Gerenciar contas

Element Software

NetApp
November 12, 2025

Índice

Gerenciar contas . . . 1
- Gerenciar contas . . . 1
  - Para maiores informações . . . 1
- Trabalhar com contas usando CHAP . . . 1
  - Algoritmos CHAP . . . 1
  - Criar uma conta . . . 2
  - Ver detalhes da conta . . . 2
  - Editar uma conta . . . 3
  - Excluir uma conta . . . 3
  - Encontre mais informações . . . 4
- Gerenciar contas de usuário administradoras de cluster . . . 4
  - tipos de conta de administrador de cluster de armazenamento . . . 4
  - Ver detalhes do administrador do cluster . . . 4
  - Crie uma conta de administrador de cluster. . . . 5
  - Editar permissões de administrador do cluster . . . 6
  - Alterar senhas para contas de administrador do cluster . . . 6
- Gerenciar LDAP . . . 7
  - Conclua as etapas de pré-configuração para suporte a LDAP. . . . 8
  - Habilite a autenticação LDAP com a interface de usuário do Element. . . . 8
  - Habilite a autenticação LDAP com a API Element. . . . 10
  - Ver detalhes do LDAP . . . 13
  - Teste a configuração LDAP . . . 13
  - Desativar LDAP . . . 15
  - Encontre mais informações . . . 15

Gerenciar contas

Gerenciar contas

Nos sistemas de armazenamento SolidFire , os locatários podem usar contas para permitir que os clientes se conectem a volumes em um cluster. Ao criar um volume, ele é atribuído a uma conta específica. Você também pode gerenciar contas de administrador de cluster para um sistema de armazenamento SolidFire .

- "Trabalhar com contas usando CHAP"
- "Gerenciar contas de usuário administradoras de cluster"

Para maiores informações

- "Documentação do SolidFire e do Element Software"
- "Plug-in NetApp Element para vCenter Server"

Trabalhar com contas usando CHAP

Nos sistemas de armazenamento SolidFire , os locatários podem usar contas para permitir que os clientes se conectem a volumes em um cluster. Uma conta contém a autenticação do Protocolo de Autenticação por Desafio e Aperto de Mão (CHAP) necessária para acessar os volumes a ela atribuídos. Ao criar um volume, ele é atribuído a uma conta específica.

Uma conta pode ter até dois mil volumes atribuídos a ela, mas um volume só pode pertencer a uma conta.

Algoritmos CHAP

A partir do Element 12.7, os algoritmos CHAP seguros e compatíveis com FIPS, SHA1, SHA-256 e SHA3-256, são suportados. Quando um iniciador iSCSI de um host está criando uma sessão iSCSI com um alvo iSCSI Element, ele solicita uma lista de algoritmos CHAP a serem usados. O dispositivo Element iSCSI escolhe o primeiro algoritmo compatível dentre os solicitados pelo iniciador iSCSI do host. Para confirmar se o alvo iSCSI do Element está escolhendo o algoritmo mais seguro, você deve configurar o iniciador iSCSI do host para enviar uma lista de algoritmos ordenados do mais seguro, por exemplo, SHA3-256, ao menos seguro, por exemplo, SHA1 ou MD5. Quando os algoritmos SHA não são solicitados pelo iniciador iSCSI do host, o alvo iSCSI Element escolhe o MD5, assumindo que a lista de algoritmos propostos pelo host contenha MD5. Você pode precisar atualizar a configuração do iniciador iSCSI do host para habilitar o suporte a algoritmos seguros.

Durante uma atualização do Element 12.7 ou posterior, se você já tiver atualizado a configuração do iniciador iSCSI do host para enviar uma solicitação de sessão com uma lista que inclua algoritmos SHA, à medida que os nós de armazenamento forem reinicializados, os novos algoritmos seguros serão ativados e novas sessões iSCSI ou as sessões reconectadas serão estabelecidas usando o protocolo mais seguro. Todas as sessões iSCSI existentes passam de MD5 para SHA durante a atualização. Se você não atualizar a configuração do iniciador iSCSI do host para solicitar SHA, as sessões iSCSI existentes continuarão usando MD5. Posteriormente, após a atualização dos algoritmos CHAP do iniciador iSCSI do host, as sessões iSCSI deverão migrar gradualmente de MD5 para SHA ao longo do tempo, com base em atividades de manutenção que resultem em reconexões de sessão iSCSI.

Por exemplo, o iniciador iSCSI padrão do host no Red Hat Enterprise Linux (RHEL) 8.3 possui o `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5` A configuração comentada resulta no iniciador iSCSI usando apenas MD5. Remover o comentário dessa configuração no host e reiniciar o iniciador iSCSI fará com que as sessões iSCSI desse host comecem a usar SHA3-256.

Se necessário, você pode usar o "ListISCSISessions" Método da API para visualizar os algoritmos CHAP utilizados em cada sessão.

Criar uma conta

Você pode criar uma conta para permitir o acesso aos volumes.

Cada nome de conta no sistema deve ser único.

1. Selecione **Gestão** > **Contas**.
2. Clique em **Criar conta**.
3. Digite um **nome de usuário**.
4. Na seção **Configurações CHAP**, insira as seguintes informações:

   Deixe os campos de credenciais em branco para gerar automaticamente uma senha.

   - **Segredo do Iniciador** para autenticação de sessão de nó CHAP.
   - **Segredo de destino** para autenticação de sessão de nó CHAP.
5. Clique em **Criar conta**.

Ver detalhes da conta

Você pode visualizar o desempenho de contas individuais em formato gráfico.

As informações do gráfico fornecem dados de entrada/saída e taxa de transferência da conta. Os níveis de atividade média e de pico são mostrados em incrementos de 10 segundos. Essas estatísticas incluem a atividade de todos os volumes atribuídos à conta.

1. Selecione **Gestão** > **Contas**.
2. Clique no ícone Ações para criar uma conta.
3. Clique em **Ver detalhes**.

Aqui estão alguns detalhes:

- **Status**: O status da conta. Valores possíveis:
  - Ativo: Uma conta ativa.
  - bloqueado: Uma conta bloqueada.
  - Removido: Uma conta que foi excluída e removida permanentemente.
- **Volumes Ativos**: O número de volumes ativos atribuídos à conta.
- **Compressão**: A pontuação de eficiência de compressão para os volumes atribuídos à conta.
- **Deduplicação**: A pontuação de eficiência de deduplicação para os volumes atribuídos à conta.
- **Provisionamento Dinâmico**: A pontuação de eficiência do provisionamento dinâmico para os volumes

atribuídos à conta.

- **Eficiência Geral**: A pontuação geral de eficiência para os volumes atribuídos à conta.

Editar uma conta

Você pode editar uma conta para alterar o status, modificar os segredos CHAP ou alterar o nome da conta.

Modificar as configurações CHAP em uma conta ou remover iniciadores ou volumes de um grupo de acesso pode fazer com que os iniciadores percam o acesso aos volumes inesperadamente. Para garantir que o acesso ao volume não seja perdido inesperadamente, sempre encerre as sessões iSCSI que serão afetadas por uma alteração de conta ou grupo de acesso e verifique se os iniciadores conseguem se reconectar aos volumes após a conclusão de quaisquer alterações nas configurações do iniciador e do cluster.

> Os volumes persistentes associados aos serviços de gerenciamento são atribuídos a uma nova conta criada durante a instalação ou atualização. Se você estiver usando volumes persistentes, não modifique nem exclua a conta associada a eles.

1. Selecione **Gestão** > **Contas**.
2. Clique no ícone Ações para criar uma conta.
3. No menu que aparecer, selecione **Editar**.
4. **Opcional:** Edite o **Nome de usuário**.
5. **Opcional:** Clique na lista suspensa **Status** e selecione um status diferente.

> Alterar o status para **bloqueado** encerra todas as conexões iSCSI com a conta, e a conta deixa de ser acessível. Os volumes associados à conta são mantidos; no entanto, esses volumes não são detectáveis por iSCSI.

6. **Opcional:** Em **Configurações CHAP**, edite as credenciais **Segredo do Iniciador** e **Segredo do Destino** usadas para autenticação da sessão do nó.

> Se você não alterar as credenciais das **Configurações CHAP**, elas permanecerão as mesmas. Se você deixar os campos de credenciais em branco, o sistema gerará novas senhas.

7. Clique em **Salvar alterações**.

Excluir uma conta

Você pode excluir uma conta quando ela não for mais necessária.

Antes de excluir a conta, apague e remova todos os volumes associados a ela.

> Os volumes persistentes associados aos serviços de gerenciamento são atribuídos a uma nova conta criada durante a instalação ou atualização. Se você estiver usando volumes persistentes, não modifique nem exclua a conta associada a eles.

1. Selecione **Gestão** > **Contas**.
2. Clique no ícone Ações da conta que deseja excluir.
3. No menu que aparecer, selecione **Excluir**.

4. Confirme a ação.

Encontre mais informações

- "Documentação do SolidFire e do Element Software"
- "Plug-in NetApp Element para vCenter Server"

Gerenciar contas de usuário administradoras de cluster

Você pode gerenciar contas de administrador de cluster para um sistema de armazenamento SolidFire criando, excluindo e editando contas de administrador de cluster, alterando a senha do administrador de cluster e configurando as definições de LDAP para gerenciar o acesso dos usuários ao sistema.

tipos de conta de administrador de cluster de armazenamento

Existem dois tipos de contas de administrador que podem existir em um cluster de armazenamento executando o software NetApp Element : a conta de administrador primário do cluster e uma conta de administrador do cluster.

- **Conta de administrador do cluster principal**

  Essa conta de administrador é criada quando o cluster é criado. Esta conta é a conta administrativa principal com o nível mais alto de acesso ao cluster. Essa conta é análoga a um usuário root em um sistema Linux. Você pode alterar a senha desta conta de administrador.

- **Conta de administrador do cluster**

  Você pode conceder a uma conta de administrador de cluster um conjunto limitado de acesso administrativo para executar tarefas específicas dentro do cluster. As credenciais atribuídas a cada conta de administrador de cluster são usadas para autenticar solicitações de API e da interface do usuário do Element dentro do sistema de armazenamento.

> É necessária uma conta de administrador de cluster local (não LDAP) para acessar os nós ativos em um cluster por meio da interface de usuário de cada nó. Não são necessárias credenciais de conta para acessar um nó que ainda não faz parte de um cluster.

Ver detalhes do administrador do cluster

1. Para criar uma conta de administrador de cluster (não LDAP) para todo o cluster, execute as seguintes ações:
   a. Clique em **Usuários** > **Administradores do cluster**.
2. Na página Administradores do Cluster, na aba Usuários, você pode visualizar as seguintes informações.
   - **ID**: Número sequencial atribuído à conta de administrador do cluster.
   - **Nome de usuário**: O nome atribuído à conta de administrador do cluster quando ela foi criada.
   - **Acesso**: As permissões de usuário atribuídas à conta do usuário. Valores possíveis:
     - ler

- reportagem
- nós
- dirige
- volumes
- contas
- Administradores do cluster
- administrador
- suporteAdministrador

> Todas as permissões estão disponíveis para o tipo de acesso de administrador.
>
> Existem tipos de acesso disponíveis através da API que não estão disponíveis na interface do usuário do Element.

+

- **Tipo**: O tipo de administrador do cluster. Valores possíveis:
  - Conjunto
  - Ldap
- **Atributos**: Se a conta de administrador do cluster foi criada usando a API Element, esta coluna mostra quaisquer pares nome-valor que foram definidos usando esse método.

  Ver"Referência da API do NetApp Element Software" .

Crie uma conta de administrador de cluster.

Você pode criar novas contas de administrador de cluster com permissões para permitir ou restringir o acesso a áreas específicas do sistema de armazenamento. Ao configurar as permissões da conta de administrador do cluster, o sistema concede direitos somente leitura para quaisquer permissões que você não atribuir ao administrador do cluster.

Se você deseja criar uma conta de administrador de cluster LDAP, certifique-se de que o LDAP esteja configurado no cluster antes de começar.

"Habilite a autenticação LDAP com a interface de usuário do Element."

Posteriormente, você poderá alterar os privilégios da conta de administrador do cluster para relatórios, nós, unidades, volumes, contas e acesso em nível de cluster. Ao habilitar uma permissão, o sistema atribui acesso de gravação para esse nível. O sistema concede ao usuário administrador acesso somente leitura para os níveis que você não selecionar.

Você também poderá remover posteriormente qualquer conta de usuário administrador de cluster criada por um administrador de sistema. Não é possível remover a conta de administrador principal do cluster que foi criada quando o cluster foi criado.

1. Para criar uma conta de administrador de cluster (não LDAP) para todo o cluster, execute as seguintes ações:
   a. Clique em **Usuários** > **Administradores do cluster**.

b. Clique em **Criar administrador de cluster**.
c. Selecione o tipo de usuário **Cluster**.
d. Insira um nome de usuário e uma senha para a conta e confirme a senha.
e. Selecione as permissões de usuário que deseja aplicar à conta.
f. Selecione a caixa de seleção para concordar com o Contrato de Licença do Usuário Final.
g. Clique em **Criar administrador de cluster**.

2. Para criar uma conta de administrador de cluster no diretório LDAP, execute as seguintes ações:

a. Clique em **Cluster** > **LDAP**.
b. Certifique-se de que a autenticação LDAP esteja habilitada.
c. Clique em **Testar autenticação do usuário** e copie o nome distinto que aparece para o usuário ou para um dos grupos aos quais o usuário pertence, para que você possa colá-lo posteriormente.
d. Clique em **Usuários** > **Administradores do cluster**.
e. Clique em **Criar administrador de cluster**.
f. Selecione o tipo de usuário LDAP.
g. No campo Nome Distinto, siga o exemplo na caixa de texto para inserir um nome distinto completo para o usuário ou grupo. Alternativamente, cole o nome distinto que você copiou anteriormente.

   Se o nome distinto fizer parte de um grupo, qualquer usuário que seja membro desse grupo no servidor LDAP terá as permissões dessa conta de administrador.

Para adicionar usuários ou grupos de Administradores de Cluster LDAP, o formato geral do nome de usuário é “LDAP:<Nome Distinto Completo>”.

a. Selecione as permissões de usuário que deseja aplicar à conta.
b. Selecione a caixa de seleção para concordar com o Contrato de Licença do Usuário Final.
c. Clique em **Criar administrador de cluster**.

Editar permissões de administrador do cluster

Você pode alterar os privilégios da conta de administrador do cluster para relatórios, nós, unidades, volumes, contas e acesso em nível de cluster. Ao habilitar uma permissão, o sistema atribui acesso de gravação para esse nível. O sistema concede ao usuário administrador acesso somente leitura para os níveis que você não selecionar.

1. Clique em **Usuários** > **Administradores do cluster**.
2. Clique no ícone Ações do administrador do cluster que você deseja editar.
3. Clique em **Editar**.
4. Selecione as permissões de usuário que deseja aplicar à conta.
5. Clique em **Salvar alterações**.

Alterar senhas para contas de administrador do cluster

Você pode usar a interface do Element para alterar as senhas do administrador do cluster.

1. Clique em **Usuários** > **Administradores do cluster**.

2. Clique no ícone Ações do administrador do cluster que você deseja editar.
3. Clique em **Editar**.
4. No campo Alterar Senha, digite uma nova senha e confirme-a.
5. Clique em **Salvar alterações**.

Informações relacionadas

- "Saiba mais sobre os tipos de acesso disponíveis para as APIs do Element."
- "Habilite a autenticação LDAP com a interface de usuário do Element."
- "Desativar LDAP"
- "Plug-in NetApp Element para vCenter Server"

Gerenciar LDAP

Você pode configurar o Lightweight Directory Access Protocol (LDAP) para habilitar a funcionalidade de login seguro baseado em diretório para o armazenamento SolidFire . Você pode configurar o LDAP no nível do cluster e autorizar usuários e grupos LDAP.

O gerenciamento de LDAP envolve a configuração da autenticação LDAP em um cluster SolidFire usando um ambiente Microsoft Active Directory existente e o teste da configuração.

Você pode usar endereços IPv4 e IPv6.

Habilitar o LDAP envolve as seguintes etapas gerais, descritas em detalhes a seguir:

1. **Conclua as etapas de pré-configuração para suporte a LDAP**. Verifique se você possui todos os detalhes necessários para configurar a autenticação LDAP.
2. **Ativar autenticação LDAP**. Utilize a interface de usuário do Element ou a API do Element.
3. **Validar a configuração LDAP**. Opcionalmente, verifique se o cluster está configurado com os valores corretos executando o método de API GetLdapConfiguration ou verificando a configuração LCAP usando a interface do usuário do Element.
4. **Teste a autenticação LDAP** (com o `readonly` usuário). Verifique se a configuração LDAP está correta executando o método da API TestLdapAuthentication ou usando a interface do usuário do Element. Para este teste inicial, use o nome de usuário “sAMAccountName” do `readonly` usuário. Isso validará se o seu cluster está configurado corretamente para autenticação LDAP e também se o `readonly` As credenciais e o acesso estão corretos. Se esta etapa falhar, repita os passos 1 a 3.
5. **Teste a autenticação LDAP** (com uma conta de usuário que você deseja adicionar). Repita o passo 4 com a conta de usuário que você deseja adicionar como administrador do cluster Element. Copie o `distinguished` nome (DN) ou o usuário (ou o grupo). Este DN será usado na etapa 6.
6. **Adicione o administrador do cluster LDAP** (copie e cole o DN da etapa de teste de autenticação LDAP). Utilizando a interface de usuário do Element ou o método da API AddLdapClusterAdmin, crie um novo usuário administrador de cluster com o nível de acesso apropriado. No campo do nome de usuário, cole o DN completo que você copiou na Etapa 5. Isso garante que o DN esteja formatado corretamente.
7. **Teste o acesso de administrador do cluster**. Faça login no cluster usando o usuário administrador LDAP do cluster recém-criado. Se você adicionou um grupo LDAP, poderá fazer login como qualquer usuário desse grupo.

Conclua as etapas de pré-configuração para suporte a LDAP.

Antes de habilitar o suporte a LDAP no Element, você deve configurar um servidor Windows Active Directory e executar outras tarefas de pré-configuração.

Passos

1. Configure um servidor Active Directory do Windows.
2. **Opcional:** Habilitar o suporte a LDAPS.
3. Criar usuários e grupos.
4. Crie uma conta de serviço somente leitura (como “sfreadonly”) para ser usada na busca do diretório LDAP.

Habilite a autenticação LDAP com a interface de usuário do Element.

Você pode configurar a integração do sistema de armazenamento com um servidor LDAP existente. Isso permite que os administradores LDAP gerenciem centralmente o acesso dos usuários ao sistema de armazenamento.

Você pode configurar o LDAP usando a interface de usuário do Element ou a API do Element. Este procedimento descreve como configurar o LDAP usando a interface de usuário do Element.

Este exemplo mostra como configurar a autenticação LDAP no SolidFire e utiliza `SearchAndBind` como tipo de autenticação. O exemplo utiliza um único servidor Active Directory do Windows Server 2012 R2.

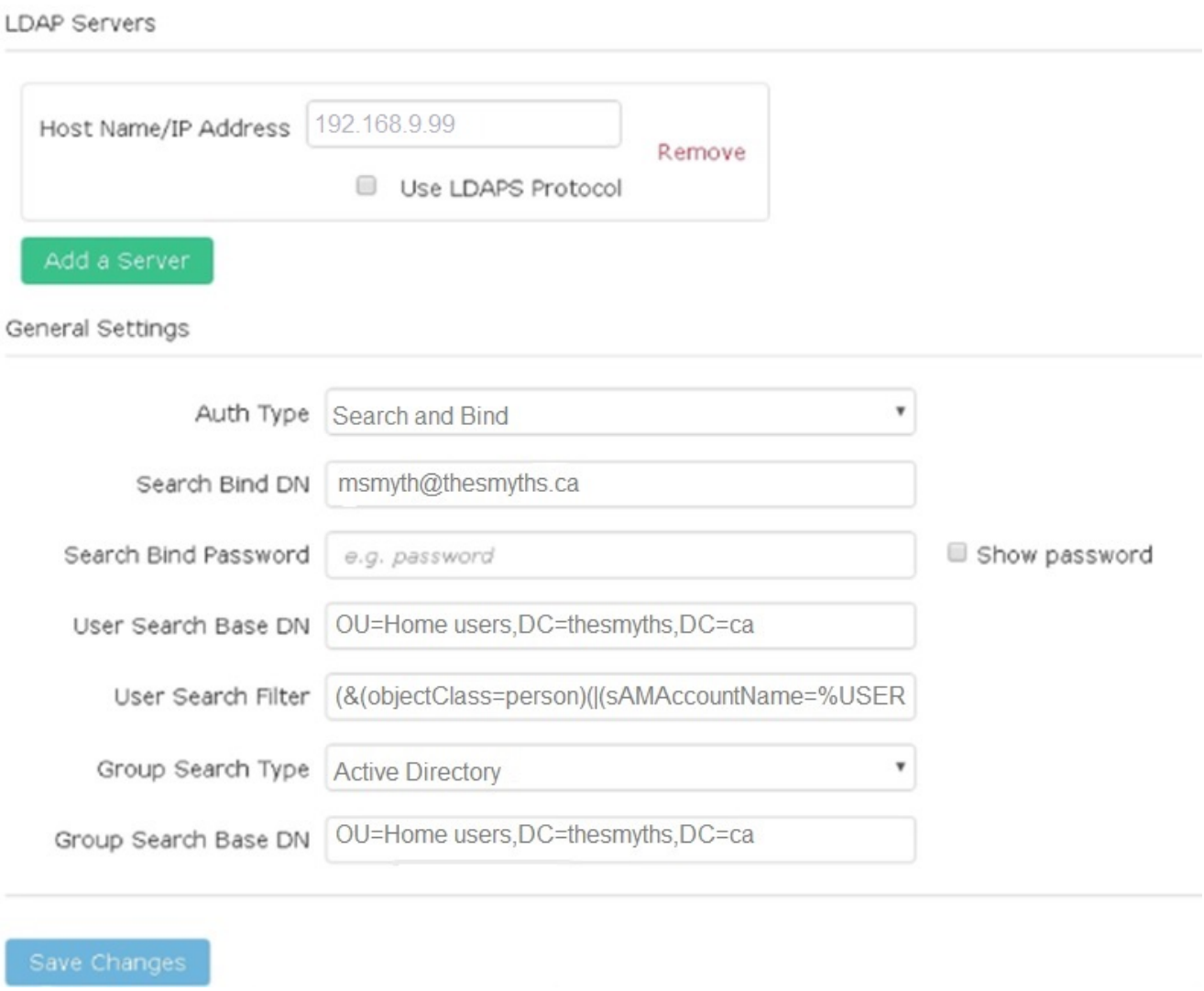
Passos

1. Clique em **Cluster** > **LDAP**.
2. Clique em **Sim** para ativar a autenticação LDAP.
3. Clique em **Adicionar um servidor**.
4. Digite o **Nome do Host/Endereço IP**.

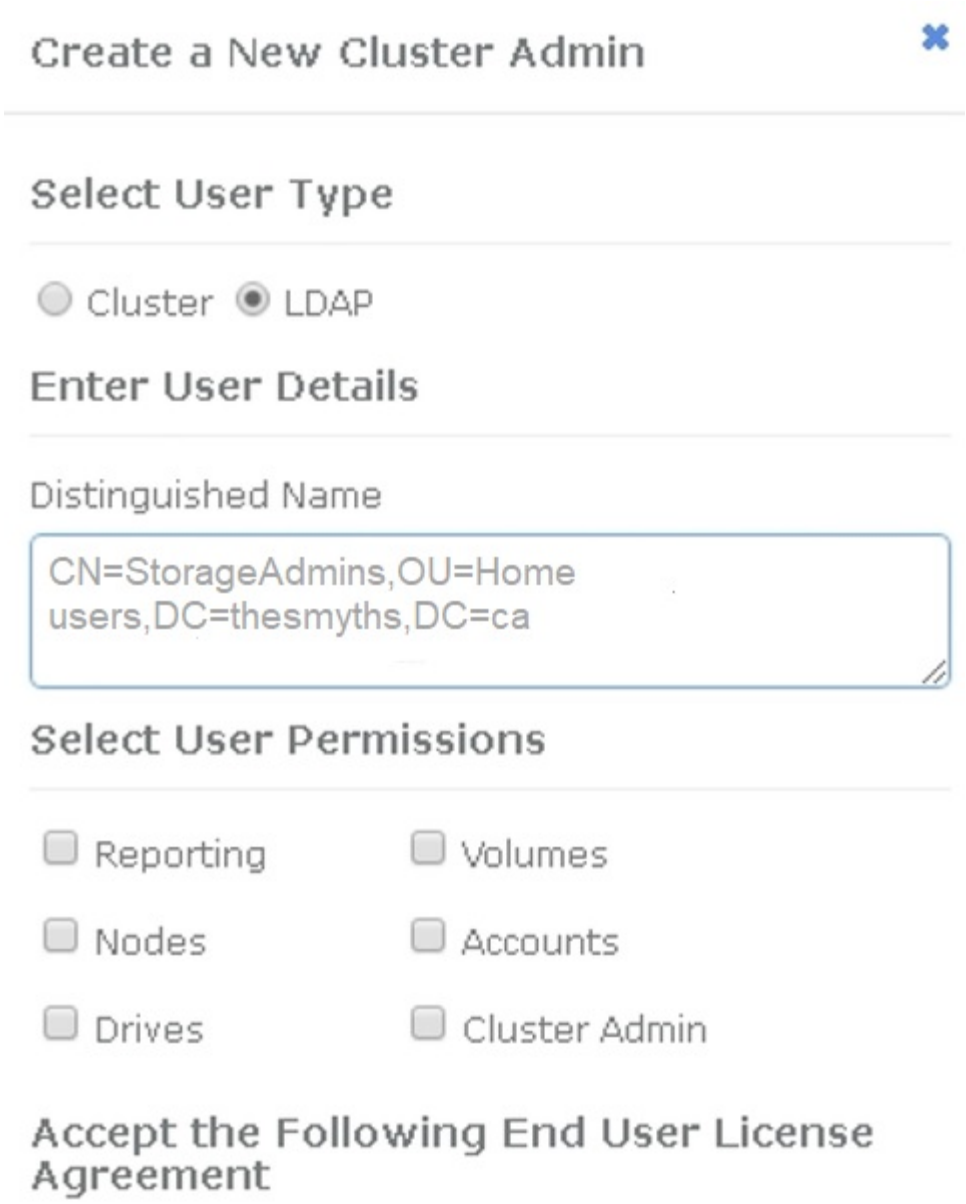
   Opcionalmente, também é possível inserir um número de porta personalizado.

   Por exemplo, para adicionar um número de porta personalizado, digite <nome do host ou endereço IP>:<número da porta>

5. **Opcional:** Selecione **Usar protocolo LDAPS**.
6. Insira as informações necessárias em **Configurações Gerais**.



7. Clique em **Ativar LDAP**.
8. Clique em **Testar autenticação do usuário** se quiser testar o acesso do usuário ao servidor.
9. Copie o nome distinto e as informações do grupo de usuários que aparecem para uso posterior na criação de administradores de cluster.
10. Clique em **Salvar alterações** para salvar as novas configurações.
11. Para criar um usuário neste grupo para que qualquer pessoa possa fazer login, complete os seguintes passos:
    a. Clique em **Usuário** > **Visualizar**.



b. Para o novo usuário, clique em **LDAP** para o Tipo de Usuário e cole o grupo que você copiou no campo Nome Distinto.
c. Selecione as permissões, normalmente todas as permissões.
d. Role a página para baixo até o Contrato de Licença do Usuário Final e clique em **Aceito**.
e. Clique em **Criar administrador de cluster**.

   Agora você tem um usuário com o valor de um grupo do Active Directory.

Para testar isso, saia da interface do usuário do Element e entre novamente como um usuário desse grupo.

Habilite a autenticação LDAP com a API Element.

Você pode configurar a integração do sistema de armazenamento com um servidor LDAP existente. Isso permite que os administradores LDAP gerenciem centralmente o acesso dos usuários ao sistema de armazenamento.

Você pode configurar o LDAP usando a interface de usuário do Element ou a API do Element. Este procedimento descreve como configurar o LDAP usando a API Element.

Para aproveitar a autenticação LDAP em um cluster SolidFire , primeiro você habilita a autenticação LDAP no cluster usando o seguinte comando: `EnableLdapAuthentication` Método da API.

Passos

1. Primeiro, habilite a autenticação LDAP no cluster usando o `EnableLdapAuthentication` Método da API.
2. Insira as informações solicitadas.

```
{
     "method":"EnableLdapAuthentication",
     "params":{
          "authType": "SearchAndBind",
          "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
          "groupSearchType": "ActiveDirectory",
          "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
          "searchBindPassword": "ReadOnlyPW",
          "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
          "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
          "serverURIs": [
               "ldap://172.27.1.189",
          [
     },
  "id":"1"
}
```

3. Altere os valores dos seguintes parâmetros:

Parâmetros utilizados	Descrição
authType: SearchAndBind	Determina que o cluster usará a conta de serviço somente leitura para primeiro procurar o usuário que está sendo autenticado e, posteriormente, vincular esse usuário se ele for encontrado e autenticado.
groupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Especifica a localização na árvore LDAP onde iniciar a busca por grupos. Neste exemplo, usamos a raiz da nossa árvore. Se sua árvore LDAP for muito grande, talvez seja interessante definir isso para uma subárvore mais granular para diminuir o tempo de busca.

Parâmetros utilizados	Descrição
userSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Especifica a localização na árvore LDAP onde iniciar a busca por usuários. Neste exemplo, usamos a raiz da nossa árvore. Se sua árvore LDAP for muito grande, talvez seja interessante definir isso para uma subárvore mais granular para diminuir o tempo de busca.
groupSearchType: ActiveDirectory	Utiliza o servidor Windows Active Directory como servidor LDAP.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Para usar o userPrincipalName (endereço de e-mail para login), você pode alterar o userSearchFilter para:
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
Ou, para pesquisar tanto o userPrincipalName quanto o sAMAccountName, você pode usar o seguinte userSearchFilter:
 	
`"(&(objectClass=person)(`
	(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))" ----

Utiliza o sAMAccountName como nome de usuário para fazer login no cluster SolidFire . Essas configurações instruem o LDAP a procurar o nome de usuário especificado durante o login no atributo sAMAccountName e também a limitar a pesquisa a entradas que tenham “person” como valor no atributo objectClass.	pesquisarBindDN
Este é o nome distinto do usuário somente leitura que será usado para pesquisar o diretório LDAP. Para o Active Directory, geralmente é mais fácil usar o userPrincipalName (formato de endereço de e-mail) para o usuário.	pesquisarBindPassword

Para testar isso, saia da interface do usuário do Element e entre novamente como um usuário desse grupo.

Ver detalhes do LDAP

Visualize as informações do LDAP na página LDAP, na guia Cluster.

Você precisa habilitar o LDAP para visualizar essas configurações do LDAP.

1. Para visualizar os detalhes do LDAP com a interface do usuário do Element, clique em **Cluster** > **LDAP**.
   - **Nome do host/Endereço IP**: Endereço de um servidor de diretório LDAP ou LDAPS.
   - **Tipo de autenticação**: O método de autenticação do usuário. Valores possíveis:
     - Ligação direta
     - Pesquisar e vincular
   - **DN de vinculação de pesquisa**: Um DN totalmente qualificado para fazer login e realizar uma pesquisa LDAP pelo usuário (requer acesso de nível de vinculação ao diretório LDAP).
   - **Senha de Vinculação da Pesquisa**: Senha usada para autenticar o acesso ao servidor LDAP.
   - **DN base da pesquisa de usuários**: O DN base da árvore usada para iniciar a pesquisa de usuários. O sistema pesquisa a subárvore a partir da localização especificada.
   - **Filtro de pesquisa de usuários**: Digite o seguinte usando o nome do seu domínio:

     ```
     (&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
     ```

   - **Tipo de pesquisa de grupo**: Tipo de pesquisa que controla o filtro de pesquisa de grupo padrão utilizado. Valores possíveis:
     - Active Directory: Associação aninhada de todos os grupos LDAP de um usuário.
     - Sem grupos: Não há suporte em grupo.
     - Membro DN: Grupos no estilo DN (nível único).
   - **DN base da pesquisa em grupo**: O DN base da árvore usada para iniciar a pesquisa em grupo. O sistema pesquisa a subárvore a partir da localização especificada.
   - **Testar a autenticação do usuário**: Após configurar o LDAP, use este método para testar a autenticação por nome de usuário e senha no servidor LDAP. Insira uma conta já existente para testar. O nome distinto e as informações do grupo de usuários são exibidos, e você pode copiá-los para uso posterior ao criar administradores de cluster.

Teste a configuração LDAP

Após configurar o LDAP, você deve testá-lo usando a interface do usuário do Element ou a API do Element. `TestLdapAuthentication` método.

Passos

1. Para testar a configuração LDAP com a interface do usuário do Element, faça o seguinte:
   a. Clique em **Cluster** > **LDAP**.
   b. Clique em **Testar autenticação LDAP**.
   c. Resolva quaisquer problemas utilizando as informações da tabela abaixo:

Mensagem de erro	Descrição
`xLDAPUserNotFound`	• O usuário que estava sendo testado não foi encontrado na lista configurada. `userSearchBaseDN` subárvore. • O `userSearchFilter` está configurado incorretamente.
`xLDAPBindFailed (Error: Invalid credentials)`	• O nome de usuário que está sendo testado é um usuário LDAP válido, mas a senha fornecida está incorreta. • O nome de usuário que está sendo testado é um usuário LDAP válido, mas a conta está atualmente desativada.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	O URI do servidor LDAP está incorreto.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	O nome de usuário ou a senha somente leitura estão configurados incorretamente.
`xLDAPSearchFailed (Error: No such object)`	O `userSearchBaseDN` não é um local válido na árvore LDAP.
`xLDAPSearchFailed (Error: Referral)`	• O `userSearchBaseDN` não é um local válido na árvore LDAP. • O `userSearchBaseDN` e `groupSearchBaseDN` estão em uma Unidade Organizacional aninhada. Isso pode causar problemas de permissão. A solução alternativa é incluir a Unidade Organizacional (OU) nas entradas DN base do usuário e do grupo (por exemplo: `ou=storage, cn=company, cn=com`)

2. Para testar a configuração LDAP com a API Element, faça o seguinte:
   a. Chame o método TestLdapAuthentication.

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

b. Analise os resultados. Se a chamada à API for bem-sucedida, os resultados incluirão o nome distinto do usuário especificado e uma lista dos grupos dos quais o usuário é membro.

```
{
"id": 1
     "result": {
         "groups": [

"CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
         ],
         "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
     }
}
```

Desativar LDAP

Você pode desativar a integração LDAP usando a interface do usuário do Element.

Antes de começar, anote todas as configurações, pois desativar o LDAP apaga todas elas.

Passos

1. Clique em **Cluster** > **LDAP**.
2. Clique em **Não**.
3. Clique em **Desativar LDAP**.

Encontre mais informações

- "Documentação do SolidFire e do Element Software"
- "Plug-in NetApp Element para vCenter Server"

Informações sobre direitos autorais

Informações sobre marcas comerciais