



Gerenciamento de acesso

SANtricity 11.9

NetApp
December 16, 2024

Índice

- Gerenciamento de acesso 1
 - Visão geral do Gerenciamento de Acesso 1
 - Conceitos 1
 - Use funções de usuário local 7
 - Use os serviços de diretório 9
 - Use SAML 19
 - FAQs 25

Gerenciamento de acesso

Visão geral do Gerenciamento de Acesso

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

Quais métodos de autenticação estão disponíveis?

Estão disponíveis os seguintes métodos de autenticação:

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

Saiba mais:

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

Como faço para configurar o Gerenciamento de Acesso?

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

Saiba mais:

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

Conceitos

Como o Gerenciamento de Acesso funciona

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

Fluxo de trabalho de configuração

A configuração do Access Management funciona da seguinte forma:

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



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

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

Funções disponíveis no Unified Manager

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

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

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

Terminologia de Gerenciamento de Acesso

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

Prazo	Descrição
Ative Directory	O Ative Directory (AD) é um serviço de diretório da Microsoft que usa LDAP para redes de domínio do Windows.
Encadernação	As operações de vinculação são usadas para autenticar clientes no servidor de diretórios. A vinculação geralmente requer credenciais de conta e senha, mas alguns servidores permitem operações anônimas de vinculação.
CA	Uma autoridade de certificação (CA) é uma entidade confiável que emite documentos eletrônicos, chamados certificados digitais, para segurança na Internet. Esses certificados identificam proprietários de sites, o que permite conexões seguras entre clientes e servidores.
Certificado	Um certificado identifica o proprietário de um site para fins de segurança, o que impede que atacantes personifiquem o site. O certificado contém informações sobre o proprietário do site e a identidade da entidade confiável que certifica (assina) essas informações.
LDAP	O LDAP (Lightweight Directory Access Protocol) é um protocolo de aplicação para acessar e manter serviços de informação de diretório distribuído. Este protocolo permite que vários aplicativos e serviços diferentes se conectem ao servidor LDAP para validar usuários.
RBAC	O controle de acesso baseado em função (RBAC) é um método de regular o acesso a recursos de computador ou rede com base nas funções de usuários individuais. O Unified Manager inclui funções predefinidas.
SAML	Security Assertion Markup Language (SAML) é um padrão baseado em XML para autenticação e autorização entre duas entidades. O SAML permite a autenticação multifator, na qual os usuários devem fornecer dois ou mais itens para provar sua identidade (por exemplo, uma senha e uma impressão digital). O recurso SAML incorporado do storage array é compatível com SAML2,0 para afirmação, autenticação e autorização de identidade.
SSO	Logon único (SSO) é um serviço de autenticação que permite que um conjunto de credenciais de login acesse vários aplicativos.
Proxy de serviços Web	O Web Services Proxy, que fornece acesso através de mecanismos HTTPS padrão, permite que os administradores configurem serviços de gerenciamento para matrizes de armazenamento. O proxy pode ser instalado em hosts Windows ou Linux. A interface do Unified Manager está disponível com o Web Services Proxy.

Permissões para funções mapeadas

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

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

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

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

Gerenciamento de acesso com funções de usuário local

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

Fluxo de trabalho de configuração

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

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



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

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

Gerenciamento

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

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

Gerenciamento de acesso com serviços de diretório

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

Fluxo de trabalho de configuração

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

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



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

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

Gerenciamento

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

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

Gerenciamento de acesso com SAML

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

Fluxo de trabalho de configuração

A configuração SAML funciona da seguinte forma:

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

administrador de segurança.



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

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



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

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



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

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

Gerenciamento

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

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

Restrições de acesso

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

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

- Janela de gerenciamento empresarial (EMW)
- Interface de linha de comando (CLI)
- Clientes de Software Developer Kits (SDK)

- Clientes na banda
- Clientes API REST de Autenticação básica HTTP
- Faça login usando o endpoint padrão da API REST

Use funções de usuário local

Ver funções de utilizador locais

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

Antes de começar

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

Sobre esta tarefa

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

Passos

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

Os usuários são mostrados na tabela:

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

Alterar senhas para perfis de usuário locais

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

Antes de começar

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

Sobre esta tarefa

Tenha em mente estas diretrizes ao escolher uma senha:

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

Passos

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

O botão alterar senha fica disponível.

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

A caixa de diálogo alterar senha será exibida.

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

Resultados

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

Altere as definições de palavra-passe do utilizador local

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

Antes de começar

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

Sobre esta tarefa

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

- A definição de alterações não afeta as palavras-passe de utilizador locais existentes.
- A definição de comprimento mínimo necessário para palavras-passe de utilizador local tem de ter entre 0 e 30 caracteres.
- Quaisquer novas senhas de usuário local devem atender ou exceder a configuração de comprimento mínimo atual.

- Não defina um comprimento mínimo para a palavra-passe se pretender que os utilizadores locais acedam ao sistema sem introduzir uma palavra-passe.

Passos

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

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

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

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

5. Clique em **Salvar**.

Use os serviços de diretório

Adicionar servidor de diretório

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

Antes de começar

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


Sobre esta tarefa

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

Passos

1. Selecione **Gerenciamento de Acesso**.
2. Na guia **Serviços de diretório**, selecione **Adicionar servidor de diretório**.
A caixa de diálogo Adicionar servidor de diretório é aberta.
3. Na guia **Configurações do servidor**, insira as credenciais do servidor LDAP.

Detalhes do campo

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

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

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

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

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

Detalhes do campo

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



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

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

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

Edite as configurações do servidor de diretório e mapeamentos de função

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

Antes de começar

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

Passos

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

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

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

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

Detalhes do campo

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

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

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

Detalhes do campo

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



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

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

Resultados

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

Remova o servidor de diretório

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

Antes de começar

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

Sobre esta tarefa

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

Passos

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

A caixa de diálogo Remover servidor de diretório é aberta.

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

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

Use SAML

Configurar SAML

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

Antes de começar

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

Sobre esta tarefa

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



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



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

Configurar a autenticação SAML é um procedimento de várias etapas.

Passo 1: Faça o upload do arquivo de metadados IDP

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

Passos

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

A página exibe uma visão geral das etapas de configuração.

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

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

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

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

5. Clique em **Importar**.

Passo 2: Exportar arquivos do provedor de serviços

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

Passos

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

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

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

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

3. No sistema local, localize o arquivo de metadados do provedor de serviços formatado em XML que você exportou.

4. A partir do servidor IDP, importe o arquivo de metadados do provedor de serviços para estabelecer a relação de confiança. Você pode importar o arquivo diretamente ou inserir manualmente as informações do controlador a partir do arquivo.

Passo 3: Mapear funções

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

Antes de começar

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

Passos

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

A caixa de diálogo Mapeamento de função é aberta.

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

Detalhes do campo

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



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

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



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

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

Passo 4: Teste o login SSO

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

Antes de começar

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

Passos

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

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

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

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

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

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

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

Passo 5: Ative o SAML

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

Antes de começar

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

- Pelo menos um mapeamento de função Monitor e um Admin de segurança está configurado.



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

Passos

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

A caixa de diálogo confirmar ativação SAML é aberta.

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

Resultados

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

Alterar mapeamentos de função SAML

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

Antes de começar

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

Passos

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

A caixa de diálogo Mapeamento de função é aberta.

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



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

Detalhes do campo

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



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

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

Resultados

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

Exporte arquivos do provedor de serviços SAML

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

Antes de começar

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

Sobre esta tarefa

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

Passos

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

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

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



O campo de nome de domínio é somente leitura.

Anote onde o arquivo é armazenado.

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

FAQs

Por que não consigo fazer login?

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

Erros de login podem ocorrer por um destes motivos:

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

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

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

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

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

Antes de mapear grupos para funções, revise as diretrizes.

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

- **Storage admin** — Acesso completo de leitura/gravação a objetos de armazenamento nas matrizes, mas sem acesso à configuração de segurança.
- **Security admin** — Acesso à configuração de segurança em Gerenciamento de Acesso e Gerenciamento de certificados.

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



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

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

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

SAML

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

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

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

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

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

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

Requisitos

Antes de começar, certifique-se de que:

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

- Um arquivo de metadados IDP é baixado do sistema IDP e está disponível no sistema local usado para acessar o Unified Manager.
- Você sabe o endereço IP ou o nome de domínio do controlador na matriz de armazenamento.

Restrições

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

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

Quais são os usuários locais?

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

Os usuários locais incluem:

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

- **Ro** (somente leitura) — este usuário inclui somente a função Monitor. Esta conta é desativada até que uma palavra-passe seja definida.

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.