



Conceitos

SANtricity 11.9

NetApp
December 16, 2024

Índice

- Conceitos 1
 - Como o Gerenciamento de Acesso funciona 1
 - Terminologia de Gerenciamento de Acesso 2
 - Permissões para funções mapeadas 3
 - Gerenciamento de acesso com funções de usuário local 3
 - Gerenciamento de acesso com serviços de diretório 4
 - Gerenciamento de acesso com SAML 5

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

Prazo	Descrição
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

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.