confiáveis e, em seguida, selecione o botão **Import**.

   Uma caixa de diálogo é aberta para importar os arquivos de certificado confiáveis.

2. Clique em **Procurar** para selecionar os arquivos de certificado para os arrays de storage.

   Os nomes dos arquivos são exibidos na caixa de diálogo.

3. Clique em **Importar**.

   Os arquivos são carregados e validados.

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

4. Clique em **Avançar** para prosseguir para a próxima etapa do assistente.

Passo 4: forneça as senhas

Você deve inserir as senhas dos arrays de storage que deseja adicionar ao seu domínio de gerenciamento.

Passos

1. Insira a senha para cada array de storage que você deseja adicionar ao Unified Manager.
2. **Opcional:** Associar arrays de storage a um grupo: na lista suspensa, selecione o grupo desejado para associar aos arrays de storage selecionados.
3. Clique em **Concluir**.

Depois que você terminar

Os arrays de storage são adicionados ao seu domínio de gerenciamento e associados ao grupo selecionado (se especificado).

Pode levar vários minutos para o Unified Manager se conectar aos arrays de storage especificados.

Descobrir um único array no SANtricity Unified Manager

Use a opção Adicionar/Descobrir Matriz de Armazenamento Única para descobrir e adicionar manualmente uma única array de storage à rede da organização.

Antes de começar

- O array de storage deve ser configurado e configurado corretamente.
- As senhas do array de storage devem ser configuradas usando o bloco Access Management do System Manager.

Passos

1. Na página Manage, selecione **Add/Discover**.

   A caixa de diálogo Adicionar/Descobrir é exibida.

2. Selecione o botão de opção **Descobrir um único array de storage**.
3. Insira o endereço IP de um dos controladores no array de storage e, em seguida, clique em **Iniciar Descoberta**.

   Pode levar vários minutos para o Unified Manager se conectar ao array de storage especificado.

   > A mensagem Storage Array Not Accessible aparece quando a conexão com o endereço IP do controlador especificado não é bem-sucedida.

4. Se solicitado, resolva quaisquer certificados autoassinados.

   Como parte do processo de descoberta, o sistema verifica se os arrays de storage descobertos estão usando certificados de uma fonte confiável. Se não for possível localizar um certificado digital para um array de storage, ele solicitará que você resolva o certificado que não é 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 array de storage tenta estabelecer uma conexão segura com o Unified Manager, mas a conexão falha ao ser confirmada como segura. Resolva certificados não confiáveis importando um certificado de autoridade certificadora (CA) emitido por uma terceira parte confiável.

6. Clique em **Next**.
7. **Opcional:** Associe o array de storage a um grupo: na lista suspensa, selecione o grupo desejado para associar ao array de storage.

   O grupo "All" está selecionado por padrão.

8. Digite a senha de administrador do array de storage que você deseja adicionar ao seu domínio de gerenciamento e, em seguida, clique em **OK**.

Depois que você terminar

O array de storage é adicionado ao Unified Manager e, se especificado, também é adicionado ao grupo que você selecionou.

Se a coleta automática de dados de suporte estiver ativada, os dados de suporte serão coletados

automaticamente para um array de storage que você adicionar.

Gerenciar arrays

Visualize o status do array de storage no SANtricity Unified Manager

SANtricity Unified Manager exibe o status de cada array de storage que foi descoberto.

Acesse a página **Gerenciar - Tudo**. Nessa página, você pode visualizar o status da conexão entre o Web Services Proxy e esse array de storage.

Os indicadores de status são descritos na tabela a seguir.

Status	Indica
Ideal	O array de storage está em estado ideal. Não há problemas com o certificado e a senha é válida.
Senha inválida	Foi fornecida uma senha inválida para o array de storage.
Certificado não confiável	Uma ou mais conexões com o array de storage não são confiáveis porque o certificado HTTPS é autoassinado e não foi importado, ou o certificado é assinado por uma CA e os certificados raiz e intermediários da CA não foram importados.
Precisa de atenção	Existe um problema com o array de storage que requer sua intervenção para corrigi-lo.
Confinamento	O array de storage está em estado bloqueado.
Desconhecido	O array de storage nunca foi contatado. Isso pode ocorrer quando o Web Services Proxy está sendo inicializado e ainda não estabeleceu contato com o array de storage, ou o array de storage está offline e nunca foi contatado desde que o Web Services Proxy foi iniciado.
Offline	O Web Services Proxy havia contatado anteriormente o array de storage, mas agora perdeu toda a conexão com ele.

Gerencie um array de storage individual no SANtricity Unified Manager

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

Passos

1. Na página Manage, selecione um ou mais arrays de storage 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**.

Alterar senhas do array de storage no SANtricity Unified Manager

Você pode atualizar as senhas usadas para visualizar e acessar arrays de storage no SANtricity Unified Manager.

Antes de começar

- Você deve estar conectado com um perfil de usuário que inclua permissões de Storage admin.
- Você deve saber a senha atual do array de storage, que é definida no System Manager.

Sobre esta tarefa

Nesta tarefa, você insere a senha atual de um array de storage para poder acessá-lo no Unified Manager. Isso pode ser necessário se a senha do array foi alterada no System Manager e agora também precisa ser alterada no Unified Manager.

Passos

1. Na página Manage, selecione um ou mais arrays de storage.
2. Selecione o menu: tarefas incomuns [Fornecer senhas do array de armazenamento].
3. Insira a senha ou senhas para cada array de storage e, em seguida, clique em **Salvar**.

Remover arrays de storage do SANtricity Unified Manager

Você pode remover um ou mais arrays de storage se não quiser mais gerenciá-los pelo SANtricity Unified Manager.

Sobre esta tarefa

Você não poderá acessar nenhum dos arrays de storage que remover. No entanto, você poderá estabelecer uma conexão com qualquer um dos arrays de storage removidos apontando um navegador diretamente para o endereço IP ou nome do host.

A remoção de um array de storage não afeta o array de storage nem seus dados de forma alguma. Se um array de storage for removido acidentalmente, ele pode ser adicionado novamente.

Passos

1. Selecione a página **Manage**.
2. Selecione um ou mais arrays de storage que deseja remover.
3. Selecione o menu: tarefas incomuns [Remover array de storage].

   O array de storage é removido de todas as visualizações no SANtricity Unified Manager.

Importação de configurações

Saiba mais sobre como importar configurações de array de storage no SANtricity Unified Manager

O recurso Importar Configurações permite realizar uma operação em lote para importar as configurações de um array para vários arrays. Esse recurso economiza tempo quando

você precisa configurar vários arrays na rede.

Que configurações podem ser importadas?

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

Saiba mais:

- "Como funciona a importação de configurações"
- "Requisitos para replicar configurações de storage"

Como faço para realizar uma importação em lote?

Em um array de storage que será usado como fonte, abra System Manager e configure as definições desejadas. Em seguida, no Unified Manager, acesse a página Manage e importe as definições para um ou mais arrays.

Saiba mais:

- "Importar configurações de alerta"
- "Importar configurações do AutoSupport"
- "Importar configurações de serviços de diretório"
- "Importar configurações de storage"
- "Importar configurações do sistema"

Conceitos

Saiba mais sobre como configurar vários arrays de storage no SANtricity Unified Manager

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

Configurações disponíveis para importação

As seguintes configurações podem ser importadas para vários arrays:

- **Alertas** — Métodos de alerta para enviar eventos importantes aos administradores, usando e-mail, um servidor syslog ou um servidor SNMP.
- **AutoSupport** — Um recurso que monitora a integridade de um array de storage e envia notificações automáticas para suporte técnico.
- **Serviços de diretório** — Um método de autenticação de usuário que é gerenciado por meio de um servidor LDAP (Lightweight Directory Access Protocol) e serviço de diretório, como o Active Directory da Microsoft.
- **Configuração de storage** — Configurações relacionadas ao seguinte:
  - Volumes (apenas volumes thick e não repositório)
  - Grupos de volume e pools

    - Atribuições de hot spare
- **Configurações do sistema** — Configurações relacionadas ao seguinte:
    - Configurações de verificação de mídia para um volume
    - Configurações de 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 um array de storage que será usado como fonte, configure as definições usando System Manager.
2. Nos arrays de storage que serão usados como destinos, faça backup da configuração usando System Manager.
3. No Unified Manager, vá para a página **Manage** e importe as configurações.
4. Na página **Operações**, revise os resultados da operação Import Settings.

Requisitos para replicar configurações de array de storage no SANtricity Unified Manager

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

Prateleiras

- As prateleiras onde os controladores residem devem ser idênticas nos arrays de origem e de destino.
- Os IDs das prateleiras devem ser idênticos nos arrays de storage de origem e de destino.
- Os módulos de expansão devem ser instalados nos mesmos slots com os mesmos tipos de drive (se o drive for usado na configuração, a localização dos drives não utilizados não importa).

Controladores

- O tipo de controlador pode ser diferente entre os arrays de origem e destino (por exemplo, importar de um E2800 para um E5700), mas o tipo de gabinete RBOD deve ser idêntico.
- Os HICs, incluindo as capacidades de DA do host, devem ser idênticos entre o array de storage de origem e o array de storage de destino.
- A importação de uma configuração duplex para simplex não é suportada; no entanto, a importação de simplex para duplex é permitida.
- As configurações de FDE não estão incluídas no processo de importação.

Status

- Os arrays de destino devem estar em status Ótimo.
- O array de origem não precisa estar no status Ótimo.

Storage

- A capacidade dos discos pode variar entre os arrays de origem e destino, desde que a capacidade de volume no destino seja maior que a da origem. (Um array de destino pode ter discos mais novos e com maior capacidade que não seriam totalmente configurados 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 targets.
- Volumes finos não estão incluídos no processo de importação.

Use importações em lote

Importar configurações de alerta no SANtricity Unified Manager

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

Antes de começar

- Os alertas são configurados no System Manager para o array de storage que você deseja usar como fonte (**Settings › Alerts**).
- A configuração existente para os arrays de storage de destino é salva no System Manager (menu: Configurações [Sistema > Salvar Configuração do Array de Storage]).

Sobre esta tarefa

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

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

Passos

1. Na página Manage, clique em **Import Settings**.

   O assistente de Configurações de Importação é aberto.

2. Na caixa de diálogo Selecionar configurações, selecione **Alertas por e-mail**, **Alertas SNMP** ou **Alertas syslog** e clique em **Avançar**.

   Uma caixa de diálogo é aberta para selecionar o array de storage de origem.

3. Na caixa de diálogo Selecionar Origem, selecione o array 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 inferior a 8.50 não estão disponíveis para seleção. Além disso, uma matriz não aparecerá nesta caixa de diálogo se Unified Manager não conseguir se comunicar com essa matriz (por exemplo, se estiver offline ou se apresentar problemas de certificado, senha ou rede).

5. Clique em **Concluir**.

   A página Operações exibe os resultados da operação de importação. Se a operação falhar, você pode

clicar na linha correspondente para ver mais informações.

Resultados

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

Importar configurações do AutoSupport no SANtricity Unified Manager

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

Antes de começar

- AutoSupport está configurado no System Manager para o array de storage que você deseja usar como fonte (**Support › Support Center**).
- A configuração existente para os arrays de storage de destino é salva no System Manager (menu: Configurações [Sistema > Salvar Configuração do Array de Storage]).

Sobre esta tarefa

As configurações importadas incluem os recursos separados (Básico AutoSupport, AutoSupport OnDemand e Diagnóstico Remoto), a janela de manutenção, o método de entrega e o cronograma de despacho.

Passos

1. Na página Manage, clique em **Import Settings**.

   O assistente de Configurações de Importação é aberto.

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

   Uma caixa de diálogo é aberta para selecionar o array de storage de origem.

3. Na caixa de diálogo Selecionar Origem, selecione o array 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 inferior a 8.50 não estão disponíveis para seleção. Além disso, uma matriz não aparecerá nesta caixa de diálogo se Unified Manager não conseguir se comunicar com essa matriz (por exemplo, se estiver offline ou se apresentar problemas de certificado, senha ou rede).

5. Clique em **Concluir**.

   A página Operações exibe os resultados da operação de importação. Se a operação falhar, você pode clicar na linha correspondente para ver mais informações.

Resultados

Os arrays de storage de destino agora estão configurados com as mesmas configurações de AutoSupport que o array de origem.

Importar configurações de serviços de diretório no SANtricity Unified Manager

Você pode importar uma configuração de serviços de diretório de um array de storage para outros arrays de storage. Essa 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 o array de storage que você deseja usar como fonte (**Settings › Gerenciamento de Acesso**).
- A configuração existente para os arrays de storage de destino é salva no System Manager (menu: Configurações [Sistema > Salvar Configuração do Array de Storage]).

Sobre esta tarefa

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

Passos

1. Na página Manage, clique em **Import Settings**.

   O assistente de Configurações de Importação é aberto.

2. Na caixa de diálogo Selecionar configurações, selecione **Directory services** e clique em **Next**.

   Uma caixa de diálogo é aberta para selecionar o array de storage de origem.

3. Na caixa de diálogo Selecionar Origem, selecione o array 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 inferior a 8.50 não estão disponíveis para seleção. Além disso, uma matriz não aparecerá nesta caixa de diálogo se Unified Manager não conseguir se comunicar com essa matriz (por exemplo, se estiver offline ou se apresentar problemas de certificado, senha ou rede).

5. Clique em **Concluir**.

   A página Operações exibe os resultados da operação de importação. Se a operação falhar, você pode clicar na linha correspondente para ver mais informações.

Resultados

Os arrays de storage de destino agora estão configurados com os mesmos serviços de diretório que o array de origem.

Importar as configurações do sistema no SANtricity Unified Manager

Você pode importar a configuração do sistema de um array de storage para outros arrays de storage. Essa 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 o array de storage que você deseja usar como origem.
- A configuração existente para os arrays de storage de destino é salva no System Manager (menu: Configurações [Sistema > Salvar Configuração do Array de Storage]).

Sobre esta tarefa

As configurações importadas incluem configurações de verificação de mídia para um volume, configurações de SSD para controladores e balanceamento de carga automático (não inclui relatórios de conectividade de host).

Passos

1. Na página Manage, clique em **Import Settings**.

   O assistente de Configurações de Importação é aberto.

2. Na caixa de diálogo Selecionar configurações, selecione **System** e clique em **Next**.

   Uma caixa de diálogo é aberta para selecionar o array de storage de origem.

3. Na caixa de diálogo Selecionar Origem, selecione o array 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 inferior a 8.50 não estão disponíveis para seleção. Além disso, uma matriz não aparecerá nesta caixa de diálogo se Unified Manager não conseguir se comunicar com essa matriz (por exemplo, se estiver offline ou se apresentar problemas de certificado, senha ou rede).

5. Clique em **Concluir**.

   A página Operações exibe os resultados da operação de importação. Se a operação falhar, você pode clicar na linha correspondente para ver mais informações.

Resultados

Os arrays de storage de destino agora estão configurados com as mesmas configurações de sistema do array de origem.

Importar as configurações de configuração de storage no SANtricity Unified Manager

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

Antes de começar

- O storage é configurado no SANtricity System Manager para o array de storage que você deseja usar como origem.
- A configuração existente para os arrays de storage de destino é salva no System Manager (menu: Configurações [Sistema > Salvar Configuração do Array de Storage]).

- Os arrays de origem e destino devem atender a estes requisitos:
  - As prateleiras onde os controladores residem devem ser idênticas.
  - Os IDs das prateleiras devem ser idênticos.
  - Os módulos de expansão devem ser populados nos mesmos slots com os mesmos tipos de unidades.
  - O tipo de gabinete RBOD deve ser idêntico.
  - Os HICs, incluindo os recursos de Data Assurance do host, devem ser idênticos.
  - Os arrays de destino devem estar em status Ótimo.
  - A capacidade de volume no array de destino é maior do que a capacidade do array de origem.
- Você compreende 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 targets.
  - Volumes finos não estão incluídos no processo de importação.

Sobre esta tarefa

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

Passos

1. Na página Manage, clique em **Import Settings**.

   O assistente de Configurações de Importação é aberto.

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

   Uma caixa de diálogo é aberta para selecionar o array de storage de origem.

3. Na caixa de diálogo Selecionar Origem, selecione o array 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 inferior a 8.50 não estão disponíveis para seleção. Além disso, uma matriz não aparecerá nesta caixa de diálogo se Unified Manager não conseguir se comunicar com essa matriz (por exemplo, se estiver offline ou se apresentar problemas de certificado, senha ou rede).

5. Clique em **Concluir**.

   A página Operações exibe os resultados da operação de importação. Se a operação falhar, você pode clicar na linha correspondente para ver mais informações.

Resultados

Os arrays de storage de destino agora estão configurados com a mesma configuração de storage do array de origem.

Perguntas frequentes sobre importação de configurações para SANtricity Unified Manager

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

Quais configurações serão importadas?

O recurso Importar Configurações é uma operação em lote que carrega configurações de um array de storage para vários arrays de storage. As configurações importadas durante essa operação dependem de como o array de storage está configurado no SANtricity System Manager.

As seguintes configurações podem ser importadas para vários arrays de storage:

- **Alertas por e-mail** — As configurações incluem um endereço de servidor de e-mail e os endereços de e-mail dos destinatários dos alertas.
- **Alertas do 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 do servidor SNMP.
- **AutoSupport** — As configurações incluem os recursos separados (Básico AutoSupport, AutoSupport OnDemand, e Diagnóstico Remoto), a janela de manutenção, o método de entrega e o cronograma de despacho.
- **Serviços de diretório** — A configuração inclui o nome de domínio e o URL de um servidor LDAP (Lightweight Directory Access Protocol), juntamente com os mapeamentos dos grupos de usuários do servidor LDAP para as funções predefinidas do array de storage.
- **Configuração de storage** — As configurações incluem volumes (somente thick e somente volumes não repositório), grupos de volume, pools e atribuições de hot spare.
- **Configurações do sistema** — As configurações incluem as definições de verificação de mídia para um volume, cache SSD para controladores e balanceamento de carga automático (não inclui relatórios de conectividade de host).

Por que não vejo todos os meus arrays de storage?

Durante a operação de Import Settings, alguns dos seus arrays de storage podem não estar disponíveis na caixa de diálogo de seleção de destino.

Os arrays de storage podem não aparecer pelos seguintes motivos:

- A versão do firmware é inferior a 8.50.
- O array de storage está offline.
- O sistema não consegue se comunicar com esse array de storage (por exemplo, o array de storage apresenta problemas com certificado, senha ou rede).

Grupos de arrays

Saiba mais sobre a visão geral de grupos no SANtricity Unified Manager

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

O que são grupos de array?

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

Existem dois tipos de grupos:

- **Grupo Todos** — O grupo Todos é o grupo padrão e inclui todos os arrays de storage descobertos em sua organização. O grupo Todos pode ser acessado na visualização principal.
- **Grupo criado pelo usuário** — Um grupo criado pelo usuário inclui os arrays de storage que você seleciona manualmente para adicionar a esse grupo. Os grupos criados pelo usuário podem ser acessados na visualização principal.

Como faço para configurar grupos?

Na página Manage Groups, você pode criar um grupo e, em seguida, adicionar arrays a esse grupo.

Saiba mais:

- "Configurar grupo de array de storage"

Configurar um grupo de arrays de storage no SANtricity Unified Manager

Você cria grupos de storage e, em seguida, adiciona arrays de storage aos grupos.

Configurar 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 o menu: Gerenciar Grupos [Create storage array group].
2. No campo **Nome**, digite um nome para o novo grupo.
3. Selecione os arrays de storage que deseja adicionar ao novo grupo.
4. Clique em **Create**.

Etapa 2: adicionar array de storage ao grupo

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

Passos

1. Na tela principal, selecione **Gerenciar** e, em seguida, selecione o grupo ao qual deseja adicionar arrays de storage.
2. Selecione o menu: Gerenciar grupos [Adicionar arrays de storage ao grupo].
3. Selecione os arrays de storage que deseja adicionar ao grupo.
4. Clique em **Adicionar**.

Remover arrays de storage de um grupo no SANtricity Unified Manager

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

Sobre esta tarefa

Remover arrays de storage de um grupo não afeta o array de storage nem seus dados de forma alguma. Se o seu array de storage for gerenciado pelo System Manager, você ainda pode gerenciá-lo usando seu navegador. Se um array de storage for removido acidentalmente de um grupo, ele pode ser adicionado novamente.

Passos

1. Na página Gerenciar, selecione o menu: Gerenciar Grupos[Remover arrays de storage do grupo].
2. Na lista suspensa, selecione o grupo que contém os arrays de storage que você deseja remover e, em seguida, clique na caixa de seleção ao lado de cada array de storage que você deseja remover do grupo.
3. Clique em **Remover**.

Excluir um grupo de array de storage no SANtricity Unified Manager

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

Sobre esta tarefa

Esta operação exclui apenas o grupo de array de storage. Os arrays de storage associados ao grupo excluído permanecem acessíveis através da visualização Manage All ou de qualquer outro grupo ao qual estejam associados.

Passos

1. Na página Gerenciar, selecione o menu: Gerenciar Grupos[Excluir grupo de array de storage].
2. Selecione um ou mais grupos de array de storage que você deseja excluir.
3. Clique em **Delete**.

Renomear um grupo de array de storage no SANtricity Unified Manager

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

Sobre esta tarefa

Tenha essas orientações em mente.

- Um nome pode ser composto por letras, números e os caracteres especiais sublinhado (_), hífen (-) e cerquilha (#). Se você escolher qualquer outro caractere, uma mensagem de erro será exibida. Você será solicitado a escolher outro nome.
- Limite o nome a 30 caracteres. Quaisquer espaços em branco no início e no final do nome são removidos.
- Use um nome exclusivo e significativo que seja fácil de entender e lembrar.
- Evite nomes arbitrários ou nomes que rapidamente percam seu significado no futuro.

Passos

1. Na tela principal, selecione **Gerenciar** e, em seguida, selecione o grupo de array de storage que deseja renomear.
2. Selecione o menu: Gerenciar Groups[Rename storage array group].
3. No campo **Nome do Grupo**, digite um novo nome para o grupo.
4. Clique em **Renomear**.

Atualizações

Saiba mais sobre o Upgrade Center no SANtricity Unified Manager

A partir do Centro de Atualização, você pode gerenciar upgrades do software SANtricity OS e da NVSRAM para vários arrays de storage.

Como funcionam as atualizações?

Você baixa o software mais recente do sistema operacional e, em seguida, atualiza um ou mais arrays.

Fluxo de trabalho de atualização

Os passos a seguir fornecem um fluxo de trabalho de alto nível para realizar atualizações de software.

1. Você baixa o arquivo de software SANtricity OS mais recente do site de suporte (um link está disponível no Unified Manager na página de suporte). Salve o arquivo no sistema host de gerenciamento (o host onde você acessa Unified Manager em um navegador) e, em seguida, descompacte o arquivo.
2. No Unified Manager, você carrega o arquivo de software do SANtricity OS e o arquivo NVSRAM no repositório (uma área do servidor Web Services Proxy onde os arquivos são armazenados). Você pode adicionar arquivos pelo **Upgrade Center › Upgrade SANtricity OS Software** ou pela Upgrade Center > Manage Software Repository.
3. Após os arquivos serem carregados no repositório, você pode então selecionar o arquivo a ser usado na atualização. Na página Upgrade SANtricity OS software (menu: Upgrade Center[Upgrade SANtricity OS software]), você seleciona o arquivo de software do SANtricity OS e o arquivo NVSRAM. Após selecionar um arquivo de software, uma lista de arrays de storage compatíveis aparece nesta página. Em seguida, você seleciona os arrays de storage que deseja atualizar com o novo software. (Você não pode selecionar arrays incompatíveis.)
4. Em seguida, você pode iniciar imediatamente a transferência e ativação do software ou optar por preparar os arquivos para ativação em outro momento. Durante o processo de atualização, Unified Manager executa as seguintes tarefas:
   a. Executa uma verificação de integridade nos arrays de storage para determinar se existem condições que possam impedir a conclusão da atualização. Se algum array falhar na verificação de integridade, você pode ignorar esse array específico e continuar a atualização para os demais, ou pode interromper todo o processo e solucionar problemas nos arrays que não foram aprovados.
   b. Transfere os arquivos de atualização para cada controlador.
   c. Reinicializa os controladores e ativa o novo software SANtricity OS, um controlador por vez. Durante a ativação, o arquivo SANtricity OS existente é substituído pelo novo arquivo.

      Você também pode especificar que o software seja ativado em um momento posterior.

Atualização imediata ou faseada

Você pode ativar a atualização imediatamente ou prepará-la para um momento posterior. Você pode optar por ativar mais tarde pelos seguintes motivos:

- **Horário do dia** — A ativação do software pode demorar bastante, então talvez seja melhor esperar até que a carga de E/S esteja mais leve. Dependendo da carga de E/S e do tamanho do cache, uma atualização do controlador geralmente leva de 15 a 25 minutos para ser concluída. Os controladores reinicializam e realizam 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 e firmware em um array de storage antes de atualizar os arquivos em outros arrays de storage.

Para ativar o software em fase de testes, acesse o **Support › Upgrade Center** e clique em **Ativar** na área intitulada 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 **Upgrade Center › Pre-Upgrade Health Check**).

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
- Hot spares em uso
- Grupos de volume incompletos
- Operações exclusivas em andamento
- Volumes ausentes
- Controlador em estado não ideal
- Número excessivo de eventos de log de eventos
- Falha na validação do banco de dados de configuração
- Unidades com versões antigas do DACstore

O que preciso saber antes de atualizar?

Antes de atualizar vários arrays de storage, revise as principais considerações como parte do seu planejamento.

Versões atuais

Você pode visualizar as versões atuais do software SANtricity OS na página Gerenciar do Unified Manager para cada array de storage. A versão é exibida na coluna Software SANtricity OS. As informações do firmware do controlador e da NVSRAM estão disponíveis em uma caixa de diálogo pop-up ao clicar 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 corretamente com os controladores.

Para informações sobre compatibilidade, consulte o "NetApp Matriz de interoperabilidade". Veja também os procedimentos nos Guias Rápidos para o seu sistema operacional. Os Guias Rápidos estão disponíveis em "Documentação do E-Series e SANtricity".

Controladores duplos

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

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

Após a conclusão da atualização, pode ser necessário redistribuir manualmente os volumes entre os controladores para garantir que os volumes retornem ao controlador proprietário correto.

Atualizar software e firmware

Execute uma verificação de integridade pré-atualização no SANtricity Unified Manager

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 array de storage para garantir que a atualização possa prosseguir.

Passos

1. Na tela principal, selecione **Gerenciar** e, em seguida, selecione **Upgrade Center › Verificação de integridade pré-atualização**.

   A caixa de diálogo Verificação de integridade pré-atualização é aberta e lista todos os sistemas de storage detectados.

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

   O progresso é exibido na caixa de diálogo enquanto a verificação de integridade é realizada.

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

> ⓘ Se algum dos arrays falhar na verificação de integridade, você pode ignorar esse array específico e continuar a atualização para os outros, ou pode interromper todo o processo e solucionar os problemas nos arrays que não foram aprovados.

Atualizar SANtricity OS

Atualize um ou mais arrays de storage com o software e o NVSRAM mais recentes para garantir que você tenha todos os recursos e correções de bugs mais recentes. Controller NVSRAM é um arquivo do controlador que especifica as configurações padrão dos controladores.

Antes de começar

- Os arquivos mais recentes do SANtricity OS estão disponíveis no sistema host onde o SANtricity Web Services Proxy e Unified Manager estão em execução.
- Você sabe se deseja ativar sua atualização de software agora ou mais tarde.

  Você pode optar por ativar mais tarde por estes motivos:

  - **Horário do dia** — A ativação do software pode demorar bastante, então talvez seja melhor esperar até que as cargas de E/S estejam mais leves. Os controladores fazem failover durante a ativação, portanto o desempenho pode ser inferior ao normal até que a atualização seja concluída.
  - **Tipo de pacote** — Você pode querer testar o novo software do sistema operacional em um array de storage antes de atualizar os arquivos em outros arrays de storage.

> Para atualizar para a versão 11.80.x ou posterior, os sistemas devem estar executando o SANtricity OS 11.70.5.

Sobre esta tarefa

> Risco de perda de dados ou risco de danos ao array de storage - Não faça alterações no array de storage enquanto a atualização estiver em andamento. Mantenha a alimentação do array de storage.

Passos

1. Se o seu array de storage contiver apenas um controlador ou se um multipath driver não estiver em uso, interrompa a atividade de E/S para o array de storage para evitar erros de aplicativo. Se o seu array de storage tiver dois controladores e você tiver um multipath driver instalado, não é necessário interromper a atividade de E/S.
2. Na tela principal, selecione **Gerenciar** e, em seguida, selecione um ou mais arrays de storage que você deseja atualizar.
3. Selecione o menu: Upgrade Center [Upgrade SANtricity OS Software].

   A página de atualização do software SANtricity OS é exibida.

4. Faça o download do pacote de software SANtricity OS mais recente do site de suporte da NetApp para o seu computador local.

   a. Clique em **Adicionar novo arquivo ao repositório de software**.
   b. Clique no link para encontrar os downloads mais recentes do **SANtricity OS**.
   c. Clique no link **Download Latest Release**.
   d. Siga as instruções restantes para baixar o arquivo SANtricity OS e o arquivo NVSRAM para o seu computador local.

O firmware assinado digitalmente é necessário na versão 8.42 e superiores. Se você tentar baixar firmware não assinado, um erro será exibido e o download será interrompido.

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

   a. No menu suspenso **Selecionar um arquivo de software SANtricity OS**, selecione o arquivo SANtricity OS que você baixou para o seu computador local.

      Caso haja vários arquivos disponíveis, os arquivos são classificados da data mais recente para a mais antiga.

      O repositório de software lista todos os arquivos de software associados ao Web Services Proxy. Se você não encontrar o arquivo que deseja usar, você pode clicar no link **Adicionar novo arquivo ao repositório de software** para navegar até o local onde o arquivo do OS que você deseja adicionar está localizado.

   a. No menu suspenso **Select an NVSRAM file**, selecione o arquivo do controlador que deseja usar.

      Caso haja vários arquivos, os arquivos são classificados da data mais recente para a mais antiga.

6. Na tabela Compatible Storage Array, revise os arrays de storage que são compatíveis com o arquivo de software do sistema operacional que você selecionou e, em seguida, selecione os arrays que deseja atualizar.
   - Os arrays de storage que você selecionou na visualização Manage e que são compatíveis com o arquivo de firmware selecionado são selecionados por padrão na tabela Compatible Storage Array.
   - Os arrays de storage que não podem ser atualizados com o arquivo de firmware selecionado não são selecionáveis na tabela de array de storage compatível, conforme indicado pelo status **Incompatível**.
7. **Opcional:** para transferir o arquivo de software para os arrays de armazenamento sem ativá-los, selecione a caixa de seleção **Transferir o software do SO para os arrays de armazenamento, marcá-lo como preparado e ativar em outro momento**.
8. Clique em **Start**.
9. Dependendo se você optou por ativar agora ou mais tarde, faça um dos seguintes:
   - Digite **TRANSFER** para confirmar que deseja transferir as versões de software do sistema operacional propostas nos arrays que você selecionou para upgrade e, em seguida, clique em **Transfer**.

     Para ativar o software transferido, selecione **Upgrade Center › Ativar Software de SO Preparado**.

   - Digite **UPGRADE** para confirmar que deseja transferir e ativar as versões de software do sistema operacional propostas nos arrays selecionados para upgrade e, em seguida, clique em **Upgrade**.

     O sistema transfere o arquivo de software para cada array de storage que você selecionou para atualizar e, em seguida, ativa esse arquivo iniciando uma reinicialização.

     As seguintes ações ocorrem durante a operação de upgrade:

   - Uma verificação de integridade pré-atualização é executada como parte do processo de atualização. A verificação de integridade pré-atualização avalia todos os componentes do array de storage para garantir que a atualização possa prosseguir.
   - Se alguma verificação de integridade falhar em um array de storage, a atualização será interrompida. Você pode clicar nas reticências (…) e selecionar **Salvar Log** para revisar os erros. Você também

pode optar por ignorar o erro de verificação de integridade e clicar em **Continuar** para prosseguir com a atualização.

- Você pode cancelar a operação de upgrade após a verificação de integridade pré-upgrade.

10. **Opcional:** Após a conclusão da atualização, você pode ver uma lista do que foi atualizado para um array de storage específico clicando nas reticências (…) e, em seguida, selecionando **Salvar Log**.

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

Ative o software do sistema operacional em modo de preparação no SANtricity Unified Manager

Você pode optar por ativar o arquivo de software imediatamente ou aguardar um momento mais conveniente. Este procedimento pressupõe que você escolheu ativar o arquivo de software em um momento posterior.

Sobre esta tarefa

Você pode transferir os arquivos de firmware sem ativá-los. Você pode optar por ativar depois pelos seguintes motivos:

- **Horário do dia** — A ativação do software pode demorar bastante, então talvez seja melhor esperar até que as cargas de E/S estejam mais leves. Os controladores reinicializam e realizam failover durante a ativação, portanto o desempenho pode ser inferior ao normal até que a atualização seja concluída.
- **Tipo de pacote** — Você pode querer testar o novo software e firmware em um array de storage antes de atualizar os arquivos em outros arrays de storage.

> Não é possível interromper o processo de ativação depois que ele começa.

Passos

1. Na tela principal, selecione **Gerenciar**. Se necessário, clique na coluna Status para classificar, na parte superior da página, todos os arrays de storage com o status "OS Upgrade (awaiting activation)."
2. Selecione um ou mais arrays de storage para os quais deseja ativar o software e, em seguida, selecione **Upgrade Center › Activate Staged OS Software**.

    As seguintes ações ocorrem durante a operação de upgrade:

    - Uma verificação de integridade pré-atualização é executada como parte do processo de ativação. A verificação de integridade pré-atualização avalia todos os componentes do array de storage para garantir que a ativação possa prosseguir.
    - Se alguma verificação de integridade falhar para um array de storage, a ativação será interrompida. Você pode clicar nas reticências (…) e selecionar **Salvar Log** para revisar os erros. Você também pode optar por ignorar o erro de verificação de integridade e então clicar em **Continuar** para prosseguir com a ativação.
    - Você pode cancelar a operação de ativação após a verificação de integridade pré-atualização. Com a conclusão bem-sucedida da verificação de integridade pré-atualização, a ativação ocorre. O tempo necessário para ativar depende da configuração do seu array de storage e dos componentes que você está ativando.

3. **Opcional:** Após a conclusão da ativação, você pode ver uma lista do que foi ativado para um array de storage específico clicando nas reticências (…) e, em seguida, selecionando **Salvar registro**.

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

Gerencie o repositório de software SANtricity no Unified Manager

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

Se você não encontrar o arquivo que deseja usar, poderá utilizar a opção Gerenciar Repositório de Software para importar um ou mais arquivos do SANtricity OS para o sistema host onde o Web Services Proxy e Unified Manager estão em execução. 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, certifique-se de que os arquivos do OS estejam disponíveis no seu sistema local.

Passos

1. Na tela principal, selecione **Gerenciar** e, em seguida, selecione **Upgrade Center › Manage Software Repository**.

   A caixa de diálogo Gerenciar repositório de software é exibida.

2. Execute uma das seguintes ações:

Opção	Faça isso….
Importar	a. Clique em **Import.** b. Clique em **Procurar** e, em seguida, navegue até o local onde os arquivos do sistema operacional que você deseja adicionar residem. Os arquivos do sistema operacional têm um nome de arquivo semelhante a `N2800-830000-000.dlp`. c. Selecione um ou mais arquivos do sistema operacional que você deseja adicionar e clique em **Importar**.
Excluir	a. Selecione um ou mais arquivos do sistema operacional que você deseja remover do repositório de software. b. Clique em **Delete**.

Resultados

Se você selecionou importar, os arquivos são carregados e validados. Se você selecionou excluir, os arquivos são removidos do repositório de software.

Limpar o software do sistema operacional em estágio no SANtricity Unified Manager

Você pode remover o software do sistema operacional em fase de preparação para garantir que uma versão pendente não seja ativada inadvertidamente em um momento posterior. Remover o software do sistema operacional em fase de preparação não afeta a versão atual em execução nos arrays de storage.

Passos

1. Na tela principal, selecione **Gerenciar** e, em seguida, selecione **Upgrade Center › Clear Staged OS Software**.

   A caixa de diálogo Limpar Software do SO em Estágio é aberta e lista todos os sistemas de storage detectados com software ou NVSRAM pendentes.

2. Se necessário, filtre ou classifique os sistemas de armazenamento na lista para que você possa visualizar todos os sistemas que possuem software em estágio.
3. Selecione as caixas de seleção para os sistemas de armazenamento com software pendente que você deseja limpar.
4. Clique em **Clear**.

   O status da operação é exibido na caixa de diálogo.

Espelhamento

Saiba mais sobre espelhamento no SANtricity Unified Manager

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

> O espelhamento síncrono não está disponível no sistema de storage EF600/EF600C ou EF300/EF300C.

O que é espelhamento?

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

Saiba mais:

- "Como o espelhamento funciona"
- "Terminologia de espelhamento"

Como configuro o espelhamento?

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

Saiba mais:

- "Fluxo de trabalho de configuração de espelhamento"
- "Requisitos para usar espelhamento"
- "Criar par espelhado assíncrono"
- "Criar par espelhado síncrono"

Conceitos

Saiba mais sobre o espelhamento SANtricity

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

O espelhamento síncrono não está disponível no sistema de storage EF600/EF600C ou EF300/EF300C.

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 um cronograma, o que minimiza ou evita o tempo de inatividade que pode resultar de corrupção de dados ou perda de dados. O espelhamento assíncrono captura o estado do volume primário em um determinado momento e copia apenas os dados que foram alterados desde a última captura de imagem. O site primário pode ser atualizado imediatamente e o site secundário pode ser atualizado conforme a largura de banda permitir. As informações são armazenadas em cache e enviadas posteriormente, à medida que os recursos de rede se tornam disponíveis. Esse tipo de espelhamento é ideal para processos periódicos, como backup e arquivamento.

O espelhamento síncrono replica volumes de dados em tempo real para garantir disponibilidade contínua. O objetivo é atingir um ponto de recuperação (RPO) de zero perda de dados, mantendo uma cópia dos dados importantes disponível caso ocorra um desastre em um dos dois arrays de storage. A cópia é idêntica aos dados de produção em todos os momentos, pois a cada gravação realizada no volume primário, uma gravação também é realizada no volume secundário. O host não recebe a 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 os tipos de espelhamento

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

Atributo	Assíncrono	Síncrono
Método de replicação	Ponto específico no tempo — O espelhamento é feito sob demanda ou automaticamente de acordo com uma programação definida pelo usuário.	Contínuo — O espelhamento é executado automaticamente de forma contínua, copiando dados de cada gravação do host.
Distância	Suporta longas distâncias entre arrays. Normalmente, a distância é limitada apenas pelas capacidades da rede e pela tecnologia de extensão de canal.	Restrito a distâncias mais curtas entre arrays. Normalmente, a distância deve ser de cerca de 10 km (6,2 milhas) do array de storage local para atender aos requisitos de latência e desempenho do aplicativo.

Atributo	Assíncrono	Síncrono
Método de comunicação	Uma rede IP padrão ou Fibre Channel.	Somente rede Fibre Channel.
Tipos de volume	Padrão ou thin.	Somente padrão.

Fluxos de trabalho de configuração do espelhamento SANtricity

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

Fluxo de trabalho de espelhamento assíncrono

O espelhamento assíncrono envolve o seguinte fluxo de trabalho:

1. Realize a configuração inicial no Unified Manager:
   a. Selecione o array de storage local como a origem para a transferência de dados.
   b. Crie ou selecione um grupo de consistência de espelhamento existente, que é um contêiner para o volume primário no array de storage local e o volume secundário no array de storage remoto. Os volumes primário e secundário são chamados de "par espelhado". Se você estiver criando o grupo de consistência de espelhamento pela primeira vez, especifique se deseja realizar sincronizações manuais ou agendadas.
   c. Selecione um volume primário do array de storage local e, em seguida, determine sua capacidade reservada. A capacidade reservada é a capacidade física alocada para ser usada na operação de cópia.
   d. Selecione um array de storage remoto como destino da transferência, um volume secundário e, em seguida, determine sua capacidade reservada.
   e. Inicie a transferência inicial de dados do volume primário para o volume secundário. Dependendo do tamanho do volume, essa transferência inicial pode levar várias horas.
2. Verifique o progresso da sincronização inicial:
   a. No Unified Manager, inicie o System Manager para o array local.
   b. No System Manager, visualize o status da operação de espelhamento. Quando o espelhamento estiver concluído, o status do par espelhado será "Ótimo".
3. Opcionalmente, você pode reagendar ou executar manualmente as 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. Há impacto mínimo na taxa de transferência de escrita e na latência.

Fluxo de trabalho de espelhamento síncrono

Espelhamento síncrono envolve o seguinte fluxo de trabalho:

1. Realize a configuração inicial no Unified Manager:

a. Selecione um array de storage local como origem para a transferência de dados.
b. Selecione um volume primário do array de storage local.
c. Selecione um array de storage remoto como destino para a transferência de dados e, em seguida, selecione um volume secundário.
d. Selecione as prioridades de sincronização e ressincronização.
e. Inicie a transferência inicial de dados do volume primário para o volume secundário. Dependendo do tamanho do volume, essa transferência inicial pode levar várias horas.

2. Verifique o progresso da sincronização inicial:
   a. No Unified Manager, inicie o System Manager para o array local.
   b. No System Manager, visualize o status da operação de espelhamento. Quando o espelhamento estiver concluído, o status do par espelhado será "Ótimo". Os dois arrays tentam permanecer sincronizados por meio de operações normais. Somente blocos novos e alterados são transferidos do volume primário para o volume secundário.
3. Opcionalmente, você pode alterar as configurações de sincronização no System Manager.

> Como a replicação síncrona é contínua, o link de replicação entre os dois sites deve fornecer largura de banda suficiente.

Saiba mais sobre a terminologia de espelhamento no SANtricity Unified Manager

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

Termo	Descrição
Array de storage local	O array de storage local é o array de storage sobre o qual você está agindo.
Grupo de consistência	Um grupo de consistência de espelhamento é um contêiner para um ou mais pares espelhados. Para operações de espelhamento assíncrono, você deve criar um grupo de consistência de espelhamento. Todos os pares espelhados em um grupo são ressincronizados simultaneamente, preservando assim um ponto de recuperação consistente. Espelhamento síncrono não utiliza grupos de consistência de espelhamento.
Par espelhado	Um par espelhado é composto por dois volumes, um volume primário e um volume secundário. No espelhamento assíncrono, um par espelhado sempre pertence a um grupo de consistência de espelhamento. As operações de gravação são realizadas primeiro no volume primário e depois replicadas para o volume secundário. Cada par espelhado em um grupo de consistência de espelhamento compartilha as mesmas configurações de sincronização.
Volume primário	O volume primário de um par espelhado é o volume de origem a ser espelhado.

Termo	Descrição
Array de storage remoto	O array de storage remoto é geralmente designado como o site secundário, que normalmente contém uma réplica dos dados em uma configuração de espelhamento.
Capacidade reservada	A capacidade reservada é a capacidade física alocada que é usada para qualquer operação de serviço de cópia e objeto de armazenamento. Ela não é diretamente legível pelo host. Esses volumes são necessários para que o controlador possa salvar de forma persistente as informações necessárias para manter o espelhamento em estado operacional. Eles contêm informações como logs delta e dados de copy-on-write.
Volume secundário	O volume secundário de um par espelhado geralmente está localizado em um site secundário e contém uma réplica dos dados.
Sincronização	A sincronização ocorre na sincronização inicial entre o array de storage local e o array de storage remoto. A sincronização também ocorre quando os volumes primário e secundário ficam dessincronizados após uma interrupção na comunicação. Quando o link de comunicação volta a funcionar, quaisquer dados não replicados são sincronizados com o array de storage do volume secundário.

Requisitos para usar espelhamento no SANtricity Unified Manager

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

Unified Manager

- O serviço Web Services Proxy deve estar em execução.
- Unified Manager deve estar sendo executado em seu host local por meio de uma conexão HTTPS.
- Unified Manager deve exibir certificados SSL válidos para o array de storage. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando Unified Manager e navegando até **Certificate › Certificate Management**.

Array de storage

> O espelhamento síncrono não está disponível no array de storage EF600/EF600C ou EF300/EF300C.

- Você precisa ter dois arrays de storage.
- Cada array de storage deve ter dois controladores.
- Os dois arrays de storage devem ser detectados no Unified Manager.
- Cada controlador, tanto no array primário quanto no array secundário, deve ter uma porta de gerenciamento Ethernet configurada e deve estar conectado à sua rede.
- Os arrays de storage possuem uma versão mínima de firmware de 7.84. (Cada um deles pode executar diferentes versões de sistema operacional.)
- Você deve saber a senha dos arrays de storage local e remoto.

- Você precisa ter capacidade livre suficiente no array de storage remoto para criar um volume secundário igual ou maior que o volume primário que você deseja espelhar.
- O espelhamento assíncrono é compatível com controladores que possuem portas de host Fibre Channel (FC) ou iSCSI, enquanto o espelhamento síncrono é compatível apenas com controladores que possuem portas de host FC.

Requisitos de conectividade

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

- Cada controlador do array de storage dedica sua porta host FC de número mais alto às operações de espelhamento.
- Se o controlador tiver tanto portas FC básicas quanto portas FC de placa de interface de host (HIC), a porta de número mais alto estará em uma HIC. Qualquer host conectado à porta dedicada será desconectado e nenhuma solicitação de login de host será aceita. As solicitações de E/S nessa porta são aceitas somente de controladores que participam de operações de espelhamento.
- As portas de espelhamento dedicadas devem ser conectadas a um ambiente de malha FC que suporte as interfaces de serviço de diretório e serviço de nomes. Em particular, FC-AL e ponto a ponto não são suportados como opções de conectividade entre os controladores que participam de relações de espelhamento.

O espelhamento através de uma interface iSCSI (somente assíncrono) requer o seguinte:

- Ao contrário do FC, iSCSI não requer uma porta dedicada. Quando o espelhamento assíncrono é usado em ambientes iSCSI, não é necessário dedicar nenhuma das portas iSCSI front-end do array de storage para uso com espelhamento assíncrono; essas portas são compartilhadas tanto para o tráfego de espelhamento assíncrono quanto para as conexões de E/S do host para o array.
- O controlador mantém uma lista de sistemas de armazenamento remoto com os quais o iniciador iSCSI tenta estabelecer uma sessão. A primeira porta que estabelece com sucesso uma conexão iSCSI é usada para toda a comunicação subsequente com esse array de storage. Se a comunicação falhar, uma nova sessão é tentada usando todas as portas disponíveis.

  Os controladores E4000 não suportam espelhamento iSCSI.

- As portas iSCSI são configuradas no nível do array, porta por porta. A comunicação entre controladores para mensagens de configuração e transferência de dados utiliza as configurações globais, incluindo as configurações para:
  - VLAN: os sistemas local e remoto devem ter a mesma configuração de VLAN para comunicar
  - Porta de escuta iSCSI
  - Quadros jumbo
  - Prioridade Ethernet

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

Candidatos a volume espelhado

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

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

- O volume secundário deve ser pelo menos tão grande quanto o volume primário.
- Um volume pode participar de apenas um relacionamento de espelhamento.
- Para um par espelhado síncrono, os volumes primário e secundário devem ser volumes padrão. Eles não podem ser volumes finos ou volumes de instantâneo.
- Para espelhamento síncrono, há limites para o número de volumes suportados em um determinado array de storage. Certifique-se de que o número de volumes configurados em seu array de storage seja menor que o limite suportado. Quando o espelhamento síncrono está ativo, os dois volumes de capacidade reservada que são criados contam para o limite de volumes.
- Para espelhamento assíncrono, o volume primário e o volume secundário devem ter as mesmas capacidades de segurança de unidade.
  - Se o volume primário for compatível com FIPS, o volume secundário deve ser compatível com FIPS.
  - Se o volume primário for compatível com FDE, o volume secundário deve ser compatível com FDE.
  - Se o volume primário não estiver usando Drive Security, o volume secundário não deve estar usando Drive Security.
- Os volumes primário e secundário não devem ter Resource Partitioning ativado.

Capacidade reservada

Espelhamento assíncrono:

- É necessário um volume de capacidade reservada para um volume primário e para um volume secundário em um par espelhado para registrar informações de gravação para recuperação de reinicializações do controlador e outras interrupções temporárias.
- Como tanto o volume primário quanto o volume secundário em um par espelhado exigem capacidade reservada adicional, você deve garantir que haja capacidade livre disponível em ambos os storage arrays na relação de espelhamento.

Espelhamento síncrono:

- É necessária capacidade reservada para um volume primário e para um volume secundário para registrar informações de gravação para recuperar de reinicializações do controlador e outras interrupções temporárias.
- Os volumes de capacidade reservada são criados automaticamente quando o espelhamento síncrono é ativado. Como tanto o volume primário quanto o volume secundário em um par espelhado exigem capacidade reservada, você deve garantir que haja capacidade livre suficiente disponível em ambos os storage arrays que participam do relacionamento de espelhamento síncrono.

Recurso de segurança da unidade

- Se você estiver usando unidades com recursos de segurança, o volume primário e o volume secundário devem ter configurações de segurança compatíveis. Essa restrição não é aplicada; portanto, você deve verificá-la por conta própria.
- Se você estiver usando unidades com recursos de segurança, o volume primário e o volume secundário devem usar o mesmo tipo de unidade. Essa restrição não é obrigatória; portanto, você deve verificar por

conta própria.

- Se você estiver usando Data Assurance (DA), o volume primário e o volume secundário devem ter as mesmas configurações de DA.

Configurar espelhamento

Crie um par espelhado assíncrono no SANtricity Unified Manager

Para configurar 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 para o Unified Manager:

- O serviço Web Services Proxy deve estar em execução.
- Unified Manager deve estar sendo executado em seu host local por meio de uma conexão HTTPS.
- Unified Manager deve exibir certificados SSL válidos para o array de storage. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando Unified Manager e navegando até **Certificate › Certificate Management**.

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

- Cada array de storage deve ter dois controladores.
- Os dois arrays de storage devem ser detectados no Unified Manager.
- Cada controlador, tanto no array primário quanto no array secundário, deve ter uma porta de gerenciamento Ethernet configurada e deve estar conectado à sua rede.
- Os arrays de storage possuem uma versão mínima de firmware de 7.84. (Cada um deles pode executar diferentes versões de sistema operacional.)
- Você deve saber a senha dos arrays de storage local e remoto.
- Você precisa ter capacidade livre suficiente no array de storage remoto para criar um volume secundário igual ou maior que o volume primário que você deseja espelhar.
- Seus arrays de storage locais e remotos estão conectados por meio de uma estrutura Fibre Channel ou interface iSCSI.
- Você criou tanto o volume primário quanto o volume 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.

Etapa 1: crie ou selecione um grupo de consistência de espelhamento

Nesta etapa, você cria um novo grupo de consistência de espelhamento ou seleciona um existente. Um grupo de consistência de espelhamento é um contêiner 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 o array de storage local que você deseja usar como fonte.

2. Selecione o menu: Ações[Create Asynchronous Mirrored Pair].

   O assistente Criar Par Espelhado Assíncrono é aberto.

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

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

   Para criar um novo grupo, faça o seguinte:

   a. Selecione **A new mirror consistency group** e clique em **Avançar**.
   b. Insira um nome exclusivo que melhor descreva os dados nos volumes que serão espelhados entre os dois arrays de storage. Um nome pode conter apenas letras, números e os caracteres especiais sublinhado (_), hífen (-) e cerquilha (#). Um nome não pode exceder 30 caracteres e não pode conter espaços.
   c. Selecione o array de storage remoto no qual você deseja estabelecer uma relação de espelhamento com o array de storage local.

      Se o seu array de storage estiver protegido por senha, o sistema solicitará uma senha.

   d. Escolha se deseja sincronizar os pares espelhados manualmente ou automaticamente:
      - **Manual** — Selecione esta opção para iniciar manualmente a sincronização de todos os pares espelhados dentro deste grupo. Observe que, quando desejar realizar uma ressincronização posteriormente, você deve iniciar o System Manager para o array de storage primário, e então acessar **Storage › Asynchronous Mirroring**, selecionar o grupo na guia **Mirror Consistency Groups** e, em seguida, selecionar **More › Manually resynchronize**.
      - **Automático** — selecione o intervalo desejado em **Minutos**, **Horas** ou **Dias**, do início da atualização anterior até o início da próxima atualização. Por exemplo, se o intervalo de sincronização estiver definido em 30 minutos, e o processo de sincronização começar às 16:00, o próximo processo começará às 16:30.
   e. Selecione as configurações de alerta desejadas:
      - Para sincronizações manuais, especifique o limite (definido pela porcentagem da capacidade restante) para quando você receber alertas.
      - Para sincronizações automáticas, você pode configurar três métodos de alerta: quando a sincronização não for concluída dentro de um período específico, quando os dados do ponto de recuperação no array remoto forem mais antigos do que um limite de tempo específico e quando a capacidade reservada estiver próxima de um limite específico (definido pela porcentagem da capacidade restante).
4. Selecione **Próximo** e vá para Passo 2: selecione o volume primário.

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

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

Passo 2: selecione o volume primário

Nesta etapa, você seleciona o volume primário a ser usado no relacionamento de espelhamento e aloca sua capacidade reservada. Ao selecionar um volume primário no array de storage local, o sistema exibe uma lista de todos os volumes elegíveis para esse par espelhado. Quaisquer volumes que não sejam elegíveis para uso não são exibidos nessa lista.

Quaisquer volumes que você adicionar ao grupo de consistência de espelhamento no array de storage local terão a função principal na relação de espelhamento.

Passos

1. Na lista de volumes elegíveis, selecione um volume que deseja usar como volume primário e clique em **Next** para alocar a capacidade reservada.
2. Na lista de candidatos elegíveis, selecione a capacidade reservada para o volume primário.

   Mantenha as seguintes diretrizes em mente:

   - 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 primário e de quanto tempo você precisa manter a capacidade.
   - Em geral, escolha uma capacidade maior para a capacidade reservada se uma ou ambas as seguintes condições existirem:
     - Você pretende manter o par espelhado por um longo período de tempo.
     - Uma grande porcentagem dos blocos de dados será alterada no volume primário devido à intensa atividade de E/S. Utilize dados históricos de desempenho ou outros utilitários do sistema operacional para ajudar a determinar a atividade típica de E/S no volume primário.
3. Selecione **Próximo** e vá para Etapa 3: selecione o volume secundário.

Etapa 3: selecione o volume secundário

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

Quaisquer volumes que você adicionar ao grupo de consistência de espelhamento no array de storage remoto terão a função secundária na relação de espelhamento.

Passos

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

Mantenha as seguintes diretrizes em mente:

- 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 primário e de quanto tempo você precisa manter a capacidade.
- Em geral, escolha uma capacidade maior para a capacidade reservada se uma ou ambas as seguintes condições existirem:
  - Você pretende manter o par espelhado por um longo período de tempo.
  - Uma grande porcentagem dos blocos de dados será alterada no volume primário devido à intensa atividade de E/S. Utilize dados históricos de desempenho ou outros utilitários do sistema operacional para ajudar a determinar a atividade típica de E/S no volume primário.

3. Selecione **Concluir** para finalizar a sequência de espelhamento assíncrono.

Resultados

Unified Manager executa as seguintes ações:

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

Se o volume que está sendo espelhado for um volume fino, somente os blocos provisionados (capacidade alocada em vez da capacidade relatada) são transferidos para o volume secundário durante a sincronização inicial. Isso reduz a quantidade de dados que deve ser transferida para concluir a sincronização inicial.

Criar um par espelhado síncrono no SANtricity Unified Manager

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

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

Antes de começar

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

- O serviço Web Services Proxy deve estar em execução.
- Unified Manager deve estar sendo executado em seu host local por meio de uma conexão HTTPS.
- Unified Manager deve exibir certificados SSL válidos para o array de storage. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando Unified Manager e navegando até **Certificate › Certificate Management**.

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

- Os dois arrays de storage que você planeja usar para espelhamento são detectados no Unified Manager.
- Cada array de storage deve ter dois controladores.

- Cada controlador, tanto no array primário quanto no array secundário, deve ter uma porta de gerenciamento Ethernet configurada e deve estar conectado à sua rede.
- Os arrays de storage possuem uma versão mínima de firmware de 7.84. (Cada um deles pode executar diferentes versões de sistema operacional.)
- Você deve saber a senha dos arrays de storage local e remoto.
- Seus arrays de storage local e remoto estão conectados por meio de uma malha Fibre Channel.
- Você criou tanto o volume primário quanto o volume secundário que deseja usar na relação de espelhamento síncrono.
- O volume principal deve ser um volume padrão. Não pode ser um volume fino nem um volume instantâneo.
- O volume secundário deve ser um volume padrão. Não pode ser um volume fino nem um volume instantâneo.
- O volume secundário deve ser pelo menos tão grande quanto o volume primário.

Sobre esta tarefa

O processo para criar pares de espelhamento síncrono é um procedimento de várias etapas.

Etapa 1: selecione o volume primário

Nesta etapa, você seleciona o volume primário a ser usado na relação de espelhamento síncrono. Ao selecionar um volume primário no array de storage local, o sistema exibe uma lista de todos os volumes elegíveis para esse par espelhado. Volumes que não são elegíveis para uso não aparecem nessa lista. O volume que você selecionar desempenha a função primária na relação de espelhamento.

Passos

1. Na página **Gerenciar**, selecione o array de storage local que você deseja usar como fonte.
2. Selecione o menu: Ações [Create Synchronous Mirrored Pair].

   O assistente Criar Par Espelhado Síncrono é aberto.

3. Na lista de volumes elegíveis, selecione um volume que você deseja usar como volume primário no espelhamento.
4. Selecione **Próximo** e vá para Etapa 2: selecione o volume secundário.

Etapa 2: selecione o volume secundário

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

Passos

1. Selecione o array de storage remoto no qual você deseja estabelecer uma relação de espelhamento com o array de storage local.

   Se o seu array de storage estiver protegido por senha, o sistema solicitará uma senha.

   - Os arrays de storage são listados pelo nome do array de storage. Se você não tiver nomeado um array de storage, ele será listado como "unnamed".

- Se o array de storage 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 você deseja usar como volume secundário no espelhamento.

> Se um volume secundário for escolhido com uma capacidade maior do que a do volume primário, a capacidade utilizável ficará limitada ao tamanho do volume primário.

3. Clique em **Próximo** e vá para Etapa 3: selecione as configurações de sincronização.

Etapa 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 com que o controlador proprietário do volume primário resincroniza os dados com o volume secundário após uma interrupção de comunicação. Você também deve selecionar a política de resincronização, manual ou automática.

Passos

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

   A prioridade de sincronização determina quanto dos recursos do sistema são utilizados 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 quanto ao volume secundário. Você pode modificar a taxa no volume primário posteriormente, acessando o System Manager e selecionando **Storage › Synchronous Mirroring › More › Edit Settings**.

   Existem cinco taxas de prioridade de sincronização:

   - Mais baixo
   - Baixo
   - Médio
   - Alto
   - Mais alto

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

2. Escolha se deseja ressincronizar os pares espelhados no array de storage remotamente manualmente ou automaticamente.
   - **Manual** (opção recomendada) — Selecione esta opção para exigir que a sincronização seja retomada manualmente após a restauração da comunicação com um par espelhado. Esta opção oferece a melhor oportunidade para recuperação de dados.
   - **Automático** — selecione esta opção para iniciar a ressincronização automaticamente após a comunicação ser restaurada em um par espelhado.

     Para retomar a sincronização manualmente, acesse System Manager e selecione **Storage › Espelhamento Síncrono**, destaque o par espelhado na tabela e selecione **Retomar** em **Mais**.

3. Clique em **Concluir** para completar a sequência de espelhamento síncrono.

Resultados

Após a ativação do espelhamento, o sistema executa as seguintes ações:

- Inicia a sincronização inicial entre o array de storage local e o array de storage remoto.
- Define a prioridade de sincronização e a política de ressincronização.
- Reserva a porta de número mais alto do HIC do controlador para transmissão de dados de espelhamento.

  As solicitações de E/S recebidas nesta porta são aceitas somente do controlador remoto preferencial proprietário do volume secundário no par espelhado. (Reservas no volume primário são permitidas.)

- Cria dois volumes de capacidade reservada, 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 que você terminar

Acesse System Manager e selecione **Home › View Operations in Progress** para visualizar o progresso da operação de espelhamento síncrono. Essa operação pode ser demorada e pode afetar o desempenho do sistema.

Perguntas frequentes sobre espelhamento de armazenamento para SANtricity Unified Manager

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

O que preciso saber antes de criar um grupo de consistência de espelhamento?

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

Atenda aos seguintes requisitos para Unified Manager:

- O serviço Web Services Proxy deve estar em execução.
- Unified Manager deve estar sendo executado em seu host local por meio de uma conexão HTTPS.
- Unified Manager deve exibir certificados SSL válidos para o array de storage. Você pode aceitar um certificado autoassinado ou instalar seu próprio certificado de segurança usando Unified Manager e navegando até **Certificate › Certificate Management**.

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

- Os dois arrays de storage devem ser detectados no Unified Manager.
- Cada array de storage deve ter dois controladores.
- Cada controlador, tanto no array primário quanto no array secundário, deve ter uma porta de gerenciamento Ethernet configurada e deve estar conectado à sua rede.
- Os arrays de storage possuem uma versão mínima de firmware de 7.84. (Cada um deles pode executar diferentes versões de sistema operacional.)

- Você deve saber a senha dos arrays de storage local e remoto.
- Seus arrays de storage locais e remotos estão conectados por meio de uma estrutura Fibre Channel ou interface iSCSI.

> O espelhamento síncrono não está disponível no sistema de storage EF600/EF600C ou EF300/EF300C.

O que preciso saber antes de criar um par espelhado?

Antes de criar um par espelhado, siga estas orientações.

- Você precisa ter dois arrays de storage.
- Cada array de storage deve ter dois controladores.
- Os dois arrays de storage devem ser detectados no Unified Manager.
- Cada controlador, tanto no array primário quanto no array secundário, deve ter uma porta de gerenciamento Ethernet configurada e deve estar conectado à sua rede.
- Os arrays de storage possuem uma versão mínima de firmware de 7.84. (Cada um deles pode executar diferentes versões de sistema operacional.)
- Você deve saber a senha dos arrays de storage local e remoto.
- Você precisa ter capacidade livre suficiente no array de storage remoto para criar um volume secundário igual ou maior que o volume primário que você deseja espelhar.
- O espelhamento assíncrono é compatível com controladores que possuem portas de host Fibre Channel (FC) ou iSCSI, enquanto o espelhamento síncrono é compatível apenas com controladores que possuem portas de host FC.

> O espelhamento síncrono não está disponível no sistema de storage EF600/EF600C ou EF300/EF300C.

Por que eu alteraria essa porcentagem?

A capacidade reservada é normalmente de 20 por cento do volume base para operações de espelhamento assíncrono. Geralmente essa capacidade é suficiente.

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

- Se a vida útil da operação de serviço de cópia de um determinado objeto de storage for muito longa.
- Se uma grande porcentagem dos blocos de dados for alterada no volume base devido à intensa atividade de E/S. Utilize dados históricos de desempenho ou outros utilitários do sistema operacional para ajudar a determinar a atividade típica de E/S no volume base.

Por que vejo mais de um candidato para capacidade reservada?

Se houver mais de um volume em um pool ou grupo de volume que atenda à porcentagem de capacidade que você selecionou para o objeto de storage, então você verá vários candidatos.

Você pode atualizar a lista de candidatos recomendados alterando a porcentagem de espaço físico em disco que deseja reservar no volume base para operações de serviço de cópia. Os melhores candidatos são

exibidos com base na sua seleção.

Por que não vejo todos os meus volumes?

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

Os volumes que não são elegíveis para uso não são exibidos nessa lista. Volumes podem não ser elegíveis por qualquer um dos seguintes motivos:

- O volume não está otimizado.
- O volume já está participando de uma relação de espelhamento.
- Para espelhamento síncrono, os volumes primário e secundário em um par espelhado devem ser volumes padrão. Eles não podem ser volumes finos ou volumes de instantâneo.
- Para espelhamento assíncrono, os volumes finos 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 de bandeja, tamanho de 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 array de storage remoto?

Ao selecionar um volume secundário no array de storage remoto, uma lista mostra todos os volumes elegíveis para esse par espelhado.

Quaisquer volumes que não são elegíveis para uso não são exibidos nessa lista. Volumes podem não ser elegíveis por qualquer um dos seguintes motivos:

- O volume é um volume não padrão, como um volume snapshot.
- O volume não está otimizado.
- 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 você estiver usando Data Assurance (DA), o volume primário e o volume secundário devem ter as mesmas configurações de DA.
  - Se o volume principal estiver habilitado para DA, o volume secundário também deve estar habilitado para DA.
  - Se o volume principal não estiver habilitado para DA, o volume secundário não deve estar habilitado para DA.
- Para espelhamento assíncrono, o volume primário e o volume secundário devem ter as mesmas capacidades de segurança de unidade.
  - Se o volume primário for compatível com FIPS, o volume secundário deve ser compatível com FIPS.
  - Se o volume primário for compatível com FDE, o volume secundário deve ser compatível com FDE.
  - Se o volume primário não estiver usando Drive Security, o volume secundário não deve estar usando Drive Security.

Qual o impacto da prioridade de sincronização nas taxas de sincronização?

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

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

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

Estas taxas de prioridade estão disponíveis:

- Mais baixo
- Baixo
- Médio
- Alto
- Mais alto

A taxa de prioridade mais baixa oferece suporte ao desempenho do sistema, mas a ressincronização demora mais. A taxa de prioridade mais alta oferece suporte à ressincronização, mas o desempenho do sistema pode ser comprometido.

Essas diretrizes aproximam, de forma geral, as diferenças entre as prioridades.

Taxa de prioridade para sincronização completa	Tempo decorrido em comparação com a taxa de sincronização mais alta
Mais baixo	Aproximadamente oito vezes mais longo do que na taxa de prioridade mais alta.
Baixo	Aproximadamente seis vezes mais longo do que na taxa de prioridade mais alta.
Médio	Aproximadamente três vezes e meia mais longo do que na taxa de prioridade mais alta.
Alto	Aproximadamente duas vezes mais longo do que na taxa de prioridade mais alta.

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

Por que é recomendável usar uma política de sincronização manual?

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

Se você utiliza uma política de ressincronização automática e ocorrerem problemas intermitentes de

comunicação durante a ressincronização, os dados no volume secundário podem ser corrompidos temporariamente. Quando a ressincronização é concluída, os dados são corrigidos.

Certificados

Visão geral dos certificados

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

O que são certificados?

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

Saiba mais:

- "Como funcionam os certificados"
- "Terminologia de certificado"

Como faço para configurar os certificados?

Em Gerenciamento de Certificados, você pode configurar certificados para a estação de gerenciamento que hospeda Unified Manager e também importar certificados para os controladores nos arrays.

Saiba mais:

- "Use certificados assinados por CA para o sistema de gerenciamento"
- "Importar certificados para arrays"

Conceitos

Como funcionam os certificados no SANtricity Unified Manager

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 web sejam transmitidas de forma criptografada, privada e inalterada, somente entre o servidor e o cliente. Usando Unified Manager, você pode gerenciar certificados para o navegador em um sistema de gerenciamento de hosts e para os controladores nos arrays de storage descobertos.

Um certificado pode ser assinado por uma autoridade confiável ou pode ser autoassinado. "Assinar" significa simplesmente que alguém validou a identidade do proprietário e determinou que seus dispositivos podem ser confiáveis. Os arrays de storage são fornecidos com um certificado autoassinado gerado automaticamente em cada controlador. Você pode continuar a usar os certificados autoassinados ou pode obter certificados assinados por CA para uma conexão mais segura entre os controladores e os sistemas host.

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

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

Ao abrir um navegador e digitar um endereço da web, seu sistema realiza um processo de verificação de certificado em segundo plano para determinar se você está se conectando a um site que inclui um certificado válido, assinado por uma CA. Geralmente, um site protegido com um certificado assinado inclui um ícone de cadeado e uma designação https no endereço. Se você tentar se conectar a um site que não contenha um certificado assinado por uma CA, seu navegador exibirá um aviso de que o site não é seguro.

A Autoridade Certificadora (CA) toma medidas para verificar sua identidade durante o processo de solicitação. Ela pode enviar um e-mail para o endereço comercial registrado da sua empresa, verificar o endereço comercial e realizar uma verificação HTTP ou DNS. Quando o processo de solicitação estiver concluído, a CA envia arquivos digitais para você carregar em um sistema de gerenciamento de host. Normalmente, esses arquivos incluem uma cadeia de confiança, conforme a seguir:

- **Raiz** — No topo da hierarquia está o certificado raiz, que contém uma chave privada usada para assinar outros certificados. A raiz identifica uma organização CA específica. Se você usar a mesma CA para todos os seus dispositivos de rede, precisará apenas de um certificado raiz.
- **Intermediário** — Ramificando-se a partir da raiz estão os certificados intermediários. A CA emite um ou mais certificados intermediários para atuarem como intermediários entre uma raiz protegida e os certificados do servidor.
- **Servidor** — Na base da cadeia está o certificado do servidor, que identifica sua entidade específica, como um site ou outro dispositivo. Cada controlador em um array de storage requer um certificado de servidor separado.

Certificados autoassinados

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

Os certificados autoassinados não são "trusted" pelos navegadores. Cada vez que você tenta se conectar a um site que contém apenas um certificado autoassinado, o navegador exibe uma mensagem de aviso. Você deve clicar em um link na mensagem de aviso que permite prosseguir para o site; ao fazer isso, você está essencialmente aceitando o certificado autoassinado.

Certificados 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 ao verificar a presença de um certificado digital. Se o navegador não localizar um certificado assinado por uma CA para o servidor, ele abre 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 por uma CA para não ver mais a mensagem de aviso.

Certificados para controladores

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

Saiba mais sobre a terminologia de certificados no SANtricity Unified Manager

Os seguintes termos aplicam-se ao gerenciamento de certificados.

Termo	Descrição
CA	Uma autoridade certificadora (CA) é uma entidade confiável que emite documentos eletrônicos, chamados certificados digitais, para segurança na Internet. Esses certificados identificam os proprietários de sites, permitindo conexões seguras entre clientes e servidores.
CSR	Uma solicitação de assinatura de certificado (CSR, na sigla em inglês) é uma mensagem enviada por um solicitante a uma autoridade certificadora (CA, na sigla em inglês). A CSR valida as informações que a CA exige para emitir um certificado.
Certificado	Um certificado identifica o proprietário de um site para fins de segurança, o que impede que invasores se façam passar pelo site. O certificado contém informações sobre o proprietário do site e a identidade da entidade confiável que certifica (assina) essas informações.
Cadeia de certificados	Uma hierarquia de arquivos que adiciona uma camada de segurança aos certificados. Normalmente, a cadeia inclui um certificado raiz no topo da hierarquia, um ou mais certificados intermediários e os certificados de servidor que identificam as entidades.
Certificado intermediário	Um ou mais certificados intermediários ramificam-se a partir da raiz na cadeia de certificados. A CA emite um ou mais certificados intermediários para atuarem como intermediários entre uma raiz protegida e os certificados do servidor.
Keystore	Um keystore é um repositório no seu sistema de gerenciamento de hosts que contém chaves privadas, juntamente com suas respectivas chaves públicas e certificados. Essas chaves e certificados identificam suas próprias entidades, como os controladores.
Certificado raiz	O certificado raiz está no topo da hierarquia na cadeia de certificados e contém uma chave privada usada para assinar outros certificados. A raiz identifica uma organização CA específica. Se você usar a mesma CA para todos os seus dispositivos de rede, precisará de apenas um certificado raiz.

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

Use certificados assinados por CA para o sistema de gerenciamento

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

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.

Sobre esta tarefa

Utilizar certificados assinados por uma CA é um procedimento de três etapas.

Etapa 1: preencha um arquivo CSR

Primeiro, você deve gerar um arquivo de solicitação de assinatura de certificado (CSR), que identifica sua organização e o sistema host onde o Web Services Proxy e Unified Manager estão instalados.

> Alternativamente, você pode gerar um arquivo CSR usando uma ferramenta como OpenSSL e pular para Etapa 2: enviar o arquivo CSR.

Passos

1. Selecione **Certificate Management**.

2. Na guia Management, selecione **Complete CSR**.
3. Insira as seguintes informações e clique em **Avançar**:
   - **Organização** — O nome completo e legal da sua empresa ou organização. Inclua sufixos, como Inc. ou Corp.
   - **Unidade organizacional (opcional)** — A divisão da sua organização que está lidando com o certificado.
   - **Cidade/Localidade** — a cidade onde seu sistema host ou empresa está localizado.
   - **Estado/Região (opcional)** — O estado ou região onde seu sistema host ou empresa está localizado.
   - **Código ISO do país** — O código ISO (Organização Internacional de Normalização) de dois dígitos do seu país, como US.
4. Insira as seguintes informações sobre o sistema host onde o Web Services Proxy está instalado:
   - **Nome comum** — O endereço IP ou o nome DNS do sistema host onde o Web Services Proxy está instalado. Certifique-se de que este endereço esteja correto; ele deve corresponder exatamente ao que você digita para acessar Unified Manager no navegador. Não inclua http:// ou https://. O nome DNS não pode começar com um caractere curinga.
   - **Endereços IP alternativos** — Se o nome comum for um endereço IP, você pode, opcionalmente, inserir quaisquer endereços IP ou aliases adicionais para o sistema host. Para várias entradas, use o formato separado por vírgulas.
   - **Nomes DNS alternativos** — Se o nome comum for um nome DNS, insira quaisquer nomes DNS adicionais para o sistema host. Para múltiplas entradas, use o formato separado por vírgulas. Se não houver nomes DNS alternativos, mas você tiver inserido um nome DNS no primeiro campo, copie esse nome aqui. O nome DNS não pode começar com um caractere curinga.
5. Certifique-se de que as informações do host estejam corretas. Se não estiverem, os certificados retornados pela CA falharão quando você tentar importá-los.
6. Clique em **Concluir**.
7. Vá para Etapa 2: enviar o arquivo CSR.

Etapa 2: enviar o arquivo CSR

Após criar um arquivo de solicitação de assinatura de certificado (CSR), você o envia para uma Certificate Authority (CA) para receber certificados de gerenciamento assinados para o sistema que hospeda Unified Manager e o Web Services Proxy.

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 arquivo CSR baixado.

   A localização da pasta do download depende do seu navegador.

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

Após enviar um arquivo CSR para a CA, NÃO gere outro arquivo CSR. Sempre que você gera um CSR, o sistema cria um par de chaves privada e pública. A chave pública faz parte do CSR, enquanto a chave privada é mantida no keystore do sistema. Quando você recebe os certificados assinados e os importa, o sistema garante que tanto a chave privada quanto a pública sejam o par original. Se as chaves não corresponderem, os certificados assinados não funcionarão e você deve solicitar novos certificados à CA.

3. Quando a CA retornar os certificados assinados, vá para Etapa 3: importar certificados de management.

Etapa 3: importar certificados de management

Após receber os certificados assinados da Autoridade Certificadora (CA), importe os certificados no sistema host onde o Web Services Proxy e a interface 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 em cadeia (por exemplo, um arquivo .p7b), você deve descompactar o arquivo em cadeia em arquivos individuais: o certificado raiz, um ou mais certificados intermediários e o certificado do servidor. Você pode usar o utilitário do Windows `certmgr` para descompactar os arquivos (clique com o botão direito e selecione **All Tasks › Export**). A codificação Base-64 é recomendada. Quando as exportações forem concluídas, um arquivo CER será exibido para cada arquivo de certificado na cadeia.
- Você copiou os arquivos de certificado para o sistema host onde o Web Services Proxy está em execução.

Passos

1. Selecione **Certificate Management**.
2. Na aba Management, selecione **Import**.

   Uma caixa de diálogo é aberta para importar os arquivos 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 criado juntamente com o CSR.

   Os nomes dos arquivos 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 de Certificate Management.

Redefinir certificados de gerenciamento

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

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.

Sobre esta tarefa

Esta tarefa exclui o certificado de gerenciamento atual do sistema host onde o Web Services Proxy e Unified Manager estão instalados. Após a redefinição do certificado, o sistema host volta a usar o certificado autoassinado.

Passos

1. Selecione **Settings > Certificates**.
2. Selecione a aba **Gerenciamento de Array** e, em seguida, selecione **Redefinir**.

   Uma caixa de diálogo Confirm Reset Management Certificate é aberta.

3. Digite `reset` no campo e clique em **Redefinir**.

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

Resultados

O sistema volta a usar o certificado autoassinado do servidor. Como resultado, o sistema solicita que os usuários aceitem manualmente o certificado autoassinado para suas sessões.

Use certificados de array

Importar certificados para arrays em SANtricity Unified Manager

Caso necessário, você pode importar certificados para os arrays de storage para que eles possam se autenticar com o sistema que hospeda SANtricity Unified Manager. Os certificados podem ser assinados por uma autoridade certificadora (CA) ou podem ser autoassinados.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.
- Se você estiver importando certificados confiáveis, os certificados deverão ser importados para os controladores do array de storage usando System Manager.

Passos

1. Selecione **Certificate Management**.
2. Selecione a guia **Trusted**.

   Esta página exibe todos os certificados relatados para os arrays de storage.

3. Selecione **Import › Certificados** para importar um certificado de CA ou **Import › Self-signed storage array certificates** para importar um certificado autoassinado.

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

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

O certificado é carregado e validado.

Excluir certificados confiáveis no SANtricity Unified Manager

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.

> Tenha em mente que a exclusão de um certificado raiz ou intermediário pode afetar vários arrays de storage, já que esses arrays podem compartilhar os mesmos arquivos de certificado.

Passos

1. Selecione **Certificate Management**.
2. Selecione a guia **Trusted**.
3. Selecione um ou mais certificados na tabela e clique em **Delete**.

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

   A caixa de diálogo Confirmar Exclusão de Certificado Confiável é aberta.

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

   O certificado é removido da tabela.

Resolver certificados não confiáveis

Certificados não confiáveis ocorrem quando um array de storage tenta estabelecer uma conexão segura com SANtricity Unified Manager, mas a conexão falha ao ser confirmada como segura.

Na página de Certificado, você pode resolver certificados não confiáveis importando um certificado autoassinado do array de storage ou importando um certificado de autoridade certificadora (CA) emitido por uma terceira parte confiável.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security Admin.
- Se você planeja importar um certificado assinado por uma autoridade certificadora (CA):
  - Você gerou uma solicitação de assinatura de certificado (arquivo .CSR) para cada controlador no array de storage e a enviou para a CA.
  - A CA retornou arquivos de certificado confiáveis.
  - Os arquivos de certificado estão disponíveis no seu sistema local.

Sobre esta tarefa

Você pode precisar instalar certificados de CA confiáveis adicionais se alguma das seguintes condições for verdadeira:

- Você adicionou recentemente um array de storage.
- Um ou ambos os certificados expiraram.
- Um ou ambos os certificados estão revogados.
- Um ou ambos os certificados estão sem um certificado raiz ou intermediário.

Passos

1. Selecione **Certificate Management**.
2. Selecione a guia **Trusted**.

   Esta página exibe todos os certificados relatados para os arrays de storage.

3. Selecione **Import › Certificados** para importar um certificado de CA ou **Import › Self-Signed storage array certificates** para importar um certificado autoassinado.

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

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

   O certificado é carregado e validado.

Gerenciar certificados

Ver certificados

Você pode visualizar informações resumidas de um certificado, que incluem a organização que utiliza o certificado, a autoridade que emitiu o certificado, o período de validade e as impressões digitais (identificadores únicos).

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de certificado não aparecem.

Passos

1. Selecione **Certificate Management**.
2. Selecione uma das seguintes abas:
   - **Gerenciamento** — Exibe o certificado do sistema que hospeda o Web Services Proxy. Um certificado de gerenciamento pode ser autoassinado ou aprovado por uma autoridade certificadora (CA). Ele permite acesso seguro ao Unified Manager.
   - **Confiável** — Mostra os certificados que Unified Manager pode acessar para arrays de storage e outros servidores remotos, como um servidor LDAP. Os certificados podem ser emitidos por uma autoridade certificadora (CA) ou podem ser autoassinados.
3. Para ver mais informações sobre um certificado, selecione a linha correspondente, selecione as reticências no final da linha e clique em **View** ou **Export**.

Exportar certificados no SANtricity Unified Manager

Você pode exportar um certificado para visualizar seus detalhes completos.

Antes de começar

Para abrir o arquivo exportado, você deve ter um aplicativo visualizador de certificados.

Passos

1. Selecione **Certificate Management**.
2. Selecione uma das seguintes abas:
   - **Gerenciamento** — Exibe o certificado do sistema que hospeda o Web Services Proxy. Um certificado de gerenciamento pode ser autoassinado ou aprovado por uma autoridade certificadora (CA). Ele permite acesso seguro ao Unified Manager.
   - **Confiável** — Mostra os certificados que Unified Manager pode acessar para arrays de storage e outros servidores remotos, como um servidor LDAP. Os certificados podem ser emitidos por uma autoridade certificadora (CA) ou podem ser autoassinados.
3. Selecione um certificado na página e, em seguida, clique nas reticências no final da linha.
4. Clique em **Exportar** e, em seguida, salve o arquivo de certificado.
5. Abra o arquivo no seu aplicativo visualizador de certificados.

Gerenciamento de acesso

Saiba mais sobre o gerenciamento de acesso do SANtricity Unified Manager

O Gerenciamento de Acesso é um método de configurar autenticação no SANtricity Unified Manager.

Quais métodos de autenticação estão disponíveis?

Os seguintes métodos de autenticação estão disponíveis:

- **Funções de usuário locais** — A autenticação é gerenciada por meio de recursos de RBAC (controle de acesso baseado em funções). As funções de usuário locais incluem perfis de usuário predefinidos e funções com permissões de acesso específicas.
- **Serviços de diretório** — A autenticação é gerenciada por meio de um servidor LDAP (Lightweight Directory Access Protocol) e um serviço de diretório, como o Microsoft Active Directory.
- **SAML** — A autenticação é gerenciada por meio de um Identity Provider (IdP) usando SAML 2.0.

Saiba mais:

- "Como funciona o gerenciamento de acessos"
- "Terminologia de gerenciamento de acesso"
- "Permissões para funções mapeadas"
- "SAML"

Como faço para configurar o Access Management?

O software SANtricity vem pré-configurado para usar funções de usuário locais. Se você quiser usar LDAP, pode configurá-lo na página Access Management.

Saiba mais:

- "Gerenciamento de acesso com funções de usuário locais"
- "Gerenciamento de acesso com serviços de diretório"
- "Configurar SAML"

Conceitos

Como funciona o gerenciamento de acesso no SANtricity Unified Manager

Utilize o Access Management para estabelecer autenticação de usuário no SANtricity Unified Manager.

Fluxo de trabalho de configuração

A configuração do Access Management funciona da seguinte maneira:

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

   > No primeiro acesso, o nome de usuário `admin` é exibido automaticamente e não pode ser alterado. O `admin` usuário tem acesso total a todas as funções do sistema. A senha deve ser definida no primeiro acesso.

2. O administrador navega até Gerenciamento de Acesso na interface de usuário, que inclui funções de usuário locais pré-configuradas. Essas funções são uma implementação das capacidades de controle de acesso baseado em funções (RBAC).
3. O administrador configura um ou mais dos seguintes métodos de autenticação:
   - **Funções de usuário locais** — A autenticação é gerenciada por meio de recursos de RBAC. As funções de usuário locais incluem usuários e funções predefinidos com permissões de acesso específicas. Os administradores podem usar essas funções de usuário locais como o único método de autenticação ou em combinação com um serviço de diretório. Nenhuma configuração é necessária, além da definição de senhas para os usuários.
   - **Serviços de diretório** — A autenticação é gerenciada por meio de um servidor LDAP (Lightweight Directory Access Protocol) e um serviço de diretório, como o Active Directory da Microsoft. Um administrador se conecta ao servidor LDAP e então mapeia os usuários LDAP para as funções de usuário locais.
   - **SAML** — A autenticação é gerenciada por meio de um Provedor de Identidade (IdP) usando a Security Assertion Markup Language (SAML) 2.0. Um administrador estabelece comunicação entre o sistema IdP e o array de storage e, em seguida, mapeia os usuários do IdP para as funções de usuário locais incorporadas no array de storage.
4. O administrador fornece aos usuários as credenciais de login para Unified Manager.
5. Os usuários acessam o sistema inserindo suas credenciais. Durante o login, o sistema executa as seguintes tarefas em segundo plano:
   - Autentica o nome de usuário e a senha na conta do usuário.
   - Determina as permissões do usuário com base nas funções atribuídas.
   - Fornece ao usuário acesso às funções na interface de usuário.
   - Exibe o nome do usuário no banner superior.

Funções disponíveis no Unified Manager

O acesso às funções depende das funções atribuídas ao usuário, que incluem o seguinte:

- **Administrador de armazenamento** — acesso completo de leitura/gravação aos objetos de armazenamento nos arrays, mas sem acesso à configuração de segurança.
- **Administrador de segurança** — Acesso à configuração de segurança em Access Management e Certificate Management.
- **Administrador de suporte** — Acesso a todos os recursos de hardware em arrays de storage, dados de falhas e eventos MEL. Sem acesso a objetos de storage ou à configuração de segurança.
- **Monitor** — Acesso somente leitura a todos os objetos de storage, mas sem acesso à configuração de segurança.

Uma função indisponível aparece acinzentada ou não é exibida na interface de usuário.

Saiba mais sobre a terminologia de gerenciamento de acesso do SANtricity Unified Manager

Saiba como os termos de Access Management se aplicam ao SANtricity Unified Manager.

Termo	Descrição
Active Directory	Active Directory (AD) é um serviço de diretório da Microsoft que utiliza LDAP para redes de domínio Windows.
Vinculação	As operações de bind são usadas para autenticar clientes no servidor de diretório. Bind geralmente requer credenciais de conta e senha, mas alguns servidores permitem operações de bind anônimas.
CA	Uma autoridade certificadora (CA) é uma entidade confiável que emite documentos eletrônicos, chamados certificados digitais, para segurança na Internet. Esses certificados identificam os proprietários de sites, permitindo conexões seguras entre clientes e servidores.
Certificado	Um certificado identifica o proprietário de um site para fins de segurança, o que impede que invasores se façam passar pelo site. O certificado contém informações sobre o proprietário do site e a identidade da entidade confiável que certifica (assina) essas informações.
LDAP	O Lightweight Directory Access Protocol (LDAP) é um protocolo de aplicação para acessar e manter serviços de informações de diretório distribuídos. Este protocolo permite que diversas aplicações e serviços se conectem ao servidor LDAP para validar usuários.
RBAC	O controle de acesso baseado em funções (RBAC) é um método de regular o acesso a recursos de computador ou de rede com base nas funções dos usuários individuais. Unified Manager inclui funções predefinidas.

Termo	Descrição
SAML	A Linguagem de Marcação de Asserção de Segurança (SAML) é um padrão baseado em XML para autenticação e autorização entre duas entidades. O SAML permite autenticação multifator, na qual os usuários devem fornecer dois ou mais itens para comprovar sua identidade (por exemplo, uma senha e impressão digital). O recurso SAML incorporado do array de storage é compatível com SAML2.0 para declaração de identidade, autenticação e autorização.
SSO	Single sign-on (SSO) é um serviço de autenticação que permite que um único conjunto de credenciais de login acesse vários aplicativos.
Proxy de Serviços Web	O Proxy de Serviços Web, que fornece acesso por meio de mecanismos HTTPS padrão, permite que os administradores configurem serviços de gerenciamento para arrays de storage. O proxy pode ser instalado em hosts Windows ou Linux. A interface Unified Manager está disponível com o Proxy de Serviços Web.

Permissões para funções mapeadas

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

As funções conferem ao usuário acesso às tarefas, conforme a seguir:

- **Administrador de armazenamento** — acesso completo de leitura/gravação aos objetos de armazenamento nos arrays, mas sem acesso à configuração de segurança.
- **Administrador de segurança** — Acesso à configuração de segurança em Access Management e Certificate Management.
- **Administrador de suporte** — Acesso a todos os recursos de hardware em arrays de storage, dados de falhas e eventos MEL. Sem acesso a objetos de storage ou à configuração de segurança.
- **Monitor** — Acesso somente leitura a todos os objetos de storage, mas sem acesso à configuração de segurança.

Se um usuário não tiver permissões para uma determinada função, essa função ficará indisponível para seleção ou não será exibida na interface de usuário.

Gerenciamento de acesso com funções de usuário locais em SANtricity Unified Manager

Os administradores podem usar os recursos de RBAC (controle de acesso baseado em funções) implementados no SANtricity Unified Manager. Esses recursos são chamados de "local user roles".

Fluxo de trabalho de configuração

As funções de usuário locais são pré-configuradas no sistema. Para usar funções de usuário locais 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 Security admin.

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

2. Um administrador analisa os perfis de usuário, que são predefinidos e não podem ser modificados.
3. Opcionalmente, o administrador atribui novas senhas para cada perfil de usuário.
4. Os usuários acessam o sistema com as credenciais que lhes foram atribuídas.

Gerenciamento

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

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

Gerenciamento de acesso com serviços de diretório no SANtricity Unified Manager

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

Fluxo de trabalho de configuração

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

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

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

2. O administrador insere as configurações do servidor LDAP. As configurações incluem o nome de domínio, a URL e as informações da conta Bind.
3. Se o servidor LDAP usar um protocolo seguro (LDAPS), o administrador carrega uma cadeia de certificados da autoridade certificadora (CA) para autenticação entre o servidor LDAP e o sistema host onde o Proxy de Serviços Web está instalado.
4. Após a conexão com o servidor ser estabelecida, o administrador mapeia os grupos de usuários para as funções de usuário locais. Essas funções são predefinidas e não podem ser modificadas.
5. O administrador testa a conexão entre o servidor LDAP e o Web Services Proxy.
6. Os usuários acessam o sistema com suas credenciais LDAP/Directory Services atribuídas.

Gerenciamento

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

- Adicionar um servidor de diretório.
- Editar configurações do servidor de diretório.
- Mapear usuários LDAP para funções de usuário locais.

- Remova um servidor de diretório.
- Alterar senhas.
- Defina um comprimento mínimo para senhas.
- Permitir que os usuários façam login sem senha.

Gerenciamento de acesso com SAML no SANtricity Unified Manager

Para o gerenciamento de acesso, os administradores podem usar os recursos do Security Assertion Markup Language (SAML) 2.0 incorporados no array.

Fluxo de trabalho de configuração

A configuração SAML funciona da seguinte forma:

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

   > O `admin` usuário tem acesso total a todas as funções no System Manager.

2. O administrador vai para a guia **SAML** em Gerenciamento de Acesso.
3. Um administrador configura a comunicação com o Identity Provider (IdP). Um IdP é um sistema externo usado para solicitar credenciais de um usuário e determinar se o usuário foi autenticado com sucesso. Para configurar a comunicação com o array de storage, o administrador baixa o arquivo de metadados do IdP do sistema IdP e, em seguida, usa Unified Manager para carregar o arquivo no array de storage.
4. Um administrador estabelece uma relação de confiança entre o Service Provider e o IdP. Um Service Provider controla a autorização do usuário; neste caso, o controlador no array de storage atua como o Service Provider. Para configurar as comunicações, o administrador usa Unified Manager para exportar um arquivo de metadados do Service Provider para o controlador. A partir do sistema IdP, o administrador então importa o arquivo de metadados para o IdP.

   > Os administradores também devem garantir que o IdP suporte a capacidade de retornar um Name ID na autenticação.

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

   > Uma vez que o SAML esteja ativado, você *não* pode desativá-lo através da interface de usuário, nem editar as configurações do IdP. Se precisar desativar ou editar a configuração do SAML, entre em contato com o Technical Support para obter assistência.

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

Gerenciamento

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

- Modificar ou criar novo mapeamento de funções
- Exportar arquivos do provedor de serviços

Restrições de acesso

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

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

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

Use funções de usuário locais

Exibir funções de usuário locais

Na guia Funções de Usuário Local, você pode visualizar o mapeamento dos usuários para as funções padrão. Esses mapeamentos fazem parte do RBAC (controle de acesso baseado em funções) aplicado no Web Services Proxy para SANtricity Unified Manager.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.

Sobre esta tarefa

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

Passos

1. Selecione **Access Management**.
2. Selecione a guia **Funções de usuário local**.

   Os usuários são apresentados na tabela:

   - **admin** — Superadministrador com acesso a todas as funções do sistema. Este usuário inclui todas as funções.
   - **storage** — O administrador responsável por todo provisionamento de storage. Este usuário inclui as seguintes funções: Storage Admin, Support Admin e Monitor.
   - **security** — O usuário responsável pela configuração de segurança, incluindo Access Management e Certificate Management. Este usuário inclui as seguintes funções: Security Admin e Monitor.
   - **support** — O usuário responsável pelos recursos de hardware, dados de falhas e upgrades de firmware. Este usuário inclui as seguintes funções: Support Admin e Monitor.
   - **monitor** — Um usuário com acesso somente leitura ao sistema. Este usuário inclui apenas a função Monitor.

- **rw** (leitura/gravação) — Este usuário inclui as seguintes funções: Storage Admin, Support Admin e Monitor.
- **ro** (somente leitura) — Este usuário inclui apenas a função Monitor.

Alterar senhas para perfis de usuário locais no SANtricity Unified Manager

Você pode alterar as senhas de usuário para cada usuário em Access Management.

Antes de começar

- Você deve estar conectado como administrador local, o que inclui permissões de Root admin.
- Você deve saber a senha do administrador local.

Sobre esta tarefa

Mantenha estas diretrizes em mente ao escolher uma senha:

- Quaisquer novas senhas de usuários locais devem atender ou exceder a configuração atual para senha mínima (em Exibir/Editar Configurações).
- As senhas diferenciam maiúsculas de minúsculas.
- Os espaços em branco no final das senhas não são removidos durante a sua criação. Certifique-se de incluir os espaços caso eles estejam presentes na senha.
- Para maior segurança, use pelo menos 15 caracteres alfanuméricos e altere a senha com frequência.

Passos

1. Selecione **Access Management**.
2. Selecione a guia **Funções de usuário local**.
3. Selecione um usuário da tabela.

   O botão Alterar Senha se torna disponível.

4. Selecione **Change Password**.

   A caixa de diálogo Alterar Senha é aberta.

5. Se não houver um comprimento mínimo de senha definido para senhas de usuários locais, você pode selecionar a caixa de seleção para exigir que o usuário insira uma senha para acessar o sistema.
6. Insira a nova senha para o usuário selecionado nos dois campos.
7. Digite sua senha de administrador local para confirmar esta operação e clique em **Alterar**.

Resultados

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

Alterar as configurações de senha do usuário local em SANtricity Unified Manager

Você pode definir o comprimento mínimo exigido para todas as novas senhas de usuários locais ou senhas de usuários locais atualizadas. Você também pode permitir que usuários locais acessem o sistema sem digitar uma senha.

Antes de começar

Você deve estar conectado como administrador local, o que inclui permissões de Root admin.

Sobre esta tarefa

Mantenha estas diretrizes em mente ao definir o comprimento mínimo para senhas de usuários locais:

- As alterações de configuração não afetam as senhas de usuários locais existentes.
- A configuração de comprimento mínimo exigido para senhas de usuários locais deve estar entre 0 e 30 caracteres.
- Quaisquer novas senhas de usuários locais devem atender ou exceder a configuração atual de comprimento mínimo.
- Não defina um comprimento mínimo para a senha se desejar que os usuários locais acessem o sistema sem inserir uma senha.

Passos

1. Selecione **Access Management**.
2. Selecione a guia **Funções de usuário local**.
3. Selecione **Visualizar/Editar Settings**.

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

4. Faça uma das seguintes ações:
   - Para permitir que os usuários locais acessem o sistema *sem* inserir uma senha, desmarque a caixa de seleção "Exigir que todas as senhas de usuários locais tenham pelo menos".
   - Para definir um comprimento mínimo de senha para todas as senhas de usuários locais, selecione a caixa de seleção "Exigir que todas as senhas de usuários locais tenham pelo menos" e então use a caixa de rotação para definir o comprimento mínimo exigido para todas as senhas de usuários locais.

     Quaisquer novas senhas de usuários locais devem atender ou exceder a configuração atual.

5. Clique em **Salvar**.

Use os serviços de diretório

Adicionar servidor de diretório em SANtricity Unified Manager

Para configurar autenticação para o Access Management, você estabelece a comunicação entre um servidor LDAP e o host que executa o Web Services Proxy para SANtricity Unified Manager. Em seguida, você mapeia os grupos de usuários LDAP para as funções de usuário locais.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- Os grupos de usuários devem ser definidos no seu serviço de diretório.
- As credenciais do servidor LDAP devem estar disponíveis, incluindo o nome de domínio, o URL do servidor e, opcionalmente, o nome de usuário e a senha da conta de vinculação.
- Para servidores LDAPS que utilizam um protocolo seguro, a cadeia de certificados do servidor LDAP deve estar instalada em sua máquina local.

Sobre esta tarefa

Adicionar um servidor de diretório é um processo de duas etapas. Primeiro você insere o nome de domínio e o URL. Se o seu servidor usa um protocolo seguro, você também deve carregar um certificado de CA para autenticação se ele for assinado por uma autoridade de assinatura não padrão. Se você tiver credenciais para uma conta de bind, também pode inserir o nome de usuário e a senha da sua conta. Em seguida, você mapeia os grupos de usuários do servidor LDAP para as funções de usuário locais.

Passos

1. Selecione **Access Management**.
2. Na guia **Directory Services**, selecione **Add Directory Server**.

   A caixa de diálogo Adicionar Servidor de Diretório é aberta.

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

Detalhes do campo

Configuração	Descrição
Configurações de configuração	Domínio(s)
Insira o nome de domínio do servidor LDAP. Para vários domínios, insira os nomes de domínio em uma lista separada por vírgulas. O nome de domínio é usado no login (*username* @*domain*) para especificar em qual servidor de diretório autenticar.	URL do servidor
Insira a URL para acessar o servidor LDAP no formato `ldap[s]://**host:***port*`.	Fazer upload do certificado (opcional)
Este campo aparece somente se um protocolo LDAPS for especificado no campo Server URL acima. Clique em **Procurar** e selecione um certificado de CA para carregar. Este é o certificado confiável ou cadeia de certificados usado para autenticação do servidor LDAP.	Vincular conta (opcional)

Configuração	Descrição
Insira uma conta de usuário somente leitura para consultas de pesquisa no servidor LDAP e para pesquisas dentro dos grupos. Insira o nome da conta em um formato do tipo LDAP. Por exemplo, se o usuário de vinculação for chamado "bindacct", então você pode inserir um valor como `CN=bindacct,CN=Users,DC=cpoc,DC=local`.	Senha de bind (opcional)
Este campo aparece quando você insere uma conta de associação. Digite a senha para a conta de bind.	Testar a conexão do servidor antes de adicionar

Configuração	Descrição
Selecione esta caixa de seleção se quiser garantir que o sistema possa se comunicar com a configuração do servidor LDAP que você inseriu. O teste ocorre depois que você clica em **Adicionar** na parte inferior da caixa de diálogo. Se esta caixa de seleção estiver marcada e o teste falhar, a configuração não será adicionada. Você deve resolver o erro ou desmarcar a caixa de seleção para ignorar o teste e adicionar a configuração.	**Configurações de privilégios**
DN base de pesquisa	Insira o contexto LDAP para pesquisar usuários, normalmente no formato de `CN=Users, DC=cpoc, DC=local`.
Atributo de nome de usuário	Insira o atributo que está vinculado ao ID do usuário para autenticação. Por exemplo: `sAMAccountName`.
Atributo(s) do grupo	Insira uma lista de atributos de grupo do usuário, que é usada para o mapeamento de grupo para função. Por exemplo: `memberOf, managedObjects`.

4. Clique na guia **Mapeamento de funções**.
5. Atribua grupos LDAP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

Detalhes do campo

Configuração	Descrição
Mapeamentos	Nome diferenciado do grupo
Especifique o nome diferenciado (DN) do grupo para o grupo de usuários LDAP a ser mapeado. Expressões regulares são suportadas. Esses caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular: \.[]{}()<>*+-=!?^$	
Funções	Clique no campo e selecione uma das funções de usuário local a serem mapeadas para o DN do grupo. Você deve selecionar individualmente cada função que deseja incluir para este grupo. A função Monitor é necessária em combinação com as outras funções para fazer login no SANtricity Unified Manager. As funções mapeadas incluem as seguintes permissões: • **Administrador de armazenamento** — acesso completo de leitura/gravação aos objetos de armazenamento nos arrays, mas sem acesso à configuração de segurança. • **Administrador de segurança** — Acesso à configuração de segurança em Access Management e Certificate Management. • **Administrador de suporte** — Acesso a todos os recursos de hardware em arrays de storage, dados de falhas e eventos MEL. Sem acesso a objetos de storage ou à configuração de segurança. • **Monitor** — Acesso somente leitura a todos os objetos de storage, mas sem acesso à configuração de segurança.

A função Monitor é obrigatória 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 **Adicionar**.

   O sistema realiza uma validação, garantindo que o array de storage e o servidor LDAP possam se comunicar. Se uma mensagem de erro aparecer, verifique as credenciais inseridas na caixa de diálogo e

insira as informações novamente, se necessário.

Edite as configurações do servidor de diretório e os mapeamentos de funções em SANtricity Unified Manager

Se você já configurou um servidor de diretório no Access Management, pode alterar suas configurações a qualquer momento. As configurações incluem as informações de conexão do servidor e os mapeamentos de grupo para função.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- É necessário definir um servidor de diretório.

Passos

1. Selecione **Access Management**.
2. Selecione a guia **Directory Services**.
3. Se mais de um servidor estiver definido, selecione o servidor que você deseja editar na tabela.
4. Selecione **Visualizar/Editar Settings**.

   A caixa de diálogo Configurações do Servidor de Diretório é aberta.

5. Na guia **Server Settings**, altere as configurações desejadas.

Detalhes do campo

Configuração	Descrição
Configurações de configuração	Domínio(s)
O(s) nome(s) de domínio do(s) servidor(es) LDAP. Para múltiplos domínios, insira os domínios em uma lista separada por vírgulas. O nome de domínio é usado no login (*username* @*domain*) para especificar em qual servidor de diretório autenticar.	URL do servidor
A URL para acessar o servidor LDAP no formato de `ldap[s]://host:port`.	Vincular conta (opcional)
A conta de usuário somente leitura para consultas de pesquisa contra o servidor LDAP e para pesquisas dentro dos grupos.	Senha de bind (opcional)
A senha da conta de bind. (Este campo aparece quando uma conta de bind é inserida.)	Teste a conexão com o servidor antes de salvar

Configuração	Descrição
Verifica se o sistema pode se comunicar com a configuração do servidor LDAP. O teste ocorre após você clicar em **Salvar**. Se esta caixa de seleção estiver marcada e o teste falhar, a configuração não será alterada. Você deve resolver o erro ou desmarcar a caixa de seleção para ignorar o teste e reeditar a configuração.	**Configurações de privilégios**
DN base de pesquisa	O contexto LDAP para pesquisar usuários, normalmente no formato de `CN=Users, DC=cpoc, DC=local`.
Atributo de nome de usuário	O atributo que está vinculado ao ID do usuário para autenticação. Por exemplo: `sAMAccountName`.
Atributo(s) do grupo	Uma lista de atributos de grupo do usuário, usada para mapeamento de grupo para função. Por exemplo: `memberOf, managedObjects`.

6. Na aba **Mapeamento de funções**, altere o mapeamento desejado.

Detalhes do campo

Configuração	Descrição
Mapeamentos	Nome diferenciado do grupo
O nome de domínio para o grupo de usuários LDAP a ser mapeado. Expressões regulares são suportadas. Esses caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular: \.[]{}()<>*+-=!?^$	
Funções	As funções a serem mapeadas para o DN do Grupo. Você deve selecionar individualmente cada função que deseja incluir neste grupo. A função Monitor é necessária em combinação com as outras funções para fazer login no SANtricity Unified Manager. As funções incluem o seguinte: • **Administrador de armazenamento** — acesso completo de leitura/gravação aos objetos de armazenamento nos arrays, mas sem acesso à configuração de segurança. • **Administrador de segurança** — Acesso à configuração de segurança em Access Management e Certificate Management. • **Administrador de suporte** — Acesso a todos os recursos de hardware em arrays de storage, dados de falhas e eventos MEL. Sem acesso a objetos de storage ou à configuração de segurança. • **Monitor** — Acesso somente leitura a todos os objetos de storage, mas sem acesso à configuração de segurança.

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

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

Resultados

Após concluir esta tarefa, todas as sessões de usuário ativas são encerradas. Apenas a sua sessão de usuário atual é mantida.

Remover servidor de diretório

Para interromper a conexão entre um servidor de diretório e o Web Services Proxy, você pode remover as informações do servidor na página Access Management. Você pode querer realizar esta tarefa se tiver configurado um novo servidor e, em seguida, quiser remover o antigo.

Antes de começar

Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.

Sobre esta tarefa

Após concluir esta tarefa, todas as sessões de usuário ativas são encerradas. Apenas a sua sessão de usuário atual é mantida.

Passos

1. Selecione **Access Management**.
2. Selecione a guia **Directory Services**.
3. Na lista, selecione o servidor de diretório que você deseja excluir.
4. Clique em **Remover**.

   A caixa de diálogo Remove Directory Server é aberta.

5. Digite `remove` no campo e clique em **Remover**.

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

Usar SAML

Configurar SAML no SANtricity Unified Manager

Para configurar autenticação para o Gerenciamento de Acesso, você pode usar os recursos da Security Assertion Markup Language (SAML) incorporados no array de storage. Essa configuração estabelece uma conexão entre um Identity Provider e o Storage Provider.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- Você deve saber o endereço IP ou nome de domínio do controlador no array de storage.
- Um administrador de IdP configurou um sistema IdP.
- Um administrador do IdP garantiu que o IdP suporta a capacidade de retornar um Name ID na autenticação.
- Um administrador assegurou que o servidor IdP e o relógio do controlador estão sincronizados (seja por meio de um servidor NTP ou ajustando as configurações do relógio do controlador).
- Um arquivo de metadados do IdP é baixado do sistema IdP e fica disponível no sistema local usado para acessar Unified Manager.

Sobre esta tarefa

Um Provedor de Identidade (IdP) é um sistema externo usado para solicitar credenciais de um usuário e determinar se esse usuário foi autenticado com sucesso. O IdP pode ser configurado para fornecer autenticação multifator e usar qualquer banco de dados de usuários, como Active Directory. Sua equipe de segurança é responsável por manter o IdP. Um Provedor de Serviços (SP) é um sistema que controla a autenticação e o acesso do usuário. Quando o Access Management é configurado com SAML, o array de storage atua como o Service Provider para solicitar autenticação do Identity Provider. Para estabelecer uma conexão entre o IdP e o array de storage, você compartilha arquivos de metadados entre essas duas entidades. Em seguida, você mapeia as entidades de usuário do IdP para as funções do array de storage. E, finalmente, você testa a conexão e os logins SSO antes de habilitar o SAML.

SAML e Serviços de Diretório. Se você habilitar SAML quando Serviços de Diretório estiver configurado como o método de autenticação, SAML substituirá Serviços de Diretório no Unified Manager. Se você desabilitar SAML depois, a configuração de Serviços de Diretório retornará à configuração anterior.

Edição e Desativação. Depois de ativar o SAML, você *não* pode desativá-lo pela interface de usuário, nem editar as configurações do IdP. Se precisar desativar ou editar a configuração do SAML, entre em contato com o Suporte Técnico para obter assistência.

Configurar a autenticação SAML é um procedimento que envolve várias etapas.

Etapa 1: Carregar o arquivo de metadados do IdP

Para fornecer ao array de storage as informações de conexão do IdP, você importa os metadados do IdP no Unified Manager. O sistema IdP precisa desses metadados para redirecionar as solicitações de autenticação para o URL correto e para validar as respostas recebidas.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **SAML**.

   A página exibe uma visão geral das etapas de configuração.

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

   A caixa de diálogo Import Identity Provider File é aberta.

4. Clique em **Procurar** para selecionar e carregar o arquivo de metadados do IdP que você copiou para o seu sistema local.

   Após selecionar o arquivo, o IdP Entity ID é exibido.

5. Clique em **Importar**.

Etapa 2: exportar arquivos do provedor de serviços

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

Passos

1. Clique no link **Export Service Provider files**.

   A caixa de diálogo Export Service Provider Files é aberta.

2. Insira o endereço IP do controlador ou o nome DNS no campo **Controlador A** e clique em **Exportar** para salvar o arquivo de metadados em seu sistema local.

   Após clicar em **Export**, os metadados do Service Provider são baixados para o seu sistema local. Anote onde o arquivo foi armazenado.

3. No sistema local, localize o 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 Service Provider para estabelecer a relação de confiança. Você pode importar o arquivo diretamente ou inserir manualmente as informações do controlador a partir do arquivo.

Etapa 3: mapear funções

Para conceder autorização e acesso ao Unified Manager, você deve mapear os atributos de usuário e as associações de grupo do IdP para as funções predefinidas do array de storage.

Antes de começar

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

Passos

1. Clique no link para **mapeamento de funções do Unified Manager**.

   A caixa de diálogo Mapeamento de Funções é aberta.

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

Detalhes do campo

Configuração	Descrição
Mapeamentos	Atributo do usuário
Especifique o atributo (por exemplo, "member of") para o grupo SAML a ser mapeado.	Valor do atributo
Especifique o valor do atributo para o grupo a ser mapeado. Expressões regulares são suportadas. Esses caracteres especiais de expressão regular devem ser escapados com uma barra invertida (\) se não fizerem parte de um padrão de expressão regular: \.[]{}()<>*+-=!?^$	
Funções	Clique no campo e selecione uma das funções do array de storage a ser mapeada para o atributo. Você deve selecionar individualmente cada função que deseja incluir. A função Monitor é necessária em combinação com as outras funções para fazer login no Unified Manager. A função Security Admin também é necessária para pelo menos um grupo. As funções mapeadas incluem as seguintes permissões: • **Administrador de armazenamento** — acesso completo de leitura/gravação aos objetos de armazenamento (por exemplo, volumes e conjuntos de discos), mas sem acesso à configuração de segurança. • **Administrador de segurança** — Acesso à configuração de segurança no Gerenciamento de Acesso, gerenciamento de certificados, gerenciamento do log de auditoria e a capacidade de ativar ou desativar a interface de gerenciamento legada (SYMbol). • **Administrador de suporte** — Acesso a todos os recursos de hardware no array de storage, dados de falhas, eventos MEL e atualizações de firmware do controlador. Sem acesso a objetos de armazenamento ou à configuração de segurança. • **Monitor** — Acesso somente leitura a todos os objetos de storage, mas sem acesso à configuração de segurança.

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

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

   Os mapeamentos de funções podem ser modificados após o SAML ser ativado.

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

Etapa 4: teste o login SSO

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

Antes de começar

- O arquivo de metadados do IdP é importado para o Unified Manager.
- Um arquivo de metadados do provedor de serviços para o controlador é importado no sistema IdP para a relação de confiança.

Passos

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

   Uma caixa de diálogo é aberta para inserir as credenciais de SSO.

2. Insira as credenciais de login de um usuário com permissões de Security Admin e de Monitor.

   Uma caixa de diálogo é aberta enquanto o sistema testa o login.

3. Procure uma mensagem de Teste bem-sucedido. Se o teste for concluído com sucesso, vá para a próxima etapa para habilitar o SAML.

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

   - O usuário pertence a um grupo com permissões de Security Admin e Monitor.
   - Os metadados que você carregou para o servidor IdP estão corretos.
   - O endereço do controlador nos arquivos de metadados do SP está correto.

Etapa 5: habilitar SAML

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

Antes de começar

- O arquivo de metadados do IdP é importado para o Unified Manager.
- Um arquivo de metadados do provedor de serviços para o controlador é importado no sistema IdP para a relação de confiança.
- Pelo menos um mapeamento de função de Monitor e um de Security Admin está configurado.

Edição e Desativação. Depois de ativar o SAML, você *não* pode desativá-lo pela interface de usuário, nem editar as configurações do IdP. Se precisar desativar ou editar a configuração do SAML, entre em contato com o Suporte Técnico para obter assistência.

Passos

1. Na aba **SAML**, selecione o link **Enable SAML**.

   A caixa de diálogo Confirm Enable SAML é aberta.

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

Resultados

Após o sistema habilitar SAML, ele encerra todas as sessões ativas e começa a autenticar os usuários por meio de SAML.

Alterar mapeamentos de funções SAML no SANtricity Unified Manager

Se você já configurou o SAML para gerenciamento de acesso, pode alterar os mapeamentos de funções entre os grupos do IdP e as funções predefinidas do array de storage.

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- Um administrador do IdP configurou os atributos do usuário e a associação a grupos no sistema IdP.
- SAML está configurado e ativado.

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **SAML**.
3. Selecione **Role Mapping**.

   A caixa de diálogo Mapeamento de Funções é aberta.

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

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

Detalhes do campo

Configuração	Descrição
Mapeamentos	Atributo do usuário
Especifique o atributo (por exemplo, "member of") para o grupo SAML a ser mapeado.	Valor do atributo
Especifique o valor do atributo para o grupo a ser mapeado.	Funções

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

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

Resultados

Após concluir esta tarefa, todas as sessões de usuário ativas são encerradas. Apenas a sua sessão de usuário atual é mantida.

Exportar arquivos do Service Provider SAML no SANtricity Unified Manager

Caso necessário, você pode exportar os metadados do Service Provider para o array de storage e reimportar o arquivo no sistema do Identity Provider (IdP).

Antes de começar

- Você precisa estar conectado com um perfil de usuário que inclua permissões de Security admin. Caso contrário, as funções de Access Management não serão exibidas.
- SAML está configurado e ativado.

Sobre esta tarefa

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

Passos

1. Selecione o menu: Configurações [Access Management].
2. Selecione a guia **SAML**.
3. Selecione **Export**.

A caixa de diálogo Export Service Provider Files é aberta.

4. Clique em **Exportar** para salvar o arquivo de metadados em seu sistema local.

   O campo de nome de domínio é somente leitura.

   Anote onde o arquivo está 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 Service Provider. Você pode importar o arquivo diretamente ou inserir manualmente as informações do controlador.
7. Clique em **Close**.

Perguntas frequentes sobre gerenciamento de acesso de usuário para SANtricity Unified Manager

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

Por que não consigo fazer login?

Se você receber um erro ao tentar fazer login, revise estas possíveis causas.

Os erros de login podem ocorrer por um destes motivos:

- Você digitou um nome de usuário ou senha incorreto.
- Você não possui privilégios suficientes.
- Você tentou fazer login várias vezes sem sucesso, o que ativou o modo de bloqueio. Aguarde 10 minutos para fazer login novamente.
- A autenticação SAML está ativada. Atualize seu navegador para fazer login.

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

Antes de adicionar um servidor de diretório em Access Management, você deve atender a certos requisitos.

- Os grupos de usuários devem ser definidos no seu serviço de diretório.
- As credenciais do servidor LDAP devem estar disponíveis, incluindo o nome de domínio, o URL do servidor e, opcionalmente, o nome de usuário e a senha da conta de vinculação.
- Para servidores LDAPS que utilizam um protocolo seguro, a cadeia de certificados do servidor LDAP deve estar instalada em sua máquina local.

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

Antes de associar grupos a funções, revise as diretrizes.

As funcionalidades do RBAC (controle de acesso baseado em funções) incluem as seguintes funções:

- **Administrador de armazenamento** — acesso completo de leitura/gravação aos objetos de armazenamento nos arrays, mas sem acesso à configuração de segurança.

- **Administrador de segurança** — Acesso à configuração de segurança em Access Management e Certificate Management.
- **Administrador de suporte** — Acesso a todos os recursos de hardware em arrays de storage, dados de falhas e eventos MEL. Sem acesso a objetos de storage ou à configuração de segurança.
- **Monitor** — Acesso somente leitura a todos os objetos de storage, mas sem acesso à configuração de segurança.

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

Se você estiver usando um servidor LDAP (Lightweight Directory Access Protocol) e Directory Services, certifique-se de que:

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

SAML

Se você estiver usando os recursos de Security Assertion Markup Language (SAML) incorporados no array de storage, certifique-se de que:

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

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

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

O que preciso saber antes de configurar e habilitar o SAML?

Antes de configurar e ativar os recursos do Security Assertion Markup Language (SAML) para autenticação, certifique-se de atender aos seguintes requisitos e compreender as restrições do SAML.

Requisitos

Antes de começar, certifique-se de que:

- Um Provedor de Identidade (IdP) está configurado em sua rede. Um IdP é um sistema externo usado para solicitar credenciais de um usuário e determinar se o usuário foi autenticado com sucesso. Sua equipe de segurança é responsável por manter o IdP.
- Um administrador do IdP configurou atributos de usuário e grupos no sistema IdP.
- Um administrador do IdP garantiu que o IdP suporta a capacidade de retornar um Name ID na autenticação.
- Um administrador assegurou que o servidor IdP e o relógio do controlador estão sincronizados (seja por meio de um servidor NTP ou ajustando as configurações do relógio do controlador).

- Um arquivo de metadados do IdP é baixado do sistema IdP e fica disponível no sistema local usado para acessar Unified Manager.
- Você sabe o endereço IP ou nome de domínio do controlador no array de storage.

Restrições

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

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

Quais são os usuários locais?

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

Usuários locais incluem:

- **admin** — Superadministrador com acesso a todas as funções no sistema. Este usuário inclui todas as funções. A senha deve ser definida no primeiro acesso.
- **storage** — O administrador responsável por todo o provisionamento de storage. Este usuário inclui as seguintes funções: Storage Admin, Support Admin e Monitor. Esta conta fica desativada até que uma senha seja definida.
- **security** — O usuário responsável pela configuração de segurança, incluindo Access Management e Certificate Management. Este usuário inclui as seguintes funções: Security Admin e Monitor. Esta conta fica desativada até que uma senha seja definida.
- **support** — O usuário responsável pelos recursos de hardware, dados de falhas e upgrades de firmware. Este usuário inclui as seguintes funções: Support Admin e Monitor. Esta conta fica desativada até que uma senha seja definida.
- **monitor** — Um usuário com acesso somente leitura ao sistema. Este usuário inclui apenas a função Monitor. Esta conta fica desativada até que uma senha seja definida.
- **rw** (leitura/gravação) — Este usuário inclui as seguintes funções: Storage Admin, Support Admin e Monitor. Esta conta está desativada até que uma senha seja definida.

- **ro** (somente leitura) — Este usuário inclui apenas a função Monitor. Esta conta está desativada até que uma senha seja definida.

Informações sobre direitos autorais

Informações sobre marcas comerciais