Conceitos

SANtricity software

NetApp
March 17, 2026

Índice

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

Informações sobre direitos autorais

Informações sobre marcas comerciais