Gerenciamento de acesso

SANtricity software

NetApp
March 17, 2026

Índice

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.
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