Gerenciamento de acesso

SANtricity 11.7

NetApp
February 13, 2025

Índice

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 ative Directory da Microsoft.

Saiba mais:

- "Como o Gerenciamento de Acesso funciona"
- "Terminologia de Gerenciamento de Acesso"
- "Permissões para funções mapeadas"

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"

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 ative Directory da Microsoft. Um administrador se coneta ao servidor LDAP e, em seguida, mapeia os usuários LDAP para as funções de usuário local.
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 aceder e manter serviços de informação de diretório distribuído. Este protocolo permite que vários aplicativos e serviços diferentes se conetem 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.
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 ative 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.

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 conetado 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 carateres 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 conetado 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 acedam 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 carateres.
- 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 conetado 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 (*username__domain*) para especificar em qual servidor de diretório se autenticar.	URL do servidor
Insira o URL para acessar o servidor LDAP na forma `ldap[s]://**host**:*port*` de .	Carregar certificado (opcional)
Este campo aparece apenas se um protocolo LDAPS for especificado no campo URL do servidor acima. 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.	Vincular conta (opcional)

Definição	Descrição
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` .	Vincular senha (opcional)
Este campo é exibido quando você insere uma conta BIND. Introduza a palavra-passe para a conta vincular.	Teste a conexão do servidor antes de adicionar

Definição	Descrição
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. 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.	• Configurações de privilégio*
Pesquisar DN base	Introduza o contexto LDAP para procurar utilizadores, normalmente na forma `CN=Users, DC=cpoc, DC=local` de .
Atributo de nome de usuário	Insira o atributo que está vinculado ao ID do usuário para autenticação. Por exemplo `sAMAccountName`: .
Atributo(s) de grupo	Insira uma lista de atributos de grupo no usuário, que é usada para mapeamento de grupo para função. Por exemplo `memberOf, managedObjects`: .

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 carateres 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 conetado 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 (*username__domain*) para especificar em qual servidor de diretório se autenticar.	URL do servidor
O URL para acessar o servidor LDAP na forma `ldap[s]://host:port` de .	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.	• 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 carateres 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.

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

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.

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.

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

Informações sobre marcas comerciais