Gerenciar contas

Element Software

NetApp
November 21, 2024

Índice

Gerenciar contas

Nos sistemas de storage da SolidFire, os locatários podem usar contas para permitir que os clientes se conetem a volumes em um cluster. Quando você cria um volume, ele é atribuído a uma conta específica. Você também pode gerenciar contas de administrador de cluster para um sistema de storage SolidFire.

- "Trabalhar com contas usando CHAP"
- "Gerenciar contas de usuários de administrador de cluster"

Para mais informações

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

Trabalhar com contas usando CHAP

Nos sistemas de storage da SolidFire, os locatários podem usar contas para permitir que os clientes se conetem a volumes em um cluster. Uma conta contém a autenticação CHAP (Challenge-Handshake Authentication Protocol) necessária para acessar os volumes atribuídos a ela. Quando você cria um volume, ele é atribuído a uma conta específica.

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

Algoritmos CHAP

A partir do Element 12,7, os algoritmos CHAP seguros compatíveis com FIPS SHA1, SHA-256 e SHA3-256 são suportados. Com o elemento 12,7, quando um iniciador iSCSI de host está criando uma sessão iSCSI com um destino iSCSI de elemento, ele solicita uma lista de algoritmos CHAP para usar. O destino iSCSI Element escolhe o primeiro algoritmo que suporta a partir da lista solicitada pelo iniciador iSCSI do host. Para confirmar que o destino iSCSI Element escolhe o algoritmo mais seguro, você deve configurar o iniciador iSCSI do host para enviar uma lista de algoritmos solicitados da maioria dos seguros, por exemplo, SHA3-256, para o menos seguro, por exemplo, SHA1 ou MD5. Quando os algoritmos SHA não são solicitados pelo iniciador iSCSI do host, o destino iSCSI do elemento escolhe MD5, assumindo que a lista de algoritmos proposta do host contém MD5. Talvez seja necessário atualizar a configuração do iniciador iSCSI do host para habilitar o suporte aos algoritmos seguros.

Durante uma atualização do Element 12,7, se você já atualizou a configuração do iniciador iSCSI do host para enviar uma solicitação de sessão com uma lista que inclui algoritmos SHA, à medida que os nós de storage reiniciam, os novos algoritmos seguros são ativados e sessões iSCSI novas ou reconetadas são 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 a usar o MD5. Posteriormente, depois de atualizar os algoritmos CHAP do iniciador iSCSI do host, as sessões iSCSI devem passar 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 de host padrão no Red Hat Enterprise Linux (RHEL) 8,3 tem a

`node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5` configuração comentada, o que resulta no iniciador iSCSI usando apenas MD5. Descomentando esta configuração no host e reiniciando o iniciador iSCSI aciona sessões iSCSI desse host para começar a usar o SHA3-256.

Se necessário, você pode usar o "Listagens" método API para ver os algoritmos CHAP que estão sendo usados para cada sessão.

Crie uma conta

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

Cada nome de conta no sistema deve ser exclusivo.

1. Selecione **Gestão** > **Contas**.
2. Clique em **criar conta**.
3. Introduza um **Nome de utilizador**.
4. Na seção **CHAP Settings**, insira as seguintes informações:

   Deixe os campos de credencial em branco para gerar automaticamente qualquer senha.

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

Ver detalhes da conta

Você pode visualizar a atividade de desempenho de contas individuais em um formato gráfico.

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

1. Selecione **Gestão** > **Contas**.
2. Clique no ícone ações de uma conta.
3. Clique em **Ver detalhes**.

Aqui estão alguns dos detalhes:

- **Status**: O status da conta. Valores possíveis:
  - Ativo: Uma conta ativa.
  - Bloqueado: Uma conta bloqueada.
  - Removido: Uma conta que foi excluída e eliminada.
- **Volumes ativos**: O número de volumes ativos atribuídos à conta.
- **Compression**: A pontuação de eficiência de compressão para os volumes atribuídos à conta.
- **Desduplicação**: A pontuação de eficiência de desduplicação para os volumes atribuídos à conta.
- **Provisionamento fino**: A pontuação de eficiência de provisionamento fino para os volumes atribuídos à conta.

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

Edite uma conta

Você pode editar uma conta para alterar o status, alterar os segredos CHAP ou modificar 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 verificar se o acesso ao volume não será perdido inesperadamente, efetue sempre logout de sessões iSCSI que serão afetadas por uma alteração de conta ou grupo de acesso e verifique se os iniciadores podem se reconetar aos volumes depois que quaisquer alterações nas configurações do iniciador e nas configurações do cluster tiverem sido concluídas.

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

1. Selecione **Gestão** > **Contas**.
2. Clique no ícone ações de uma conta.
3. No menu resultante, 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** termina todas as conexões iSCSI para a conta e a conta não está mais acessível. Os volumes associados à conta são mantidos; no entanto, os volumes não são detetáveis iSCSI.

6. **Opcional:** em **Configurações CHAP**, edite as credenciais **segredo do Iniciador** e **segredo do alvo** usadas para autenticação de sessão de nó.

   Se você não alterar as credenciais **CHAP Settings**, elas permanecerão as mesmas. Se você deixar os campos de credenciais em branco, o sistema gera novas senhas.

7. Clique em **Salvar alterações**.

Eliminar uma conta

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

Exclua e limpe quaisquer volumes associados à conta antes de excluir a conta.

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

1. Selecione **Gestão** > **Contas**.
2. Clique no ícone ações da conta que deseja excluir.
3. No menu resultante, selecione **Excluir**.
4. Confirme a ação.

Encontre mais informações

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

Gerenciar contas de usuários de administrador 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 configurações LDAP para gerenciar o acesso do sistema para os usuários.

Tipos de conta de administrador de cluster de storage

Existem dois tipos de contas de administrador que podem existir em um cluster de storage que executa o software NetApp Element: A conta de administrador de cluster principal e uma conta de administrador de cluster.

- * Conta de administrador de cluster principal*

  Esta conta de administrador é criada quando o cluster é criado. Esta conta é a conta administrativa primária com o mais alto nível de acesso ao cluster. Essa conta é análoga a um usuário root em um sistema Linux. Pode alterar a palavra-passe desta conta de administrador.

- **Conta de administrador de cluster**

  Você pode dar a uma conta de administrador de cluster um intervalo limitado de acesso administrativo para executar tarefas específicas dentro de um cluster. As credenciais atribuídas a cada conta de administrador de cluster são usadas para autenticar solicitações de API e IU de elementos no sistema de storage.

> É necessária uma conta de administrador de cluster local (não LDAP) para aceder a nós ativos num cluster através da IU por nó. As credenciais da conta não são necessárias para acessar um nó que ainda não faz parte de um cluster.

Exibir detalhes do administrador do cluster

1. Para criar uma conta de administrador de cluster (não LDAP) em todo o cluster, execute as seguintes ações:
   a. Clique em **Users** > **Cluster Admins**.
2. Na página Administradores de cluster da guia usuários, você pode exibir as seguintes informações.
   - **ID**: Número sequencial atribuído à conta de administrador do cluster.
   - **Nome de usuário**: O nome dado à conta de administrador do cluster quando ela foi criada.
   - **Access**: As permissões de usuário atribuídas à conta de usuário. Valores possíveis:
     - leia
     - relatórios
     - nós

- unidades
- volumes
- contas
- ClusterAdmins
- administrador
- SupportAdmin

Todas as permissões estão disponíveis para o tipo de acesso do administrador.

- **Type**: O tipo de administrador de cluster. Valores possíveis:
  - Cluster
  - LDAP
- **Atributos**: Se a conta de administrador de cluster foi criada usando a API Element, essa coluna mostrará os pares nome-valor que foram definidos usando esse método.

  "Referência da API do software NetApp Element"Consulte .

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 definir permissões de conta de administrador de cluster, o sistema concede direitos somente de leitura para quaisquer permissões que você não atribua ao administrador do cluster.

Se pretender criar uma conta de administrador de cluster LDAP, certifique-se de que o LDAP está configurado no cluster antes de começar.

"Ative a autenticação LDAP com a interface do usuário Element"

Mais tarde, você pode alterar o Privileges de contas de administrador de cluster para geração de relatórios, nós, unidades, volumes, contas e acesso em nível de cluster. Quando você ativa 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 selecionou.

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

1. Para criar uma conta de administrador de cluster (não LDAP) em todo o cluster, execute as seguintes ações:
   a. Clique em **Users** > **Cluster Admins**.
   b. Clique em **Create Cluster Admin**.
   c. Selecione o tipo de usuário **Cluster**.
   d. Introduza um nome de utilizador e uma palavra-passe para a conta e confirme a palavra-passe.
   e. Selecione permissões de usuário para aplicar à conta.
   f. Marque a caixa de seleção para concordar com o Contrato de Licença de Usuário final.
   g. Clique em **Create Cluster Admin**.

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 está ativada.

   c. Clique em **testar autenticação do usuário** e copie o nome distinto que aparece para o usuário ou um dos grupos dos quais o usuário é membro para que você possa colá-lo mais tarde.

   d. Clique em **Users** > **Cluster Admins**.

   e. Clique em **Create Cluster Admin**.

   f. Selecione o tipo de utilizador 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 do 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 permissões dessa conta de administrador.

   Para adicionar usuários ou grupos de administrador de cluster LDAP, o formato geral do nome de usuário é "'LDAP: Nome distinto completo>".

   a. Selecione permissões de usuário para aplicar à conta.

   b. Marque a caixa de seleção para concordar com o Contrato de Licença de Usuário final.

   c. Clique em **Create Cluster Admin**.

Editar permissões de administrador do cluster

Você pode alterar o Privileges da conta de administrador do cluster para geração de relatórios, nós, unidades, volumes, contas e acesso em nível de cluster. Quando você ativa 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 selecionou.

1. Clique em **Users** > **Cluster Admins**.
2. Clique no ícone ações do administrador do cluster que deseja editar.
3. Clique em **Editar**.
4. Selecione permissões de usuário para aplicar à conta.
5. Clique em **Salvar alterações**.

Alterar senhas para contas de administrador de cluster

Você pode usar a IU do elemento para alterar as senhas do administrador do cluster.

1. Clique em **Users** > **Cluster Admins**.
2. Clique no ícone ações do administrador do cluster que deseja editar.
3. Clique em **Editar**.
4. No campo alterar palavra-passe, introduza uma nova palavra-passe e confirme-a.
5. Clique em **Salvar alterações**.

Encontre mais informações

- "Ative a autenticação LDAP com a interface do usuário Element"
- "Desativar LDAP"
- "Documentação do software SolidFire e Element"
- "Plug-in do NetApp Element para vCenter Server"

Gerenciar LDAP

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

O gerenciamento do LDAP envolve a configuração da autenticação LDAP em um cluster do SolidFire usando um ambiente existente do Microsoft ative Directory e testar a configuração.

Você pode usar endereços IPv4 e IPv6.

A ativação do LDAP envolve as seguintes etapas de alto nível, descritas em detalhes:

1. **Etapas de pré-configuração completas para suporte LDAP**. Valide que você tem todos os detalhes necessários para configurar a autenticação LDAP.
2. **Ativar autenticação LDAP**. Use a IU do Element ou a API Element.
3. **Validar a configuração LDAP**. Opcionalmente, verifique se o cluster está configurado com os valores corretos executando o método API GetLdapConfiguration ou verificando a configuração LCAP usando a IU do elemento.
4. **Teste a autenticação LDAP** (com o `readonly` usuário). Teste se a configuração LDAP está correta executando o método API TestLdapAuthentication ou usando a IU do Element. Para este teste inicial, use o nome de usuário "AMAccountName" do `readonly` usuário. Isso validará se o cluster está configurado corretamente para autenticação LDAP e também validará se as `readonly` 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 setp 4 com uma conta de usuário que você deseja adicionar como administrador de cluster de elementos. Copie o `distinguished` nome (DN) ou o usuário (ou o grupo). Este DN será utilizado no passo 6.
6. **Adicione o administrador do cluster LDAP** (copie e cole o DN da etapa de autenticação LDAP de teste). Usando a IU do Element ou o método da API AddLdapClusterAdmin, crie um novo usuário de administrador de cluster com o nível de acesso apropriado. Para o nome de usuário, cole no 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 de administrador de cluster LDAP recém-criado. Se tiver adicionado um grupo LDAP, pode iniciar sessão como qualquer utilizador nesse grupo.

Conclua as etapas de pré-configuração para suporte a LDAP

Antes de ativar o suporte LDAP no Element, você deve configurar um Windows ative Directory Server e executar outras tarefas de pré-configuração.

Passos

1. Configurar um Windows ative Directory Server.
2. * Opcional: * Ativar suporte LDAPS.
3. Crie usuários e grupos.
4. Crie uma conta de serviço somente leitura (como "somente leitura") a ser usada para pesquisar o diretório LDAP.

Ative a autenticação LDAP com a interface do usuário Element

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

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

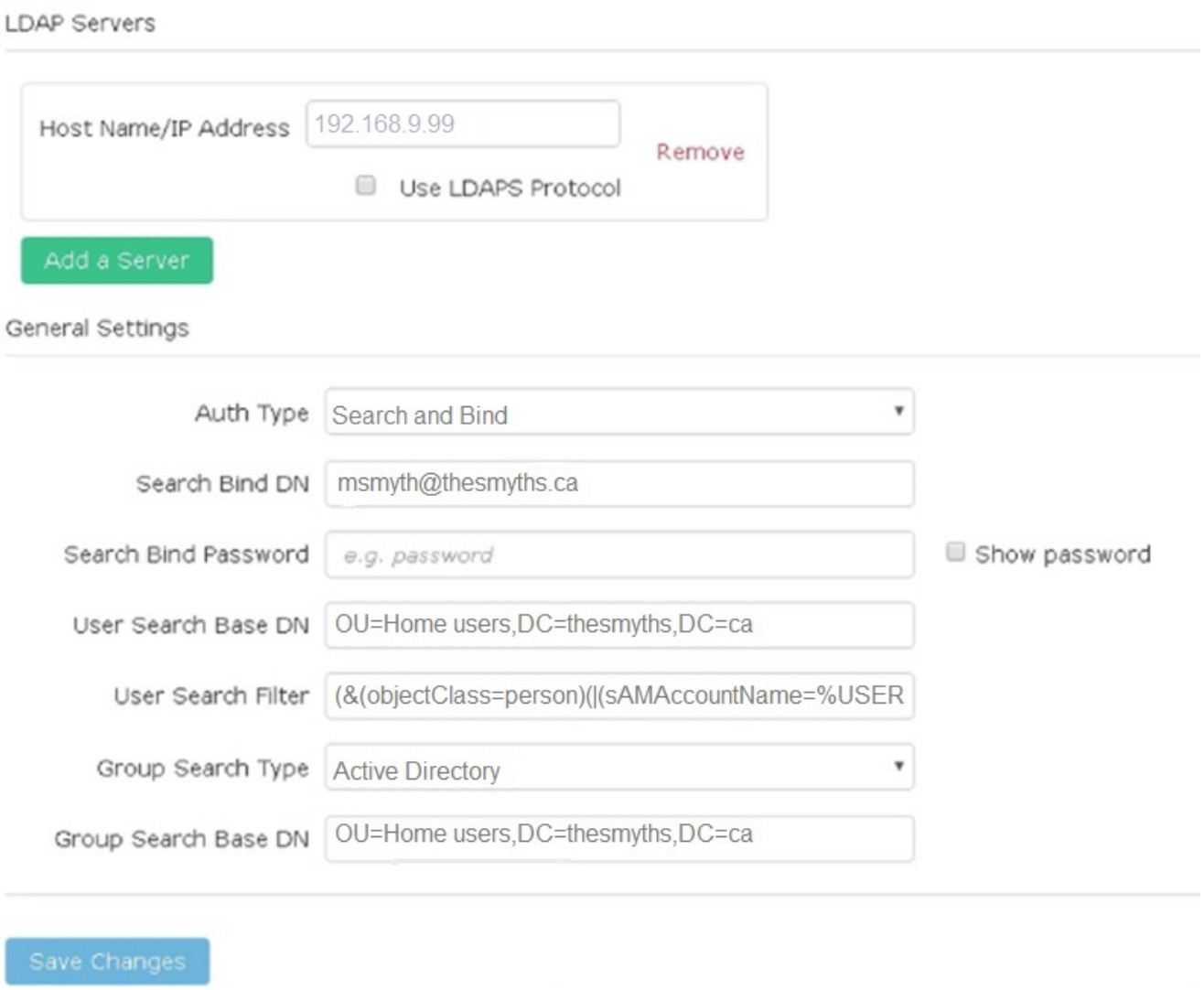
Este exemplo mostra como configurar a autenticação LDAP no SolidFire e usa `SearchAndBind` como o tipo de autenticação. O exemplo usa um único servidor ative Directory do Windows Server 2012 R2.

Passos

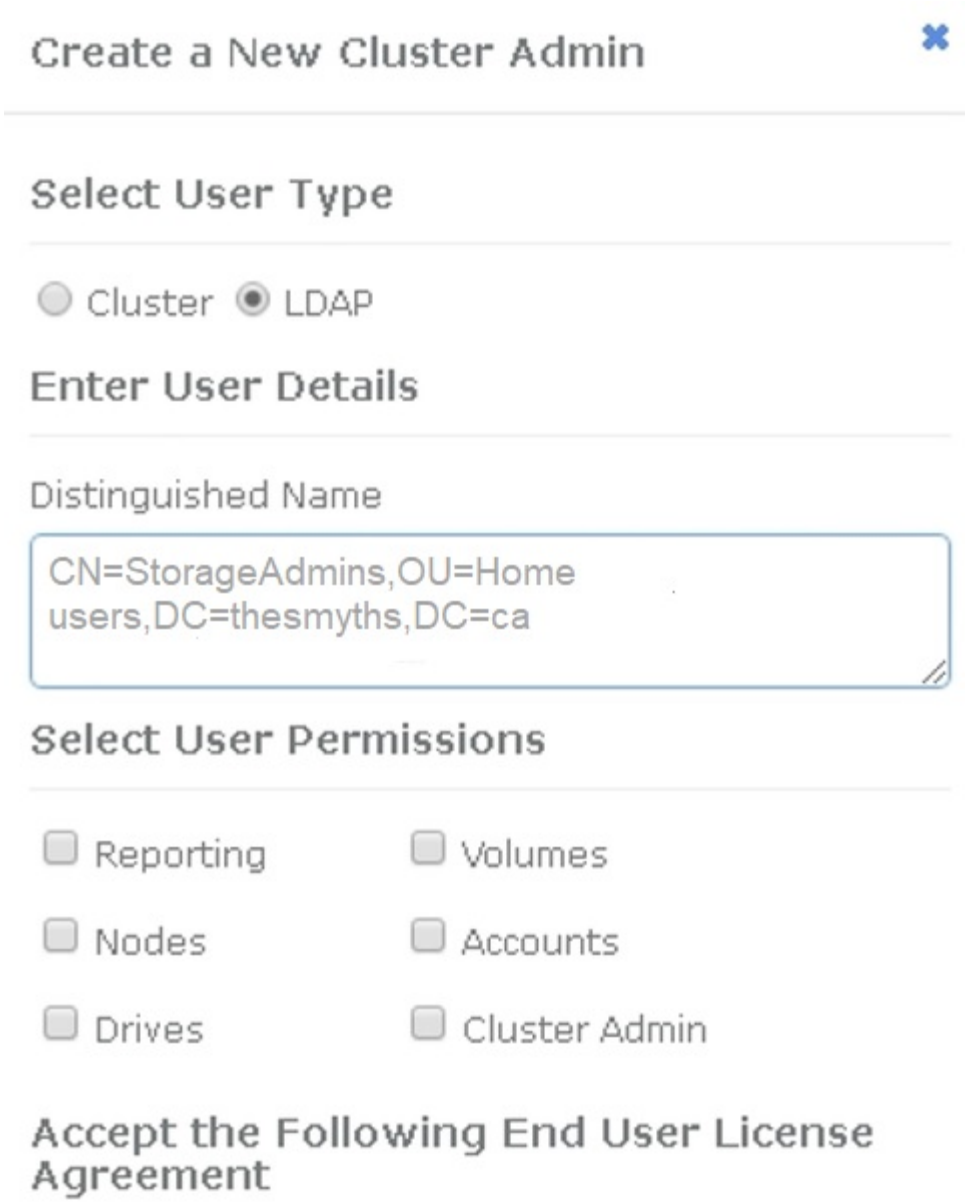
1. Clique em **Cluster** > **LDAP**.
2. Clique em **Yes** para ativar a autenticação LDAP.
3. Clique em **Adicionar um servidor**.
4. Introduza o **Nome do anfitrião/endereço IP**.

   Um número de porta personalizado opcional também pode ser inserido.

   Por exemplo, para adicionar um número de porta personalizado, introduza [nome do anfitrião ou endereço ip>:<port number>
5. **Opcional:** Selecione **Use LDAPS Protocol**.
6. Insira as informações necessárias em **Configurações gerais**.



7. Clique em **Ativar LDAP**.
8. Clique em **Test User Authentication** (testar autenticação do utilizador) se pretender testar o acesso ao servidor de um utilizador.
9. Copie o nome distinto e as informações do grupo de usuários que aparecem para uso posterior ao criar 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 o seguinte:
    a. Clique em **User** > **View**.



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 para baixo até o Contrato de Licença de Usuário final e clique em **Aceito**.
e. Clique em **Create Cluster Admin**.

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

Para testar isso, faça logout da IU do Element e faça login novamente como um usuário nesse grupo.

Ative a autenticação LDAP com a API Element

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

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

Para utilizar a autenticação LDAP num cluster SolidFire, ative primeiro a autenticação LDAP no cluster utilizando o `EnableLdapAuthentication` método API.

Passos

1. Ative a autenticação LDAP primeiro no cluster usando o `EnableLdapAuthentication` método API.
2. Introduza as informações necessárias.

```
{
     "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 readonly para primeiro procurar o usuário que está sendo autenticado e, posteriormente, vincular esse usuário se for encontrado e autenticado.
GroupSearchBaseDN: dc-prodtest,dc-SolidFire,DC-net	Especifica a localização na árvore LDAP para começar a procurar grupos. Para este exemplo, usamos a raiz da nossa árvore. Se a árvore LDAP for muito grande, talvez você queira definir isso como uma subárvore mais granular para diminuir os tempos de pesquisa.
UserSearchBaseDN: dc-prodtest,dc-SolidFire,DC-NET	Especifica a localização na árvore LDAP para começar a procurar usuários. Para este exemplo, usamos a raiz da nossa árvore. Se a árvore LDAP for muito grande, talvez você queira definir isso como uma subárvore mais granular para diminuir os tempos de pesquisa.

Parâmetros utilizados	Descrição
GroupSearchType: ActiveDirectory	Usa o servidor do ative Directory do Windows 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 userPrincipalName e sAMAccountName, você pode usar o seguinte userSearchFilter:
 	
`"(&(objectClass=person)(`
	(SAMAccountName) (userPrincipalName:%USERNAME%))" ----

Aproveita o sAMAccountName como nosso nome de usuário para fazer login no cluster do SolidFire. Essas configurações dizem ao LDAP que procure o nome de usuário especificado durante o login no atributo sAMAccountName e também limitam a pesquisa a entradas que têm "'pessoa'" como um valor no atributo objectClass.	SearchBindDN
Este é o nome distinto do usuário readonly que será usado para pesquisar o diretório LDAP. Para o diretório ativo, geralmente é mais fácil usar o userPrincipalName (formato de endereço de e-mail) para o usuário.	SearchBindPassword

Para testar isso, faça logout da IU do Element e faça login novamente como um usuário nesse grupo.

Ver detalhes do LDAP

Exibir informações LDAP na página LDAP na guia Cluster.

Tem de ativar o LDAP para visualizar estas definições de configuração LDAP.

1. Para exibir detalhes do LDAP com a IU do Element, clique em **Cluster** > **LDAP**.

- **Nome do host/endereço IP**: Endereço de um servidor de diretório LDAP ou LDAPS.
- **Auth Type**: O método de autenticação do usuário. Valores possíveis:
  - Ligação direta
  - Pesquisa e Bind
- **Pesquisar DN**: Um DN totalmente qualificado para fazer login para realizar uma pesquisa LDAP para o usuário (precisa de acesso ao diretório LDAP).
- **Pesquisar vincular senha**: Senha usada para autenticar o acesso ao servidor LDAP.
- **User Search base DN**: O DN base da árvore usada para iniciar a pesquisa do usuário. O sistema procura a subárvore a partir da localização especificada.
- **Filtro de pesquisa do usuário**: Insira o seguinte usando seu nome de domínio:

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

- **Tipo de pesquisa de grupo**: Tipo de pesquisa que controla o filtro de pesquisa de grupo padrão usado. Valores possíveis:
  - Ative Directory: Associação aninhada de todos os grupos LDAP de um usuário.
  - Sem grupos: Sem apoio de grupo.
  - DN do Membro: Grupos do tipo DN do Membro (nível único).
- **Group Search base DN**: O DN base da árvore usado para iniciar a pesquisa de grupo. O sistema procura a subárvore a partir da localização especificada.
- **Testar autenticação do usuário**: Depois que o LDAP estiver configurado, use-o para testar a autenticação do nome de usuário e senha para o servidor LDAP. Insira uma conta que já existe para testar isso. As informações de nome distinto e grupo de usuários são exibidas, que você pode copiar para uso posterior ao criar administradores de cluster.

Teste a configuração LDAP

Depois de configurar o LDAP, você deve testá-lo usando a IU do Element ou o método da API Element `TestLdapAuthentication`.

Passos

1. Para testar a configuração LDAP com a IU do Element, faça o seguinte:
   a. Clique em **Cluster** > **LDAP**.
   b. Clique em **Test LDAP Authentication** (testar autenticação LDAP).
   c. Resolva quaisquer problemas usando as informações na tabela abaixo:

Mensagem de erro	Descrição
`xLDAPUserNotFound`	• O usuário que está sendo testado não foi encontrado na subárvore configurada `userSearchBaseDN`. • O `userSearchFilter` está configurado incorretamente.

Mensagem de erro	Descrição
`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 utilizador que está a ser testado é um utilizador 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 utilizador ou palavra-passe só de leitura está configurado 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. • Os `userSearchBaseDN` e `groupSearchBaseDN` estão em uma ou aninhada. Isso pode causar problemas de permissão. A solução alternativa é incluir a UO nas entradas DN de base de usuário e 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. Reveja os resultados. Se a chamada de API for bem-sucedida, os resultados incluem o nome distinto

do usuário especificado e uma lista de grupos nos 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 IU do Element.

Antes de começar, deve anotar todas as definições de configuração, porque a desativação do LDAP apaga todas as definições.

Passos

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

Encontre mais informações

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

Informações sobre direitos autorais

Informações sobre marcas comerciais