# Instalar e configurar o SnapCenter Server

SnapCenter software

NetApp
November 06, 2025

# Índice

# Instalar e configurar o SnapCenter Server

## Prepare-se para instalar o SnapCenter Server

### Requisitos para instalar o SnapCenter Server

Antes de instalar o SnapCenter Server em um host Windows ou Linux, você deve revisar e garantir que todos os requisitos sejam atendidos para seu ambiente.

#### Requisitos de domínio e grupo de trabalho para host Windows

O SnapCenter Server pode ser instalado em um host Windows que esteja em um domínio ou em um grupo de trabalho.

O usuário com privilégios de administrador tem permissão para instalar o servidor SnapCenter .

- Domínio do Active Directory: você deve usar um usuário de domínio com direitos de administrador local. O usuário do domínio deve ser membro do grupo Administrador local no host Windows.
- Grupos de trabalho: você deve usar uma conta local que tenha direitos de administrador local.

Embora relações de confiança de domínio, florestas multidomínio e relações de confiança entre domínios sejam suportadas, domínios entre florestas não são suportados. A documentação da Microsoft sobre domínios e relações de confiança do Active Directory contém mais informações.

Após instalar o SnapCenter Server, você não deve alterar o domínio no qual o host SnapCenter está localizado. Se você remover o host do SnapCenter Server do domínio em que ele estava quando o SnapCenter Server foi instalado e tentar desinstalar o SnapCenter Server, a operação de desinstalação falhará.

#### Requisitos de espaço e dimensionamento

Você deve estar familiarizado com os requisitos de espaço e dimensionamento.

| Item | Requisitos do host do Windows | Requisitos do host Linux |
|---|---|---|
| Sistemas Operacionais | Microsoft Windows<br><br>Somente as versões em inglês, alemão, japonês e chinês simplificado dos sistemas operacionais são suportadas.<br><br>Para obter as informações mais recentes sobre as versões suportadas, consultehttps://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT["Ferramenta de Matriz de Interoperabilidade da NetApp"^] . | • Red Hat Enterprise Linux (RHEL) 8 e 9<br>• Servidor SUSE Linux Enterprise (SLES) 15<br><br>Para obter as informações mais recentes sobre as versões suportadas, consultehttps://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT["Ferramenta de Matriz de Interoperabilidade da NetApp"^] . |

| Item | Requisitos do host do Windows | Requisitos do host Linux |
| --- | --- | --- |
| Contagem mínima de CPU | 4 núcleos | 4 núcleos |
| RAM mínima | 8 GB<br>O pool de buffer do servidor MySQL usa 20% da RAM total. | 8 GB |
| Espaço mínimo no disco rígido para o software e logs do SnapCenter Server | 7 GB<br>Se você tiver o repositório SnapCenter na mesma unidade onde o SnapCenter Server está instalado, é recomendável ter 15 GB. | 15 GB |
| Espaço mínimo no disco rígido para o repositório SnapCenter | 8 GB<br>OBSERVAÇÃO: se você tiver o SnapCenter Server na mesma unidade onde o repositório do SnapCenter está instalado, é recomendável ter 15 GB. | Não aplicável |

| Item | Requisitos do host do Windows | Requisitos do host Linux |
| --- | --- | --- |
| Pacotes de software necessários | • Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes)<br>• PowerShell 7.4.2 ou posterior<br><br>Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet" . | • .NET Framework 8.0.12 (e todos os patches 8.0.x subsequentes)<br>• PowerShell 7.4.2 ou posterior<br>• Nginx é um servidor web que pode ser usado como um proxy reverso<br>• Pam-devel<br><br>PAM (Pluggable Authentication Modules) é uma ferramenta de segurança do sistema que permite que os administradores de sistema definam políticas de autenticação sem precisar recompilar programas que fazem autenticação. |

O ASP.NET Core precisa do IIS_IUSRS para acessar o sistema de arquivos temporário no SnapCenter Server no Windows.

### Requisitos do host SAN

O SnapCenter não inclui utilitários de host ou um DSM. Se o host SnapCenter fizer parte de um ambiente SAN (FC/iSCSI), talvez seja necessário instalar e configurar software adicional no host do SnapCenter Server.

- Utilitários de host: Os utilitários de host oferecem suporte a FC e iSCSI e permitem que você use MPIO em seus servidores Windows. "Saber mais" .
- Microsoft DSM para Windows MPIO: Este software funciona com drivers Windows MPIO para gerenciar vários caminhos entre computadores host NetApp e Windows. Um DSM é necessário para configurações de alta disponibilidade.

Se você estava usando o ONTAP DSM, você deve migrar para o Microsoft DSM. Para obter mais informações, consulte "Como migrar do ONTAP DSM para o Microsoft DSM" .

### Requisitos do navegador

O SnapCenter software é compatível com o Chrome 125 e posteriores e o Microsoft Edge 110.0.1587.17 e posteriores.

### Requisitos portuários

O SnapCenter software requer portas diferentes para comunicação entre diferentes componentes.

- Os aplicativos não podem compartilhar uma porta.
- Para portas personalizáveis, você pode selecionar uma porta personalizada durante a instalação se não quiser usar a porta padrão.

- Para portas fixas, você deve aceitar o número de porta padrão.
- Firewalls
  - Firewalls, proxies ou outros dispositivos de rede não devem interferir nas conexões.
  - Se você especificar uma porta personalizada ao instalar o SnapCenter, deverá adicionar uma regra de firewall no host do plug-in para essa porta para o SnapCenter Plug-in Loader.

A tabela a seguir lista as diferentes portas e seus valores padrão.

| Nome da porta | Números de porta | Protocolo | Direção | Descrição |
|---|---|---|---|---|
| Porta da web do SnapCenter | 8146 | HTTPS | Bidirecional | Esta porta é usada para comunicação entre o cliente SnapCenter (o usuário SnapCenter ) e o SnapCenter Server e também é usada para comunicação dos hosts de plug-in com o SnapCenter Server.<br><br>Você pode personalizar o número da porta. |
| Porta de comunicação SnapCenter SMCore | 8145 | HTTPS | Bidirecional | Esta porta é usada para comunicação entre o SnapCenter Server e os hosts onde os plug-ins do SnapCenter estão instalados.<br><br>Você pode personalizar o número da porta. |

| Nome da porta | Números de porta | Protocolo | Direção | Descrição |
|---|---|---|---|---|
| Porta de serviço do agendador | 8154 | HTTPS | | Esta porta é usada para orquestrar os fluxos de trabalho do agendador do SnapCenter para todos os plug-ins gerenciados no host do servidor SnapCenter de maneira centralizada.<br><br>Você pode personalizar o número da porta. |
| Porta RabbitMQ | 5672 | TCP | | Esta é a porta padrão na qual o RabbitMQ escuta e é usada para comunicação do modelo publicador-assinante entre o serviço Scheduler e o SnapCenter. |
| Porta MySQL | 3306 | HTTPS | | A porta é usada para comunicação com o banco de dados do repositório SnapCenter . Você pode criar conexões seguras do SnapCenter Server para o servidor MySQL."Saber mais" |
| Hosts de plug-ins do Windows | 135, 445 | TCP | | Esta porta é usada para comunicação entre o SnapCenter Server e o host no qual o plug-in está sendo instalado. O intervalo de portas dinâmicas adicionais especificado pela Microsoft também deve ser aberto. |

| Nome da porta | Números de porta | Protocolo | Direção | Descrição |
|---|---|---|---|---|
| Hosts de plug-in Linux ou AIX | 22 | SSH | Unidirecional | Esta porta é usada para comunicação entre o SnapCenter Server e o host, iniciada do servidor para o host cliente. |
| Pacote de plug-ins SnapCenter para Windows, Linux ou AIX | 8145 | HTTPS | Bidirecional | Esta porta é usada para comunicação entre o SMCore e os hosts onde o pacote de plug-ins está instalado. Personalizável.<br><br>Você pode personalizar o número da porta. |
| Plug-in SnapCenter para banco de dados Oracle | 27216 | | | A porta JDBC padrão é usada pelo plug-in para Oracle para conexão ao banco de dados Oracle. |
| Plug-in SnapCenter para banco de dados Exchange | 909 | | | A porta NET.TCP padrão é usada pelo plug-in para Windows para conexão aos retornos de chamada do Exchange VSS. |
| Plug-ins compatíveis com a NetApp para SnapCenter | 9090 | HTTPS | | Esta é uma porta interna usada somente no host do plug-in; nenhuma exceção de firewall é necessária.<br><br>A comunicação entre o SnapCenter Server e os plug-ins é roteada pela porta 8145. |

| Nome da porta | Números de porta | Protocolo | Direção | Descrição |
| --- | --- | --- | --- | --- |
| Cluster ONTAP ou porta de comunicação SVM | • 443 (HTTPS)<br>• 80 (HTTP) | • HTTPS<br>• HTTP | Bidirecional | A porta é usada pelo SAL (Storage Abstraction Layer) para comunicação entre o host que executa o SnapCenter Server e o SVM. Atualmente, a porta também é usada pelo SAL nos hosts do plug-in SnapCenter for Windows para comunicação entre o host do plug-in SnapCenter e o SVM. |
| Plug-in SnapCenter para banco de dados SAP HANA | • 3instance_number13<br>• 3instance_number15 | • HTTPS<br>• HTTP | Bidirecional | Para um contêiner de banco de dados multilocatário (MDC) de locatário único, o número da porta termina em 13; para um não MDC, o número da porta termina em 15.<br><br>Você pode personalizar o número da porta. |
| Plug-in SnapCenter para PostgreSQL | 5432 | | | Esta porta é a porta padrão do PostgreSQL usada para comunicação do plug-in do PostgreSQL com o cluster do PostgreSQL.<br><br>Você pode personalizar o número da porta. |

## Registre-se para acessar o SnapCenter software

Você deve se registrar para acessar o SnapCenter software se for novo no Amazon FSx for NetApp ONTAP ou Azure NetApp Files e não tiver uma conta NetApp existente.

**Antes de começar**

- Você deve ter acesso ao ID de e-mail corporativo.
- Se você estiver usando o Azure NetApp Files, deverá ter o ID de assinatura do Azure.
- Se estiver usando o Amazon FSx for NetApp ONTAP, você deverá ter o ID do sistema de arquivos do seu sistema de arquivos FSx para ONTAP .

**Sobre esta tarefa**

Seu registro está sujeito a validações de informações e pode levar até um dia para confirmar e atualizar a nova conta do NetApp Support Site (NSS) para acesso **total** a partir do acesso **de convidado**.

**Passos**

1. Clique https://mysupport.netapp.com/site/user/registration para registro.
2. Insira seu ID de e-mail corporativo, preencha o captcha, aceite a política de privacidade da NetApp e clique em **Enviar**.
3. Autentique o registro inserindo o OTP enviado para seu ID de e-mail e clique em **Continuar**.
4. Na página de conclusão do registro, insira os seguintes detalhes para concluir o registro.
   a. Selecione * Cliente NetApp / Usuário final*.
   b. No campo NÚMERO DE SÉRIE, insira a ID da assinatura do Azure se estiver usando o Azure NetApp Files ou a ID do sistema de arquivos se estiver usando o Amazon FSx for NetApp ONTAP.

Você pode abrir um tíquete em https://mysupport.netapp.com/site/help se você enfrentar algum problema durante o registro ou para saber o status.

## Autenticação multifator (MFA)

### Gerenciar autenticação multifator (MFA)

Você pode gerenciar a funcionalidade de autenticação multifator (MFA) no servidor do Serviço de Federação do Active Directory (AD FS) e no SnapCenter Server.

#### Habilitar autenticação multifator (MFA)

Você pode habilitar a funcionalidade MFA para o SnapCenter Server usando comandos do PowerShell.

**Sobre esta tarefa**

- O SnapCenter oferece suporte a logins baseados em SSO quando outros aplicativos são configurados no mesmo AD FS. Em determinadas configurações do AD FS, o SnapCenter pode exigir autenticação do usuário por motivos de segurança, dependendo da persistência da sessão do AD FS.
- As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando `Get-Help command_name` . Alternativamente, você também pode ver "Guia de referência do cmdlet do software SnapCenter" .

**Antes de começar**

- O Serviço de Federação do Active Directory (AD FS) do Windows deve estar ativo e em execução no respectivo domínio.
- Você deve ter um serviço de autenticação multifator compatível com AD FS, como Azure MFA, Cisco Duo e assim por diante.

- O registro de data e hora do servidor SnapCenter e AD FS deve ser o mesmo, independentemente do fuso horário.
- Obtenha e configure o certificado de CA autorizado para o SnapCenter Server.

  O Certificado CA é obrigatório pelos seguintes motivos:

  - Garante que as comunicações ADFS-F5 não sejam interrompidas porque os certificados autoassinados são exclusivos no nível do nó.
  - Garante que durante a atualização, o reparo ou a recuperação de desastres (DR) em uma configuração autônoma ou de alta disponibilidade, o certificado autoassinado não seja recriado, evitando assim a reconfiguração do MFA.
  - Garante resoluções IP-FQDN.

    Para obter informações sobre o certificado CA, consulte"Gerar arquivo CSR de certificado CA" .

**Passos**

1. Conecte-se ao host dos Serviços de Federação do Active Directory (AD FS).
2. Baixe o arquivo de metadados da federação do AD FS em"https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml".
3. Copie o arquivo baixado para o SnapCenter Server para habilitar o recurso MFA.
4. Efetue login no SnapCenter Server como usuário administrador do SnapCenter por meio do PowerShell.
5. Usando a sessão do PowerShell, gere o arquivo de metadados do SnapCenter MFA usando o cmdlet *New-SmMultifactorAuthenticationMetadata -path*.

   O parâmetro path especifica o caminho para salvar o arquivo de metadados MFA no host do SnapCenter Server.
6. Copie o arquivo gerado para o host do AD FS para configurar o SnapCenter como a entidade do cliente.
7. Habilite o MFA para o SnapCenter Server usando o `Set-SmMultiFactorAuthentication` cmdlet.
8. (Opcional) Verifique o status e as configurações da configuração do MFA usando `Get-SmMultiFactorAuthentication` cmdlet.
9. Acesse o console de gerenciamento da Microsoft (MMC) e execute as seguintes etapas:
   a. Clique em **Arquivo** > **Adicionar/Remover Snapin**.
   b. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
   c. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
   d. Clique em **Console Root** > **Certificados – Computador local** > **Pessoal** > **Certificados**.
   e. Clique com o botão direito do mouse no certificado CA vinculado ao SnapCenter e selecione **Todas as tarefas** > **Gerenciar chaves privadas**.
   f. No assistente de permissões, execute as seguintes etapas:
      i. Clique em **Adicionar**.
      ii. Clique em **Locais** e selecione o host em questão (topo da hierarquia).
      iii. Clique em **OK** na janela pop-up **Locais**.
      iv. No campo de nome do objeto, digite 'IIS_IUSRS', clique em **Verificar nomes** e clique em **OK**.

Se a verificação for bem-sucedida, clique em **OK**.

10. No host do AD FS, abra o assistente de gerenciamento do AD FS e execute as seguintes etapas:
    a. Clique com o botão direito em **Relying Party Trusts** > **Adicionar Relying Party Trust** > **Iniciar**.
    b. Selecione a segunda opção, navegue pelo arquivo de metadados do SnapCenter MFA e clique em **Avançar**.
    c. Especifique um nome de exibição e clique em **Avançar**.
    d. Escolha uma política de controle de acesso conforme necessário e clique em **Avançar**.
    e. Selecione as configurações na próxima aba como padrão.
    f. Clique em **Concluir**.

    O SnapCenter agora é refletido como uma parte confiável com o nome de exibição fornecido.

11. Selecione o nome e execute os seguintes passos:
    a. Clique em **Editar política de emissão de reivindicações**.
    b. Clique em **Adicionar regra** e clique em **Avançar**.
    c. Especifique um nome para a regra de reivindicação.
    d. Selecione **Active Directory** como o armazenamento de atributos.
    e. Selecione o atributo como **User-Principal-Name** e o tipo de declaração de saída como **Name-ID**.
    f. Clique em **Concluir**.
12. Execute os seguintes comandos do PowerShell no servidor ADFS.

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-SigningCertificateRevocationCheck None

Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-EncryptionCertificateRevocationCheck None
```

13. Execute as seguintes etapas para confirmar se os metadados foram importados com sucesso.
    a. Clique com o botão direito do mouse na parte confiável e selecione **Propriedades**.
    b. Certifique-se de que os campos Endpoints, Identificadores e Assinatura estejam preenchidos.
14. Feche todas as abas do navegador e abra-o novamente para limpar os cookies de sessão existentes ou ativos e faça login novamente.

A funcionalidade SnapCenter MFA também pode ser habilitada usando APIs REST.

Para obter informações sobre solução de problemas, consulte "Tentativas simultâneas de login em várias guias mostram erro de MFA" .

#### Atualizar metadados do AD FS MFA

Você deve atualizar os metadados do AD FS MFA no SnapCenter sempre que houver qualquer modificação no servidor AD FS, como atualização, renovação de certificado CA, DR e assim por diante.

**Passos**

1. Baixe o arquivo de metadados da federação do AD FS em"https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"

2. Copie o arquivo baixado para o SnapCenter Server para atualizar a configuração do MFA.
3. Atualize os metadados do AD FS no SnapCenter executando o seguinte cmdlet:

   ```
   Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
   ```

4. Feche todas as abas do navegador e abra-o novamente para limpar os cookies de sessão existentes ou ativos e faça login novamente.

#### Atualizar metadados do SnapCenter MFA

Você deve atualizar os metadados do SnapCenter MFA no AD FS sempre que houver qualquer modificação no servidor ADFS, como reparo, renovação de certificado CA, DR e assim por diante.

**Passos**

1. No host do AD FS, abra o assistente de gerenciamento do AD FS e execute as seguintes etapas:
   a. Selecione **Relying Party Trusts**.
   b. Clique com o botão direito do mouse na parte confiável que foi criada para o SnapCenter e selecione **Excluir**.

      O nome definido pelo usuário da parte confiável será exibido.

   c. Habilite a autenticação multifator (MFA).

      Ver "Habilitar autenticação multifator" .
2. Feche todas as abas do navegador e abra-o novamente para limpar os cookies de sessão existentes ou ativos e faça login novamente.

#### Desativar autenticação multifator (MFA)

**Passos**

1. Desabilite o MFA e limpe os arquivos de configuração que foram criados quando o MFA foi habilitado usando o `Set-SmMultiFactorAuthentication` cmdlet.
2. Feche todas as abas do navegador e abra-o novamente para limpar os cookies de sessão existentes ou ativos e faça login novamente.

### Gerenciar autenticação multifator (MFA) usando Rest API, PowerShell e SCCLI

O login MFA é compatível com navegador, API REST, PowerShell e SCCLI. O MFA é suportado por um gerenciador de identidade do AD FS. Você pode habilitar o MFA, desabilitar o MFA e configurar o MFA a partir da GUI, API REST, PowerShell e SCCLI.

#### Configurar o AD FS como OAuth/OIDC

**Configurar o AD FS usando o assistente da GUI do Windows**

1. Navegue até **Painel do Gerenciador de Servidores** > **Ferramentas** > **Gerenciamento do ADFS**.
2. Navegue até **ADFS** > **Grupos de Aplicativos**.
   a. Clique com o botão direito do mouse em **Grupos de aplicativos**.
   b. Selecione **Adicionar grupo de aplicativos** e insira **Nome do aplicativo**.

c. Selecione **Aplicativo do Servidor**.

d. Clique em **Avançar**.

3. Copie **Identificador do Cliente**.

   Este é o ID do cliente. .. Adicione URL de retorno de chamada (URL do SnapCenter Server) na URL de redirecionamento. .. Clique em **Avançar**.

4. Selecione **Gerar segredo compartilhado**.

   Copie o valor secreto. Este é o segredo do cliente. .. Clique em **Avançar**.

5. Na página **Resumo**, clique em **Avançar**.

   a. Na página **Concluído**, clique em **Fechar**.

6. Clique com o botão direito do mouse no **Grupo de Aplicativos** recém-adicionado e selecione **Propriedades**.

7. Selecione **Adicionar aplicativo** em Propriedades do aplicativo.

8. Clique em **Adicionar aplicativo**.

   Selecione Web API e clique em **Avançar**.

9. Na página Configurar API da Web, insira a URL do SnapCenter Server e o Identificador do Cliente criados na etapa anterior na seção Identificador.

   a. Clique em **Adicionar**.

   b. Clique em **Avançar**.

10. Na página **Escolher política de controle de acesso**, selecione a política de controle com base em suas necessidades (por exemplo, Permitir todos e exigir MFA) e clique em **Avançar**.

11. Na página **Configurar permissão do aplicativo**, por padrão o openid é selecionado como um escopo, clique em **Avançar**.

12. Na página **Resumo**, clique em **Avançar**.

    Na página **Concluído**, clique em **Fechar**.

13. Na página **Propriedades do aplicativo de exemplo**, clique em **OK**.

14. Token JWT emitido por um servidor de autorização (AD FS) e destinado a ser consumido pelo recurso.

    A declaração 'aud' ou de público deste token deve corresponder ao identificador do recurso ou da API da Web.

15. Edite a WebAPI selecionada e verifique se o URL de retorno de chamada (URL do SnapCenter Server) e o identificador do cliente foram adicionados corretamente.

    Configure o OpenID Connect para fornecer um nome de usuário como declarações.

16. Abra a ferramenta **Gerenciamento do AD FS** localizada no menu **Ferramentas** no canto superior direito do Gerenciador do Servidor.

    a. Selecione a pasta **Grupos de Aplicativos** na barra lateral esquerda.

    b. Selecione a API da Web e clique em **EDITAR**.

    c. Guia de regras de transformação de emissão

17. Clique em **Adicionar regra**.
    a. Selecione **Enviar atributos LDAP como declarações** no menu suspenso Modelo de regra de declaração.
    b. Clique em **Avançar**.
18. Digite o nome da **Regra de reivindicação**.
    a. Selecione **Active Directory** no menu suspenso Armazenamento de atributos.
    b. Selecione **Nome-Principal-do-Usuário** no menu suspenso **Atributo LDAP** e **UPN** no menu suspenso Tipo de Reivindicação de Saída*.
    c. Clique em **Concluir**.

#### Criar grupo de aplicativos usando comandos do PowerShell

Você pode criar o grupo de aplicativos, a API da Web e adicionar o escopo e as declarações usando comandos do PowerShell. Esses comandos estão disponíveis em formato de script automatizado. Para mais informações, consulte <link para o artigo da KB>.

1. Crie o novo Grupo de Aplicativos no AD FS usando o seguinte comando.

   ```
   New-AdfsApplicationGroup -Name $ClientRoleIdentifier
   -ApplicationGroupIdentifier $ClientRoleIdentifier
   ```

   `ClientRoleIdentifier`nome do seu grupo de aplicação

   `redirectURL`URL válida para redirecionamento após autorização

2. Crie o aplicativo do servidor AD FS e gere o segredo do cliente.

   ```
   Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"
   -ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL
   -Identifier $identifier -GenerateClientSecret
   ```

3. Crie o aplicativo ADFS Web API e configure o nome da política que ele deve usar.

   ```
   $identifier = (New-Guid).Guid

   Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
   -Name "App Web API"

   -Identifier $identifier -AccessControlPolicyName "Permit everyone"
   ```

4. Obtenha o ID do cliente e o segredo do cliente da saída dos comandos a seguir, pois eles são exibidos apenas uma vez.

   ```
   "client_id = $identifier"

   "client_secret: "$($ADFSApp.ClientSecret)
   ```

5. Conceda ao aplicativo AD FS as permissões allatclaims e openid.

   ```
   Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
   -ServerRoleIdentifier $identifier -ScopeNames @('openid')
   ```

```
$transformrule = @"

@RuleTemplate = "LdapClaims"

@RuleName = "AD User properties and Groups"

c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer ==

"AD AUTHORITY"]

⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. Escreva o arquivo de regras de transformação.

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii $relativePath = Get-Item .\issueancetransformrules.tmp
```

7. Nomeie o aplicativo Web API e defina suas regras de transformação de emissão usando um arquivo externo.

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

#### Atualizar tempo de expiração do token de acesso

Você pode atualizar o tempo de expiração do token de acesso usando o comando do PowerShell.

**Sobre esta tarefa**

- Um token de acesso pode ser usado somente para uma combinação específica de usuário, cliente e recurso. Os tokens de acesso não podem ser revogados e são válidos até expirarem.
- Por padrão, o tempo de expiração de um token de acesso é de 60 minutos. Este tempo mínimo de expiração é suficiente e dimensionado. Você deve fornecer valor suficiente para evitar quaisquer trabalhos críticos para os negócios em andamento.

**Etapa**

Para atualizar o tempo de expiração do token de acesso para um grupo de aplicativos WebApi, use o seguinte comando no servidor AD FS.

+ `Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"`

#### Obter o token do portador do AD FS

Você deve preencher os parâmetros mencionados abaixo em qualquer cliente REST (como o Postman) e ele solicitará que você preencha as credenciais do usuário. Além disso, você deve inserir a autenticação de segundo fator (algo que você tem e algo que você é) para obter o token do portador.

+ A validade do token portador é configurável no servidor AD FS por aplicativo e o período de validade padrão é de 60 minutos.

| Campo | Valor |
|---|---|
| Tipo de subsídio | Código de autorização |
| URL de retorno de chamada | Insira a URL base do seu aplicativo se você não tiver uma URL de retorno de chamada. |
| URL de autenticação | [adfs-nome-de-domínio]/adfs/oauth2/autorizar |
| URL do token de acesso | [nome-de-domínio-adfs]/adfs/oauth2/token |
| ID do cliente | Insira o ID do cliente do AD FS |
| Segredo do cliente | Digite o segredo do cliente do AD FS |
| Escopo | OpenID |
| Autenticação do cliente | Enviar como cabeçalho AUTH básico |
| Recurso | Na aba **Opções Avançadas**, adicione o campo Recurso com o mesmo valor que o URL de retorno de chamada, que vem como um valor “aud” no token JWT. |

### Configurar MFA no SnapCenter Server usando PowerShell, SCCLI e REST API

Você pode configurar o MFA no SnapCenter Server usando PowerShell, SCCLI e REST API.

#### Autenticação SnapCenter MFA CLI

No PowerShell e no SCCLI, o cmdlet existente (Open-SmConnection) é estendido com mais um campo chamado "AccessToken" para usar o token do portador para autenticar o usuário.

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port
<String>] [-RoleName <String>] [ -AccessToken <string>]
```

Após a execução do cmdlet acima, uma sessão é criada para o respectivo usuário executar outros cmdlets do SnapCenter .

#### Autenticação SnapCenter MFA Rest API

Use o token portador no formato *Authorization=Bearer <access token>* no cliente REST API (como Postman ou swagger) e mencione o RoleName do usuário no cabeçalho para obter uma resposta bem-sucedida do SnapCenter.

#### Fluxo de trabalho da API REST do MFA

Quando o MFA é configurado com o AD FS, você deve autenticar usando um token de acesso (portador) para acessar o aplicativo SnapCenter por qualquer API Rest.

### Sobre esta tarefa

- Você pode usar qualquer cliente REST, como Postman, Swagger UI ou FireCamp.
- Obtenha um token de acesso e use-o para autenticar solicitações subsequentes (SnapCenter Rest API) para executar qualquer operação.

### Passos

### Para autenticar através do AD FS MFA

1. Configure o cliente REST para chamar o ponto de extremidade do AD FS para obter o token de acesso.

   Ao clicar no botão para obter um token de acesso para um aplicativo, você será redirecionado para a página SSO do AD FS, onde deverá fornecer suas credenciais do AD e autenticar com o MFA. 1. Na página SSO do AD FS, digite seu nome de usuário ou e-mail na caixa de texto Nome de usuário.

   + Os nomes de usuário devem ser formatados como usuário@domínio ou domínio\usuário.

2. Na caixa de texto Senha, digite sua senha.
3. Clique em **Entrar**.
4. Na seção **Opções de login**, selecione uma opção de autenticação e autentique (dependendo da sua configuração).
   - Push: aprove a notificação push que é enviada para seu telefone.
   - Código QR: Use o aplicativo móvel AUTH Point para escanear o código QR e digite o código de verificação mostrado no aplicativo
   - Senha de uso único: digite a senha de uso único para seu token.
5. Após a autenticação bem-sucedida, um pop-up será aberto contendo o acesso, o ID e o token de atualização.

   Copie o token de acesso e use-o na API Rest do SnapCenter para executar a operação.

6. Na API Rest, você deve passar o token de acesso e o nome da função na seção de cabeçalho.
7. O SnapCenter valida esse token de acesso do AD FS.

   Se for um token válido, o SnapCenter o decodifica e obtém o nome de usuário.

8. Usando o nome de usuário e o nome da função, o SnapCenter autentica o usuário para uma execução de API.

   Se a autenticação for bem-sucedida, o SnapCenter retornará o resultado, caso contrário, uma mensagem de erro será exibida.

#### Habilitar ou desabilitar a funcionalidade SnapCenter MFA para REST API, CLI e GUI

### GUI

### Passos

1. Efetue login no SnapCenter Server como Administrador do SnapCenter .
2. Clique em **Configurações** > **Configurações globais** > **Configurações de autenticação multifator (MFA)**
3. Selecione a interface (GUI/RST API/CLI) para habilitar ou desabilitar o login MFA.

### Interface do PowerShell

### Passos

1. Execute os comandos do PowerShell ou da CLI para habilitar o MFA para GUI, REST API, PowerShell e SCCLI.

   ```
   Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled
   -IsCliMFAEnabled -Path
   ```

   O parâmetro path especifica o local do arquivo XML de metadados do AD FS MFA.

   Habilita o MFA para SnapCenter GUI, Rest API, PowerShell e SCCLI configurados com o caminho de arquivo de metadados do AD FS especificado.

2. Verifique o status e as configurações da configuração do MFA usando o `Get-SmMultiFactorAuthentication` cmdlet.

### Interface SCCLI

### Passos

1. ```
   # sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true
   -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path
   "C:\ADFS_metadata\abc.xml"
   ```
2. ```
   # sccli Get-SmMultiFactorAuthentication
   ```

### APIs REST

1. Execute a seguinte API de postagem para habilitar MFA para GUI, REST API, PowerShell e SCCLI.

| Parâmetro | Valor |
|---|---|
| URL solicitada | /api/4.9/settings/autenticação multifator |
| Método HTTP | Publicar |
| Corpo da solicitação | { "IsGuiMFAEnabled": falso, "IsRestApiMFAEnabled": verdadeiro, "IsCliMFAEnabled": falso, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml" } |

| | |
|---|---|
| Corpo de Resposta | { "MFAConfiguration": { "IsGuiMFAEnabled": falso, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": nulo, "IsRestApiMFAEnabled": verdadeiro, "IsCliMFAEnabled": falso, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } } |

2. Verifique o status e as configurações da configuração do MFA usando a seguinte API.

| Parâmetro | Valor |
|---|---|
| URL solicitada | /api/4.9/settings/autenticação multifator |
| Método HTTP | Pegar |
| Corpo de Resposta | { "MFAConfiguration": { "IsGuiMFAEnabled": falso, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": nulo, "IsRestApiMFAEnabled": verdadeiro, "IsCliMFAEnabled": falso, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } } |

# Instalar o SnapCenter Server

## Instalar o SnapCenter Server no host Windows

Você pode executar o executável do instalador do SnapCenter Server para instalar o SnapCenter Server.

Opcionalmente, você pode executar vários procedimentos de instalação e configuração usando cmdlets do PowerShell. Você deve usar o PowerShell 7.4.2 ou posterior.

A instalação silenciosa do SnapCenter Server a partir da linha de comando não é suportada.

**Antes de começar**

- O host do SnapCenter Server deve estar atualizado com as atualizações do Windows, sem reinicializações pendentes do sistema.
- Você deve ter certeza de que o MySQL Server não está instalado no host onde você planeja instalar o SnapCenter Server.
- Você deve ter habilitado a depuração do instalador do Windows.

  Consulte o site da Microsoft para obter informações sobre como habilitar "Registro do instalador do Windows" .

Você não deve instalar o SnapCenter Server em um host que tenha o Microsoft Exchange Server, o Active Directory ou servidores de nomes de domínio.

**Passos**

1. Baixe o pacote de instalação do SnapCenter Server em "Site de suporte da NetApp" .
2. Inicie a instalação do SnapCenter Server clicando duas vezes no arquivo .exe baixado.

   Após iniciar a instalação, todas as pré-verificações são executadas e, se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas são exibidas.

   Você pode ignorar as mensagens de aviso e prosseguir com a instalação; no entanto, os erros deverão ser corrigidos.

3. Revise os valores pré-preenchidos necessários para a instalação do SnapCenter Server e modifique-os, se necessário.

   Você não precisa especificar a senha para o banco de dados do repositório do MySQL Server. Durante a instalação do SnapCenter Server, a senha é gerada automaticamente.

   O caractere especial “%” is not supported in the custom path for the repository database. If you include "` %`" no caminho, a instalação falha.

4. Clique em **Instalar agora**.

   Se você tiver especificado algum valor inválido, mensagens de erro apropriadas serão exibidas. Você deve inserir novamente os valores e então iniciar a instalação.

   Se você clicar no botão **Cancelar**, a etapa que está sendo executada será concluída e, em seguida, iniciará a operação de reversão. O SnapCenter Server será completamente removido do host.

   Entretanto, se você clicar em **Cancelar** quando as operações "Reinicialização do site do SnapCenter Server" ou "Aguardando o início do SnapCenter Server" estiverem sendo executadas, a instalação prosseguirá sem cancelar a operação.

   Os arquivos de log são sempre listados (os mais antigos primeiro) na pasta %temp% do usuário administrador. Se você quiser redirecionar os locais de log, inicie a instalação do SnapCenter Server no prompt de comando executando:`C:\installer_location\installer_name.exe /log"C:\"`

### Recursos habilitados no host Windows durante a instalação

O instalador do SnapCenter Server habilita os recursos e funções do Windows no seu host Windows durante a instalação. Elas podem ser interessantes para solução de problemas e manutenção do sistema host.

| Categoria | Recurso |
| --- | --- |
| Servidor Web | • Serviços de Informação da Internet<br>• Serviços da World Wide Web<br>• Recursos HTTP comuns<br>◦ Documento Padrão<br>◦ Navegação de diretório<br>◦ Erros HTTP<br>◦ Redirecionamento HTTP<br>◦ Conteúdo estático<br>◦ Publicação WebDAV<br>• Saúde e Diagnóstico<br>◦ Registro personalizado<br>◦ Registro HTTP<br>◦ Ferramentas de registro<br>◦ Monitor de Solicitação<br>◦ Rastreamento<br>• Recursos de desempenho<br>◦ Compressão de conteúdo estático<br>• Segurança<br>◦ Segurança IP<br>◦ Autenticação Básica<br>◦ Suporte centralizado para certificado SSL<br>◦ Autenticação de mapeamento de certificado de cliente<br>◦ Autenticação de mapeamento de certificado do cliente IIS<br>◦ Restrições de IP e domínio<br>◦ Filtragem de solicitações<br>◦ Autorização de URL<br>◦ Autenticação do Windows<br>• Recursos de desenvolvimento de aplicativos<br>◦ Extensibilidade .NET 4.5<br>◦ Inicialização do aplicativo<br>◦ Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes)<br>◦ Inclusões do lado do servidor<br>◦ Protocolo WebSocket<br>Ferramentas de Gestão<br>Console de gerenciamento do IIS |

| Categoria | Recurso |
| --- | --- |
| Scripts e ferramentas de gerenciamento do IIS | • Serviço de Gerenciamento do IIS<br>• Ferramentas de gerenciamento da Web |
| Recursos do .NET Framework 8.0.12 | • Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes)<br>• Ativação HTTP do Windows Communication Foundation (WCF)45<br>◦ Ativação TCP<br>◦ Ativação HTTP<br>Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet" . |
| Serviço de Ativação de Processos do Windows | Modelo de Processo |
| APIs de configuração | Todos |

## Instalar o SnapCenter Server no host Linux

Você pode executar o executável do instalador do SnapCenter Server para instalar o SnapCenter Server.

**Antes de começar**

- Se você quiser instalar o SnapCenter Server usando um usuário não root que não tenha privilégios suficientes para instalar o SnapCenter, obtenha o arquivo de soma de verificação sudoers no site de suporte da NetApp . Você deve usar o arquivo de soma de verificação apropriado com base na versão do Linux.
- Se o pacote sudo não estiver disponível no SUSE Linux, instale-o para evitar falhas de autenticação.
- Para o SUSE Linux, configure o nome do host para evitar falha na instalação.
- Verifique o status seguro do Linux executando o comando `sestatus` . Se o *status do SELinux* for "habilitado" e o *modo atual* for "imposto", execute o seguinte:
  - Execute o comando: `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

    O valor padrão de *WEBAPP_EXTERNAL_PORT* é 8146
  - Se o firewall bloquear a porta, execute `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`

    O valor padrão de *WEBAPP_EXTERNAL_PORT* é 8146
  - Execute os seguintes comandos no diretório onde você tem permissão de leitura e gravação:

- `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

  Se o comando retornar "nada a fazer", execute-o novamente após instalar o SnapCenter Server.

- Se o comando criar *my-nginx.pp*, execute o comando para tornar o pacote de política ativo: `sudo semodule -i my-nginx.pp`

◦ O caminho usado para o diretório MySQL PID é */var/opt/mysqld*. Execute os seguintes comandos para definir as permissões para instalação do MySQL.

- `mkdir /var/opt/mysqld`
- `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`
- `sudo restorecon -Rv /var/opt/mysqld`

◦ O caminho usado para o diretório de dados do MySQL é */INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/*. Execute os seguintes comandos para definir as permissões para o diretório de dados do MySQL.

- `mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`
- `sudo semanage fcontext -a -t mysqld_db_t "/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"`
- `sudo restorecon -Rv /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

**Sobre esta tarefa**

- Quando o SnapCenter Server é instalado no host Linux, serviços de terceiros, como MySQL, RabbitMq e Errlang, são instalados. Você não deve desinstalá-los.
- O SnapCenter Server instalado no host Linux não suporta:
  - Alta disponibilidade
  - Plug-ins do Windows
  - Active Directory (suporta apenas usuários locais, tanto usuários root quanto não root com credenciais)
  - Autenticação baseada em chave para efetuar login no SnapCenter
- Durante a instalação do .NET Runtime, se a instalação não resolver as dependências da biblioteca *libicu*, instale *libicu* executando o comando: `yum install -y libicu`
- Se a instalação do SnapCenter Server falhar devido à indisponibilidade do *Perl*, instale o *Perl* executando o comando: `yum install -y perl`

**Passos**

1. Baixe o seguinte de "Site de suporte da NetApp" para */diretório inicial*.
   - Pacote de instalação do SnapCenter Server - **snapcenter-linux-server-(el8/el9/sles15).bin**
   - Arquivo de chave pública - **snapcenter_public_key.pub**
   - Arquivo de assinatura respectivo - **snapcenter-linux-server-(el8/el9/sles15).bin.sig**
2. Valide o arquivo de assinatura. `$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>`
3. Para instalação de usuário não root, adicione o conteúdo visudo especificado em **snapcenter_server_checksum_(el8/el9/sles15).txt** disponível junto com o instalador .bin.

4. Atribua a permissão de execução para o instalador .bin. `chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`
5. Execute uma das ações para instalar o SnapCenter Server.

| Se você quiser executar… | Faça isso… |
| --- | --- |
| Instalação interativa | `./snapcenter-linux-server-(el8/el9/sles15).bin`<br><br>Você será solicitado a inserir os seguintes detalhes:<br><br>• A porta externa do webapp usada para acessar o SnapCenter Server fora do host Linux. O valor padrão é 8146.<br>• O usuário do SnapCenter Server que instalará o SnapCenter Server.<br>• O diretório de instalação onde os pacotes serão instalados. |

| Se você quiser executar… | Faça isso… |
| --- | --- |
| Instalação não interativa | `sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEDULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename>`<br><br>Exemplo: sudo ./snapcenter_linux_server.bin -i silent -DWEBAPP_EXTERNAL_PORT=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_DIR=/opt -DINSTALL_LOG_NAME=InstallerLog.log<br><br>Os logs serão armazenados em */var/opt/snapcenter/logs*.<br><br>Parâmetros a serem passados para instalar o SnapCenter Server:<br><br>• DWEBAPP_EXTERNAL_PORT: Porta externa do Webapp usada para acessar o SnapCenter Server fora do host Linux. O valor padrão é 8146.<br>• DWEBAPP_INTERNAL_PORT: Porta interna do Webapp usada para acessar o SnapCenter Server no host Linux. O valor padrão é 8147.<br>• DSMCORE_PORT: Porta SMCore na qual os serviços smcore estão sendo executados. O valor padrão é 8145.<br>• DSCHEDULER_PORT: Porta do agendador na qual os serviços do agendador estão sendo executados. O valor padrão é 8154.<br>• DSNAPCENTER_SERVER_USER: Usuário do SnapCenter Server que instalará o SnapCenter Server. Para *DSNAPCENTER_SERVER_USER*, o padrão é o usuário que executa o instalador.<br>• DUSER_INSTALL_DIR: Diretório de instalação onde os pacotes serão instalados. Para *DUSER_INSTALL_DIR*, o diretório de instalação padrão é */opt*.<br>• DINSTALL_LOG_NAME: Nome do arquivo de log onde os logs de instalação serão armazenados. Este é um parâmetro opcional e, se especificado, nenhum log será exibido no console. Se você não especificar este parâmetro, os logs serão exibidos no console e também armazenados no arquivo de log padrão.<br><br>DSELINUX: Se o *status do SELinux* for |

**O que vem a seguir?**

- Se o *status do SELinux* for "habilitado" e o *modo atual* for "imposto", o serviço **nginx** falhará ao iniciar. Você deve executar os seguintes comandos:
  a. Vá para o diretório inicial.
  b. Execute o comando: `journalctl -x|grep nginx`
  c. Se a porta interna do Webapp (8147) não tiver permissão para escutar, execute os seguintes comandos:
     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
     - `semodule -i my-nginx.pp`
  d. Correr `setsebool -P httpd_can_network_connect on`

- "habilitado", o *modo atual* for "imposto" e você tiver executado os comandos mencionados na seção Antes de começar, especifique este parâmetro e atribua o valor como 1. O valor padrão é 0.
- DUPGRADE: O valor padrão é 0. Especifique este parâmetro e seu valor como qualquer número inteiro diferente de 0 para atualizar o SnapCenter Server.

**Recursos habilitados no host Linux durante a instalação**

O SnapCenter Server instala os pacotes de software abaixo que podem ajudar na solução de problemas e na manutenção do sistema host.

- Rabbitmq
- Erlang

## Registrar SnapCenter

Se você é novo nos produtos NetApp e não tem uma conta NetApp existente, registre o SnapCenter para habilitar o suporte.

**Passos**

1. Após instalar o SnapCenter, navegue até **Ajuda > Sobre**.
2. Na caixa de diálogo *Sobre o SnapCenter*, anote a instância do SnapCenter , um número de 20 dígitos que começa com 971.
3. Clique https://register.netapp.com .
4. Clique em *Não sou um cliente registrado da NetApp *.
5. Especifique seus dados para se registrar.
6. Deixe o campo SN de referência da NetApp em branco.
7. Selecione * SnapCenter* no menu suspenso Linha de produtos.
8. Selecione o provedor de cobrança.
9. Insira o ID da instância do SnapCenter de 20 dígitos.
10. Clique em **Enviar**.

## Efetue login no SnapCenter usando autorização RBAC

O SnapCenter oferece suporte ao controle de acesso baseado em função (RBAC). O administrador do SnapCenter atribui funções e recursos por meio do SnapCenter RBAC a um usuário no grupo de trabalho ou no Active Directory, ou a grupos no Active Directory. O usuário do RBAC agora pode fazer login no SnapCenter com as funções atribuídas.

**Antes de começar**

- Você deve habilitar o Serviço de Ativação de Processos do Windows (WAS) no Gerenciador do Windows Server.
- Se você quiser usar o Internet Explorer como navegador para efetuar login no SnapCenter Server, certifique-se de que o Modo Protegido no Internet Explorer esteja desabilitado.
- Se o SnapCenter Server estiver instalado no host Linux, você deverá efetuar login usando a conta de usuário que foi usada para instalar o SnapCenter Server.

**Sobre esta tarefa**

Durante a instalação, o assistente de instalação do SnapCenter Server cria um atalho e o coloca na área de trabalho e no menu Iniciar do host onde o SnapCenter está instalado. Além disso, no final da instalação, o assistente de instalação exibe o URL do SnapCenter com base nas informações fornecidas durante a instalação, que você pode copiar se quiser fazer login de um sistema remoto.

Se você tiver várias guias abertas no seu navegador, fechar apenas a guia do navegador SnapCenter não fará seu logout do SnapCenter. Para encerrar sua conexão com o SnapCenter, você deve sair do SnapCenter clicando no botão **Sair** ou fechando todo o navegador da web.

**Melhores práticas:** Por motivos de segurança, é recomendável que você não habilite seu navegador para salvar sua senha do SnapCenter .

A URL da GUI padrão é uma conexão segura com a porta padrão 8146 no servidor onde o SnapCenter Server está instalado (*https://server:8146*). Se você forneceu uma porta de servidor diferente durante a instalação do SnapCenter , essa porta será usada.

Para implantação de Alta Disponibilidade (HA), você deve acessar o SnapCenter usando o IP do cluster virtual *https://Virtual_Cluster_IP_or_FQDN:8146*. Se você não vir a interface do usuário do SnapCenter ao navegar até *https://Virtual_Cluster_IP_or_FQDN:8146* no Internet Explorer (IE), adicione o endereço IP ou FQDN do Virtual Cluster como um site confiável no IE em cada host de plug-in ou desative a Segurança Aprimorada do IE em cada host de plug-in. Para obter mais informações, consulte "Não é possível acessar o endereço IP do cluster de uma rede externa" .

Além de usar a GUI do SnapCenter , você pode usar cmdlets do PowerShell para criar scripts para executar operações de configuração, backup e restauração. Alguns cmdlets podem ter mudado a cada versão do SnapCenter . O "Guia de referência do cmdlet do software SnapCenter" tem os detalhes.

Se estiver efetuando login no SnapCenter pela primeira vez, você deverá fazer login usando as credenciais fornecidas durante o processo de instalação.

**Passos**

1. Inicie o SnapCenter a partir do atalho localizado na área de trabalho do host local, ou a partir da URL fornecida no final da instalação, ou a partir da URL fornecida pelo administrador do SnapCenter .
2. Insira as credenciais do usuário.

| Para especificar o seguinte… | Use um destes formatos… |
| --- | --- |
| Administrador de domínio | • NetBIOS\Nome de usuário<br>• Sufixo UserName@UPN<br>Por exemplo, username@netapp.com<br>• Domínio FQDN\Nome de usuário |
| Administrador local | Nome de usuário |

3. Se você tiver mais de uma função atribuída, na caixa Função, selecione a função que deseja usar para esta sessão de login.

   Seu usuário atual e a função associada são exibidos no canto superior direito do SnapCenter depois que você faz login.

**Resultado**

A página Painel é exibida.

Se o registro falhar com o erro de que o site não pode ser acessado, você deve mapear o certificado SSL para o SnapCenter. "Saber mais"

**Depois que você terminar**

Após efetuar login no SnapCenter Server como um usuário RBAC pela primeira vez, atualize a lista de recursos.

Se você tiver domínios não confiáveis do Active Directory que deseja que o SnapCenter suporte, registre esses domínios no SnapCenter antes de configurar as funções para os usuários em domínios não confiáveis. "Saber mais" .

Se você quiser adicionar o host do plug-in no SnapCenter em execução no host Linux, deverá obter o arquivo de soma de verificação no local: */opt/ NetApp/snapcenter/SnapManagerWeb/Repository*.

A partir da versão 6.0, um atalho para o SnapCenter PowerShell é criado na área de trabalho. Você pode acessar diretamente os cmdlets do SnapCenter PowerShell usando o atalho.

**Efetue login no SnapCenter usando a autenticação multifator (MFA)**

O SnapCenter Server oferece suporte a MFA para contas de domínio, que fazem parte do diretório ativo.

**Antes de começar**

Você deveria ter habilitado o MFA. Para obter informações sobre como habilitar o MFA, consulte"Habilitar autenticação multifator"

**Sobre esta tarefa**

- Somente FQDN é suportado
- Usuários de grupos de trabalho e de domínio cruzado não podem efetuar login usando MFA

**Passos**

1. Inicie o SnapCenter a partir do atalho localizado na área de trabalho do host local, ou a partir da URL fornecida no final da instalação, ou a partir da URL fornecida pelo administrador do SnapCenter .
2. Na página de login do AD FS, insira o nome de usuário e a senha.

   Quando a mensagem de erro de nome de usuário ou senha inválidos for exibida na página do AD FS, você deve verificar o seguinte:

   - Se o nome de usuário ou a senha são válidos

     A conta de usuário deve existir no Active Directory (AD)

   - Se você excedeu o máximo de tentativas permitidas definido no AD
   - Se o AD e o AD FS estão ativos e em execução

### Modificar o tempo limite da sessão da GUI padrão do SnapCenter

Você pode modificar o período de tempo limite da sessão da GUI do SnapCenter para torná-lo menor ou maior que o período de tempo limite padrão de 20 minutos.

Como recurso de segurança, após um período padrão de 15 minutos de inatividade, o SnapCenter avisa que você será desconectado da sessão da GUI em 5 minutos. Por padrão, o SnapCenter desconecta você da sessão da GUI após 20 minutos de inatividade, e você deve efetuar login novamente.

**Passos**

1. No painel de navegação esquerdo, clique em **Configurações** > **Configurações globais**.
2. Na página Configurações globais, clique em **Configurações de configuração**.
3. No campo Tempo limite da sessão, insira o novo tempo limite da sessão em minutos e clique em **Salvar**.

### Proteja o servidor web SnapCenter desabilitando o SSL 3.0

Por motivos de segurança, você deve desabilitar o protocolo Secure Socket Layer (SSL) 3.0 no Microsoft IIS se ele estiver habilitado no seu servidor web SnapCenter .

Há falhas no protocolo SSL 3.0 que um invasor pode usar para causar falhas de conexão ou realizar ataques man-in-the-middle e observar o tráfego de criptografia entre seu site e seus visitantes.

**Passos**

1. Para iniciar o Editor do Registro no host do servidor web SnapCenter , clique em **Iniciar** > **Executar** e digite regedit.
2. No Editor do Registro, navegue até HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\.
   - Se a chave do servidor já existir:
     i. Selecione o DWORD habilitado e clique em **Editar** > **Modificar**.
     ii. Altere o valor para 0 e clique em **OK**.
   - Se a chave do servidor não existir:

i. Clique em **Editar** > **Novo** > **Chave** e nomeie a chave como Servidor.

ii. Com a nova chave do servidor selecionada, clique em **Editar** > **Novo** > **DWORD**.

iii. Nomeie o novo DWORD como Habilitado e insira 0 como valor.

3. Feche o Editor do Registro.

# Configurar o SnapCenter Server

## Adicionar e provisionar o sistema de armazenamento

### Adicionar sistemas de armazenamento

Você deve configurar o sistema de armazenamento que dá ao SnapCenter acesso ao armazenamento ONTAP , aos sistemas ASA r2 ou ao Amazon FSx for NetApp ONTAP para executar operações de proteção e provisionamento de dados.

Você pode adicionar um SVM autônomo ou um cluster composto por vários SVMs. Se estiver usando o Amazon FSx for NetApp ONTAP, você pode adicionar o LIF de administração do FSx composto por vários SVMs usando a conta fsxadmin ou adicionar o FSx SVM no SnapCenter.

**Antes de começar**

- Você deve ter as permissões necessárias na função de administrador de infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estejam em andamento.

  As instalações do plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento porque o cache do host pode não ser atualizado e o status dos bancos de dados pode ser exibido na GUI do SnapCenter como “Não disponível para backup” ou "`Não no armazenamento NetApp ".

- Os nomes dos sistemas de armazenamento devem ser exclusivos.

  O SnapCenter não oferece suporte a vários sistemas de armazenamento com o mesmo nome em clusters diferentes. Cada sistema de armazenamento suportado pelo SnapCenter deve ter um nome exclusivo e um endereço IP LIF de dados exclusivo.

**Sobre esta tarefa**

- Ao configurar sistemas de armazenamento, você também pode habilitar os recursos do Sistema de Gerenciamento de Eventos (EMS) e do AutoSupport . A ferramenta AutoSupport coleta dados sobre a integridade do seu sistema e os envia automaticamente ao suporte técnico da NetApp , permitindo que eles solucionem problemas do seu sistema.

  Se você habilitar esses recursos, o SnapCenter enviará informações do AutoSupport ao sistema de armazenamento e mensagens EMS ao syslog do sistema de armazenamento quando um recurso for protegido, uma operação de restauração ou clonagem for concluída com sucesso ou uma operação falhar.

- Se você estiver planejando replicar Snapshots para um destino SnapMirror ou SnapVault , deverá configurar conexões do sistema de armazenamento para o SVM ou Cluster de destino, bem como para o SVM ou Cluster de origem.

Se você alterar a senha do sistema de armazenamento, os trabalhos agendados, o backup sob demanda e as operações de restauração poderão falhar. Depois de alterar a senha do sistema de armazenamento, você pode atualizá-la clicando em **Modificar** na guia Armazenamento.

**Passos**

1. No painel de navegação esquerdo, clique em **Sistemas de armazenamento**.
2. Na página Sistemas de Armazenamento, clique em **Novo**.
3. Na página Adicionar sistema de armazenamento, forneça as seguintes informações:

| Para este campo… | Faça isso… |
| --- | --- |
| Sistema de armazenamento | Digite o nome do sistema de armazenamento ou endereço IP.<br>Os nomes dos sistemas de armazenamento, sem incluir o nome de domínio, devem ter 15 caracteres ou menos e devem ser resolvíveis. Para criar conexões de sistema de armazenamento com nomes com mais de 15 caracteres, você pode usar o cmdlet Add-SmStorageConnectionPowerShell.<br>Para sistemas de armazenamento com configuração MetroCluster (MCC), é recomendável registrar clusters locais e pares para operações sem interrupções.<br>O SnapCenter não oferece suporte a várias SVMs com o mesmo nome em clusters diferentes. Cada SVM suportado pelo SnapCenter deve ter um nome exclusivo.<br>Depois de adicionar a conexão de armazenamento ao SnapCenter, você não deve renomear o SVM ou o Cluster usando o ONTAP.<br>Se o SVM for adicionado com um nome curto ou FQDN, ele deverá ser resolvível tanto no SnapCenter quanto no host do plug-in. |
| Nome de usuário/Senha | Insira as credenciais do usuário de armazenamento que tem os privilégios necessários para acessar o sistema de armazenamento. |

| Para este campo… | Faça isso… |
| --- | --- |
| Configurações do Sistema de Gerenciamento de Eventos (EMS) e AutoSupport | Se você quiser enviar mensagens EMS para o syslog do sistema de armazenamento ou se quiser que mensagens do AutoSupport sejam enviadas ao sistema de armazenamento para proteção aplicada, operações de restauração concluídas ou operações com falha, marque a caixa de seleção apropriada.<br><br>Quando você seleciona a caixa de seleção **Enviar notificação do AutoSupport para operações com falha no sistema de armazenamento**, a caixa de seleção **Registrar eventos do SnapCenter Server no syslog** também é selecionada porque o sistema de mensagens EMS é necessário para habilitar as notificações do AutoSupport . |

4. Clique em **Mais opções** se quiser modificar os valores padrão atribuídos à plataforma, protocolo, porta e tempo limite.

   a. Em Plataforma, selecione uma das opções na lista suspensa.

      Se o SVM for o sistema de armazenamento secundário em um relacionamento de backup, marque a caixa de seleção **Secundário**. Quando a opção **Secundária** é selecionada, o SnapCenter não executa uma verificação de licença imediatamente.

   Se você adicionou SVM no SnapCenter , o usuário precisa selecionar manualmente o tipo de plataforma no menu suspenso.

   a. Em Protocolo, selecione o protocolo que foi configurado durante a configuração do SVM ou do Cluster, normalmente HTTPS.
   b. Digite a porta que o sistema de armazenamento aceita.

      A porta padrão 443 normalmente funciona.

   c. Insira o tempo em segundos que deve decorrer antes que as tentativas de comunicação sejam interrompidas.

      O valor padrão é 60 segundos.

   d. Se o SVM tiver várias interfaces de gerenciamento, marque a caixa de seleção **IP preferencial** e insira o endereço IP preferencial para conexões SVM.
   e. Clique em **Salvar**.
5. Clique em **Enviar**.

**Resultado**

Na página Sistemas de Armazenamento, no menu suspenso **Tipo**, execute uma das seguintes ações:

- Selecione * ONTAP SVMs * se quiser visualizar todos os SVMs que foram adicionados.

  Se você adicionou FSx SVMs, eles serão listados aqui.

- Selecione * Clusters ONTAP * se quiser visualizar todos os clusters que foram adicionados.

  Se você adicionou clusters FSx usando fsxadmin, os clusters FSx serão listados aqui.

  Ao clicar no nome do cluster, todas as SVMs que fazem parte do cluster são exibidas na seção Máquinas Virtuais de Armazenamento.

  Se um novo SVM for adicionado ao cluster ONTAP usando a GUI do ONTAP , clique em **Rediscover** para visualizar o SVM recém-adicionado.

**Depois que você terminar**

Um administrador de cluster deve habilitar o AutoSupport em cada nó do sistema de armazenamento para enviar notificações por e-mail de todos os sistemas de armazenamento aos quais o SnapCenter tem acesso, executando o seguinte comando na linha de comando do sistema de armazenamento:

```
autosupport trigger modify -node nodename -autosupport-message client.app.info
-to enable -noteto enable
```

O administrador da Máquina Virtual de Armazenamento (SVM) não tem acesso ao AutoSupport.

**Conexões e credenciais de armazenamento**

Antes de executar operações de proteção de dados, você deve configurar as conexões de armazenamento e adicionar as credenciais que o SnapCenter Server e os plug-ins do SnapCenter usarão.

**Conexões de armazenamento**

As conexões de armazenamento dão ao SnapCenter Server e aos plug-ins do SnapCenter acesso ao armazenamento ONTAP . A configuração dessas conexões também envolve a configuração dos recursos do AutoSupport e do Sistema de Gerenciamento de Eventos (EMS).

**Credenciais**

- Administrador de domínio ou qualquer membro do grupo de administradores

  Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema em que você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são:

  - *NetBIOS\Nome do Usuário*
  - *FQDN do domínio\Nome do usuário*
  - *Nome de usuário@upn*
- Administrador local (somente para grupos de trabalho)

  Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host.

  O formato válido para o campo Nome de usuário é: *UserName*

- Credenciais para grupos de recursos individuais

  Se você configurar credenciais para grupos de recursos individuais e o nome de usuário não tiver privilégios de administrador completos, será necessário atribuir pelo menos os privilégios de grupo de recursos e backup ao nome de usuário.

## Provisionar armazenamento em hosts Windows

### Criar e gerenciar igroups

Crie grupos de iniciadores (igroups) para especificar quais hosts podem acessar um determinado LUN no sistema de armazenamento. Você pode usar o SnapCenter para criar, renomear, modificar ou excluir um igroup em um host Windows.

#### Criar um igroup

Você pode usar o SnapCenter para criar um igroup em um host Windows. O igroup estará disponível no assistente Criar Disco ou Conectar Disco quando você mapear o igroup para um LUN.

**Passos**

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Igroup**.
3. Na página Grupos de Iniciadores, clique em **Novo**.
4. Na caixa de diálogo Criar Igroup, defina o igroup:

| Neste campo… | Faça isso… |
|---|---|
| Sistema de armazenamento | Selecione o SVM para o LUN que você mapeará para o igroup. |
| Hospedar | Selecione o host no qual você deseja criar o igroup. |
| Nome do Igroup | Digite o nome do igroup. |
| Iniciadores | Selecione o iniciador. |
| Tipo | Selecione o tipo de iniciador, iSCSI, FCP ou misto (FCP e iSCSI). |

5. Quando estiver satisfeito com suas entradas, clique em **OK**.

   O SnapCenter cria o igroup no sistema de armazenamento.

#### Renomear um igroup

Você pode usar o SnapCenter para renomear um igroup existente.

**Passos**

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Igroup**.
3. Na página Grupos de Iniciadores, clique no campo **Máquina Virtual de Armazenamento** para exibir uma lista de SVMs disponíveis e, em seguida, selecione a SVM para o igroup que você deseja renomear.
4. Na lista de igroups do SVM, selecione o igroup que deseja renomear e clique em **Renomear**.
5. Na caixa de diálogo Renomear igroup, insira o novo nome para o igroup e clique em **Renomear**.

### Modificar um igroup

Você pode usar o SnapCenter para adicionar iniciadores de igroup a um igroup existente. Ao criar um igroup, você pode adicionar apenas um host. Se você quiser criar um igroup para um cluster, poderá modificar o igroup para adicionar outros nós a esse igroup.

### Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Igroup**.
3. Na página Grupos de Iniciadores, clique no campo **Máquina Virtual de Armazenamento** para exibir uma lista suspensa de SVMs disponíveis e selecione a SVM para o igroup que você deseja modificar.
4. Na lista de igroups, selecione um igroup e clique em **Adicionar iniciador ao igroup**.
5. Selecione um host.
6. Selecione os iniciadores e clique em **OK**.

### Excluir um igroup

Você pode usar o SnapCenter para excluir um igroup quando não precisar mais dele.

### Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Igroup**.
3. Na página Grupos de Iniciadores, clique no campo **Máquina Virtual de Armazenamento** para exibir uma lista suspensa de SVMs disponíveis e selecione a SVM para o igroup que você deseja excluir.
4. Na lista de igroups do SVM, selecione o igroup que deseja excluir e clique em **Excluir**.
5. Na caixa de diálogo Excluir igroup, clique em **OK**.

   O SnapCenter exclui o igroup.

#### Criar e gerenciar discos

## O host do Windows vê LUNs no seu sistema de armazenamento como discos virtuais. Você pode usar o SnapCenter para criar e configurar um LUN conectado via FC ou via iSCSI.

- O SnapCenter suporta apenas discos básicos. Os discos dinâmicos não são suportados.
- Para GPT, apenas uma partição de dados é permitida e para MBR, uma partição primária com um volume formatado com NTFS ou CSVFS e um caminho de montagem.

- Estilos de partição suportados: GPT, MBR; em uma VM VMware UEFI, apenas discos iSCSI são suportados

> O SnapCenter não suporta renomear um disco. Se um disco gerenciado pelo SnapCenter for renomeado, as operações do SnapCenter não serão bem-sucedidas.

### Visualizar os discos em um host

Você pode visualizar os discos em cada host Windows que você gerencia com o SnapCenter.

#### Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Discos**.
3. Selecione o host na lista suspensa **Host**.

   Os discos estão listados.

### Exibir discos agrupados

Você pode visualizar discos clusterizados no cluster que você gerencia com o SnapCenter. Os discos em cluster são exibidos somente quando você seleciona o cluster no menu suspenso Hosts.

#### Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Discos**.
3. Selecione o cluster na lista suspensa **Host**.

   Os discos estão listados.

### Estabelecer uma sessão iSCSI

Se estiver usando iSCSI para se conectar a um LUN, você deverá estabelecer uma sessão iSCSI antes de criar o LUN para habilitar a comunicação.

#### Antes de começar

- Você deve ter definido o nó do sistema de armazenamento como um destino iSCSI.
- Você deve ter iniciado o serviço iSCSI no sistema de armazenamento. "Saber mais"

#### Sobre esta tarefa

Você pode estabelecer uma sessão iSCSI somente entre as mesmas versões de IP, de IPv6 para IPv6 ou de IPv4 para IPv4.

Você pode usar um endereço IPv6 de link local para gerenciamento de sessão iSCSI e para comunicação entre um host e um destino somente quando ambos estiverem na mesma sub-rede.

Se você alterar o nome de um iniciador iSCSI, o acesso aos destinos iSCSI será afetado. Após alterar o nome, talvez seja necessário reconfigurar os destinos acessados pelo iniciador para que eles possam

reconhecer o novo nome. Você deve reiniciar o host após alterar o nome de um iniciador iSCSI.

Se o seu host tiver mais de uma interface iSCSI, depois de estabelecer uma sessão iSCSI com o SnapCenter usando um endereço IP na primeira interface, você não poderá estabelecer uma sessão iSCSI de outra interface com um endereço IP diferente.

**Passos**

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Sessão iSCSI**.
3. Na lista suspensa **Máquina Virtual de Armazenamento**, selecione a máquina virtual de armazenamento (SVM) para o destino iSCSI.
4. Na lista suspensa **Host**, selecione o host da sessão.
5. Clique em **Estabelecer Sessão**.

   O assistente Estabelecer Sessão é exibido.

6. No assistente Estabelecer Sessão, identifique o destino:

| Neste campo… | Digitar… |
|---|---|
| Nome do nó de destino | O nome do nó do destino iSCSI<br><br>Se houver um nome de nó de destino existente, o nome será exibido em formato somente leitura. |
| Endereço do portal de destino | O endereço IP do portal da rede de destino |
| Porta do portal de destino | A porta TCP do portal da rede de destino |
| Endereço do portal do iniciador | O endereço IP do portal da rede iniciadora |

7. Quando estiver satisfeito com suas entradas, clique em **Conectar**.

   O SnapCenter estabelece a sessão iSCSI.

8. Repita este procedimento para estabelecer uma sessão para cada alvo.

**Crie LUNs ou discos conectados por FC ou iSCSI**

O host do Windows vê os LUNs no seu sistema de armazenamento como discos virtuais. Você pode usar o SnapCenter para criar e configurar um LUN conectado via FC ou via iSCSI.

Se você quiser criar e formatar discos fora do SnapCenter, somente os sistemas de arquivos NTFS e CSVFS são suportados.

**Antes de começar**

- Você deve ter criado um volume para o LUN no seu sistema de armazenamento.

  O volume deve conter apenas LUNs e apenas LUNs criados com o SnapCenter.

Não é possível criar um LUN em um volume clone criado SnapCenter, a menos que o clone já tenha sido dividido.

- Você deve ter iniciado o serviço FC ou iSCSI no sistema de armazenamento.
- Se estiver usando iSCSI, você deverá ter estabelecido uma sessão iSCSI com o sistema de armazenamento.
- O pacote de plug-ins do SnapCenter para Windows deve ser instalado somente no host no qual você está criando o disco.

**Sobre esta tarefa**

- Não é possível conectar um LUN a mais de um host, a menos que o LUN seja compartilhado por hosts em um cluster de failover do Windows Server.
- Se um LUN for compartilhado por hosts em um cluster de failover do Windows Server que usa CSV (Cluster Shared Volumes), você deverá criar o disco no host que possui o grupo de clusters.

**Passos**

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Discos**.
3. Selecione o host na lista suspensa **Host**.
4. Clique em **Novo**.

   O assistente Criar disco é aberto.

5. Na página Nome do LUN, identifique o LUN:

| Neste campo… | Faça isso… |
|---|---|
| Sistema de armazenamento | Selecione o SVM para o LUN. |
| Caminho LUN | Clique em **Procurar** para selecionar o caminho completo da pasta que contém o LUN. |
| Nome da LUN | Digite o nome do LUN. |
| Tamanho do cluster | Selecione o tamanho de alocação do bloco LUN para o cluster.<br><br>O tamanho do cluster depende do sistema operacional e dos aplicativos. |
| Rótulo LUN | Opcionalmente, insira um texto descritivo para o LUN. |

6. Na página Tipo de disco, selecione o tipo de disco:

| Selecione… | Se… |
| --- | --- |
| Disco dedicado | O LUN pode ser acessado por apenas um host.<br><br>Ignore o campo **Grupo de recursos**. |
| Disco compartilhado | O LUN é compartilhado por hosts em um cluster de failover do Windows Server.<br><br>Insira o nome do grupo de recursos do cluster no campo **Grupo de recursos**. Você precisa criar o disco em apenas um host no cluster de failover. |
| Volume compartilhado do cluster (CSV) | O LUN é compartilhado por hosts em um cluster de failover do Windows Server que usa CSV.<br><br>Insira o nome do grupo de recursos do cluster no campo **Grupo de recursos**. Certifique-se de que o host no qual você está criando o disco seja o proprietário do grupo de clusters. |

7. Na página Propriedades da unidade, especifique as propriedades da unidade:

| Propriedade | Descrição |
| --- | --- |
| Atribuição automática de ponto de montagem | O SnapCenter atribui automaticamente um ponto de montagem de volume com base na unidade do sistema.<br><br>Por exemplo, se a unidade do sistema for C:, a atribuição automática criará um ponto de montagem de volume na unidade C: (C:\scmnpt\). A atribuição automática não é suportada para discos compartilhados. |
| Atribuir letra de unidade | Monte o disco na unidade selecionada na lista suspensa adjacente. |
| Usar ponto de montagem de volume | Monte o disco no caminho da unidade especificado no campo adjacente.<br><br>A raiz do ponto de montagem do volume deve pertencer ao host no qual você está criando o disco. |
| Não atribua letra de unidade ou ponto de montagem de volume | Escolha esta opção se preferir montar o disco manualmente no Windows. |
| Tamanho da LUN | Especifique o tamanho do LUN; mínimo de 150 MB.<br><br>Selecione MB, GB ou TB na lista suspensa ao lado. |

| Propriedade | Descrição |
| --- | --- |
| Use o provisionamento fino para o volume que hospeda este LUN | Provisionamento fino do LUN.<br><br>O provisionamento fino aloca apenas a quantidade de espaço de armazenamento necessária de cada vez, permitindo que o LUN cresça eficientemente até a capacidade máxima disponível.<br><br>Certifique-se de que haja espaço suficiente disponível no volume para acomodar todo o armazenamento LUN que você acha que precisará. |
| Escolha o tipo de partição | Selecione a partição GPT para uma tabela de partição GUID ou a partição MBR para um registro mestre de inicialização.<br><br>Partições MBR podem causar problemas de desalinhamento em clusters de failover do Windows Server.<br><br>Discos de partição de interface de firmware extensível unificada (UEFI) não são suportados. |

8. Na página Map LUN, selecione o iniciador iSCSI ou FC no host:

| Neste campo… | Faça isso… |
| --- | --- |
| Hospedar | Clique duas vezes no nome do grupo de clusters para exibir uma lista suspensa que mostra os hosts que pertencem ao cluster e, em seguida, selecione o host para o iniciador.<br><br>Este campo será exibido somente se o LUN for compartilhado por hosts em um cluster de failover do Windows Server. |
| Escolha o iniciador do host | Selecione **Fibre Channel** ou **iSCSI** e, em seguida, selecione o iniciador no host.<br><br>Você pode selecionar vários iniciadores FC se estiver usando FC com E/S multicaminho (MPIO). |

9. Na página Tipo de grupo, especifique se deseja mapear um igroup existente para o LUN ou criar um novo igroup:

| Selecione… | Se… |
| --- | --- |
| Criar novo igroup para iniciadores selecionados | Você deseja criar um novo igroup para os iniciadores selecionados. |

| Selecione… | Se… |
| --- | --- |
| Escolha um igroup existente ou especifique um novo igroup para iniciadores selecionados | Você deseja especificar um igroup existente para os iniciadores selecionados ou criar um novo igroup com o nome especificado.<br><br>Digite o nome do igroup no campo **nome do igroup**. Digite as primeiras letras do nome do igroup existente para preencher automaticamente o campo. |

10. Na página Resumo, revise suas seleções e clique em **Concluir**.

    O SnapCenter cria o LUN e o conecta à unidade ou caminho de unidade especificado no host.

### Redimensionar um disco

Você pode aumentar ou diminuir o tamanho de um disco conforme as necessidades do seu sistema de armazenamento mudam.

#### Sobre esta tarefa

- Para LUN com provisionamento fino, o tamanho da geometria do LUN ONTAP é mostrado como o tamanho máximo.
- Para LUN com provisionamento espesso, o tamanho expansível (tamanho disponível no volume) é mostrado como o tamanho máximo.
- LUNs com partições no estilo MBR têm um limite de tamanho de 2 TB.
- LUNs com partições no estilo GPT têm um limite de tamanho de sistema de armazenamento de 16 TB.
- É uma boa ideia fazer um Snapshot antes de redimensionar um LUN.
- Se você precisar restaurar um LUN de um Snapshot feito antes do LUN ser redimensionado, o SnapCenter redimensionará automaticamente o LUN para o tamanho do Snapshot.

  Após a operação de restauração, os dados adicionados ao LUN após o redimensionamento devem ser restaurados a partir de um Snapshot feito após o redimensionamento.

#### Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Discos**.
3. Selecione o host na lista suspensa Host.

   Os discos estão listados.

4. Selecione o disco que deseja redimensionar e clique em **Redimensionar**.
5. Na caixa de diálogo Redimensionar disco, use a ferramenta deslizante para especificar o novo tamanho do disco ou insira o novo tamanho no campo Tamanho.

Se você inserir o tamanho manualmente, precisará clicar fora do campo Tamanho antes que o botão Reduzir ou Expandir seja habilitado adequadamente. Além disso, você deve clicar em MB, GB ou TB para especificar a unidade de medida.

6. Quando estiver satisfeito com suas entradas, clique em **Reduzir** ou **Expandir**, conforme apropriado.

   O SnapCenter redimensiona o disco.

### Conecte um disco

Você pode usar o assistente Conectar Disco para conectar um LUN existente a um host ou para reconectar um LUN que foi desconectado.

**Antes de começar**

- Você deve ter iniciado o serviço FC ou iSCSI no sistema de armazenamento.
- Se estiver usando iSCSI, você deverá ter estabelecido uma sessão iSCSI com o sistema de armazenamento.
- Não é possível conectar um LUN a mais de um host, a menos que o LUN seja compartilhado por hosts em um cluster de failover do Windows Server.
- Se o LUN for compartilhado por hosts em um cluster de failover do Windows Server que usa CSV (Cluster Shared Volumes), você deverá conectar o disco no host que possui o grupo de clusters.
- O Plug-in para Windows precisa ser instalado somente no host no qual você está conectando o disco.

**Passos**

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Discos**.
3. Selecione o host na lista suspensa **Host**.
4. Clique em **Conectar**.

   O assistente Conectar disco é aberto.

5. Na página Nome do LUN, identifique o LUN ao qual deseja se conectar:

| Neste campo… | Faça isso… |
|---|---|
| Sistema de armazenamento | Selecione o SVM para o LUN. |
| Caminho LUN | Clique em **Procurar** para selecionar o caminho completo do volume que contém o LUN. |
| Nome da LUN | Digite o nome do LUN. |
| Tamanho do cluster | Selecione o tamanho de alocação do bloco LUN para o cluster.<br><br>O tamanho do cluster depende do sistema operacional e dos aplicativos. |

| Neste campo… | Faça isso… |
| --- | --- |
| Rótulo LUN | Opcionalmente, insira um texto descritivo para o LUN. |

6. Na página Tipo de disco, selecione o tipo de disco:

| Selecione… | Se… |
| --- | --- |
| Disco dedicado | O LUN pode ser acessado por apenas um host. |
| Disco compartilhado | O LUN é compartilhado por hosts em um cluster de failover do Windows Server.<br><br>Você só precisa conectar o disco a um host no cluster de failover. |
| Volume compartilhado do cluster (CSV) | O LUN é compartilhado por hosts em um cluster de failover do Windows Server que usa CSV.<br><br>Certifique-se de que o host no qual você está se conectando ao disco seja o proprietário do grupo de cluster. |

7. Na página Propriedades da unidade, especifique as propriedades da unidade:

| Propriedade | Descrição |
| --- | --- |
| Atribuição automática | Deixe o SnapCenter atribuir automaticamente um ponto de montagem de volume com base na unidade do sistema.<br><br>Por exemplo, se a unidade do sistema for C:, a propriedade de atribuição automática criará um ponto de montagem de volume na unidade C: (C:\scmnpt\). A propriedade de atribuição automática não é suportada para discos compartilhados. |
| Atribuir letra de unidade | Monte o disco na unidade selecionada na lista suspensa ao lado. |
| Usar ponto de montagem de volume | Monte o disco no caminho da unidade especificado no campo ao lado.<br><br>A raiz do ponto de montagem do volume deve pertencer ao host no qual você está criando o disco. |

| Propriedade | Descrição |
| --- | --- |
| Não atribua letra de unidade ou ponto de montagem de volume | Escolha esta opção se preferir montar o disco manualmente no Windows. |

8. Na página Map LUN, selecione o iniciador iSCSI ou FC no host:

| Neste campo… | Faça isso… |
| --- | --- |
| Hospedar | Clique duas vezes no nome do grupo de clusters para exibir uma lista suspensa que mostra os hosts que pertencem ao cluster e, em seguida, selecione o host para o iniciador.<br><br>Este campo será exibido somente se o LUN for compartilhado por hosts em um cluster de failover do Windows Server. |
| Escolha o iniciador do host | Selecione **Fibre Channel** ou **iSCSI** e, em seguida, selecione o iniciador no host.<br><br>Você pode selecionar vários iniciadores FC se estiver usando FC com MPIO. |

9. Na página Tipo de grupo, especifique se deseja mapear um igroup existente para o LUN ou criar um novo igroup:

| Selecione… | Se… |
| --- | --- |
| Criar novo igroup para iniciadores selecionados | Você deseja criar um novo igroup para os iniciadores selecionados. |
| Escolha um igroup existente ou especifique um novo igroup para iniciadores selecionados | Você deseja especificar um igroup existente para os iniciadores selecionados ou criar um novo igroup com o nome especificado.<br><br>Digite o nome do igroup no campo **nome do igroup**. Digite as primeiras letras do nome do igroup existente para preencher o campo automaticamente. |

10. Na página Resumo, revise suas seleções e clique em **Concluir**.

    O SnapCenter conecta o LUN à unidade ou caminho de unidade especificado no host.

### Desconectar um disco

Você pode desconectar um LUN de um host sem afetar o conteúdo do LUN, com uma exceção: se você desconectar um clone antes que ele seja dividido, perderá o conteúdo do clone.

#### Antes de começar

- Certifique-se de que o LUN não esteja sendo usado por nenhum aplicativo.
- Certifique-se de que o LUN não esteja sendo monitorado com software de monitoramento.
- Se o LUN for compartilhado, certifique-se de remover as dependências de recursos do cluster do LUN e verifique se todos os nós no cluster estão ligados, funcionando corretamente e disponíveis para o SnapCenter.

**Sobre esta tarefa**

Se você desconectar um LUN em um volume FlexClone criado SnapCenter e nenhum outro LUN no volume estiver conectado, o SnapCenter excluirá o volume. Antes de desconectar o LUN, o SnapCenter exibe uma mensagem avisando que o volume FlexClone pode ser excluído.

Para evitar a exclusão automática do volume FlexClone , você deve renomear o volume antes de desconectar o último LUN. Ao renomear o volume, certifique-se de alterar vários caracteres além do último caractere do nome.

**Passos**

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Discos**.
3. Selecione o host na lista suspensa **Host**.

   Os discos estão listados.
4. Selecione o disco que você deseja desconectar e clique em **Desconectar**.
5. Na caixa de diálogo Desconectar disco, clique em **OK**.

   O SnapCenter desconecta o disco.

**Excluir um disco**

Você pode excluir um disco quando não precisar mais dele. Depois de excluir um disco, não é possível recuperá-lo.

**Passos**

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Discos**.
3. Selecione o host na lista suspensa **Host**.

   Os discos estão listados.
4. Selecione o disco que deseja excluir e clique em **Excluir**.
5. Na caixa de diálogo Excluir disco, clique em **OK**.

   O SnapCenter exclui o disco.

#### Crie e gerencie compartilhamentos SMB

## Para configurar um compartilhamento SMB3 em uma máquina virtual de armazenamento

(SVM), você pode usar a interface de usuário do SnapCenter ou cmdlets do PowerShell.

**Melhores práticas:** o uso de cmdlets é recomendado porque permite que você aproveite os modelos fornecidos com o SnapCenter para automatizar a configuração de compartilhamento.

Os modelos encapsulam as melhores práticas para configuração de volume e compartilhamento. Você pode encontrar os modelos na pasta Modelos na pasta de instalação do Pacote de plug-ins do SnapCenter para Windows.

Se você se sentir confortável, poderá criar seus próprios modelos seguindo os modelos fornecidos. Você deve revisar os parâmetros na documentação do cmdlet antes de criar um modelo personalizado.

### Criar um compartilhamento SMB

Você pode usar a página Compartilhamentos do SnapCenter para criar um compartilhamento SMB3 em uma máquina virtual de armazenamento (SVM).

Você não pode usar o SnapCenter para fazer backup de bancos de dados em compartilhamentos SMB. O suporte para PMEs é limitado apenas ao provisionamento.

**Passos**

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Compartilhamentos**.
3. Selecione a SVM na lista suspensa **Máquina Virtual de Armazenamento**.
4. Clique em **Novo**.

   A caixa de diálogo Novo compartilhamento é aberta.

5. Na caixa de diálogo Novo compartilhamento, defina o compartilhamento:

| Neste campo… | Faça isso… |
|---|---|
| Descrição | Insira um texto descritivo para o compartilhamento. |
| Nome do compartilhamento | Digite o nome do compartilhamento, por exemplo, test_share.<br><br>O nome que você inserir para o compartilhamento também será usado como nome do volume.<br><br>O nome da ação:<br><br>• Deve ser uma string UTF-8.<br>• Não deve incluir os seguintes caracteres: caracteres de controle de 0x00 a 0x1F (ambos inclusivos), 0x22 (aspas duplas) e caracteres especiais `\ / [ ] : (vertical bar) < > + = ; , ?` |

| Neste campo… | Faça isso… |
| --- | --- |
| Compartilhar caminho | • Clique no campo para inserir um novo caminho para o sistema de arquivos, por exemplo, /.<br>• Clique duas vezes no campo para selecionar em uma lista de caminhos de sistema de arquivos existentes. |

6. Quando estiver satisfeito com suas entradas, clique em **OK**.

   O SnapCenter cria o compartilhamento SMB no SVM.

### Excluir um compartilhamento SMB

Você pode excluir um compartilhamento SMB quando não precisar mais dele.

#### Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Compartilhamentos**.
3. Na página Compartilhamentos, clique no campo **Máquina Virtual de Armazenamento** para exibir uma lista suspensa com uma lista de máquinas virtuais de armazenamento (SVMs) disponíveis e selecione a SVM para o compartilhamento que você deseja excluir.
4. Na lista de compartilhamentos no SVM, selecione o compartilhamento que deseja excluir e clique em **Excluir**.
5. Na caixa de diálogo Excluir compartilhamento, clique em **OK**.

   O SnapCenter exclui o compartilhamento SMB do SVM.

#### Recupere espaço no sistema de armazenamento

Embora o NTFS rastreie o espaço disponível em um LUN quando os arquivos são excluídos ou modificados, ele não relata as novas informações ao sistema de armazenamento. Você pode executar o cmdlet de recuperação de espaço do PowerShell no host do Plug-in para Windows para garantir que os blocos recém-liberados sejam marcados como disponíveis no armazenamento.

Se estiver executando o cmdlet em um host de plug-in remoto, você deverá executar o cmdlet SnapCenterOpen-SMConnection para abrir uma conexão com o SnapCenter Server.

##### Antes de começar

- Você deve garantir que o processo de recuperação de espaço tenha sido concluído antes de executar uma operação de restauração.
- Se o LUN for compartilhado por hosts em um cluster de failover do Windows Server, você deverá executar a recuperação de espaço no host que possui o grupo de clusters.
- Para um desempenho ideal de armazenamento, você deve executar a recuperação de espaço com a maior frequência possível.

Você deve garantir que todo o sistema de arquivos NTFS tenha sido verificado.

### Sobre esta tarefa

- A recuperação de espaço consome muito tempo e exige muita CPU, por isso, geralmente, é melhor executar a operação quando o uso do sistema de armazenamento e do host Windows estiver baixo.
- A recuperação de espaço recupera quase todo o espaço disponível, mas não 100%.
- Você não deve executar a desfragmentação do disco ao mesmo tempo em que estiver recuperando espaço.

  Fazer isso pode atrasar o processo de recuperação.

### Etapa

No prompt de comando do PowerShell do servidor de aplicativos, digite o seguinte comando:

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

drive_path é o caminho da unidade mapeado para o LUN.

#### Provisionar armazenamento usando cmdlets do PowerShell

Se não quiser usar a GUI do SnapCenter para executar tarefas de provisionamento de host e recuperação de espaço, você pode usar os cmdlets do PowerShell. Você pode usar cmdlets diretamente ou adicioná-los a scripts.

Se estiver executando os cmdlets em um host de plug-in remoto, você deverá executar o cmdlet SnapCenter Open-SMConnection para abrir uma conexão com o SnapCenter Server.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Se os cmdlets do SnapCenter PowerShell estiverem quebrados devido à remoção do SnapDrive para Windows do servidor, consulte "Os cmdlets do SnapCenter são interrompidos quando o SnapDrive para Windows é desinstalado" .

### Provisionar armazenamento em ambientes VMware

Você pode usar o SnapCenter Plug-in para Microsoft Windows em ambientes VMware para criar e gerenciar LUNs e gerenciar Snapshots.

#### Plataformas de sistema operacional convidado VMware suportadas

- Versões suportadas do Windows Server
- Configurações de cluster da Microsoft

  Suporte para até 16 nós suportados no VMware ao usar o Microsoft iSCSI Software Initiator ou até dois nós usando FC

- LUNs RDM

Suporte para um máximo de 56 LUNs RDM com quatro controladores LSI Logic SCSI para RDMS normal ou 42 LUNs RDM com três controladores LSI Logic SCSI em um plug-in VMware VM MSCS box-to-box para configuração do Windows

Suporta o controlador SCSI VMware ParaVirtual. 256 discos podem ser suportados em discos RDM.

Para obter as informações mais recentes sobre as versões suportadas, consulte "Ferramenta de Matriz de Interoperabilidade da NetApp" .

**Limitações relacionadas ao servidor VMware ESXi**

- A instalação do Plug-in para Windows em um cluster da Microsoft em máquinas virtuais usando credenciais ESXi não é suportada.

  Você deve usar suas credenciais do vCenter ao instalar o Plug-in para Windows em máquinas virtuais em cluster.

- Todos os nós em cluster devem usar o mesmo ID de destino (no adaptador SCSI virtual) para o mesmo disco em cluster.
- Ao criar um RDM LUN fora do Plug-in para Windows, você deve reiniciar o serviço do plug-in para que ele reconheça o disco recém-criado.
- Não é possível usar iniciadores iSCSI e FC ao mesmo tempo em um sistema operacional convidado VMware.

**Privilégios mínimos do vCenter necessários para operações do SnapCenter RDM**

Você deve ter os seguintes privilégios do vCenter no host para executar operações RDM em um sistema operacional convidado:

- Armazenamento de dados: Remover arquivo
- Host: Configuração > Configuração da partição de armazenamento
- Máquina Virtual: Configuração

Você deve atribuir esses privilégios a uma função no nível do Virtual Center Server. A função à qual você atribui esses privilégios não pode ser atribuída a nenhum usuário sem privilégios de root.

Depois de atribuir esses privilégios, você pode instalar o Plug-in para Windows no sistema operacional convidado.

#### Gerenciar LUNs FC RDM em um cluster Microsoft

Você pode usar o Plug-in para Windows para gerenciar um cluster Microsoft usando LUNs FC RDM, mas primeiro você deve criar o quorum RDM compartilhado e o armazenamento compartilhado fora do plug-in e, em seguida, adicionar os discos às máquinas virtuais no cluster.

A partir do ESXi 5.5, você também pode usar hardware ESX iSCSI e FCoE para gerenciar um cluster Microsoft. O plug-in para Windows inclui suporte pronto para uso para clusters da Microsoft.

**Requisitos**

O plug-in para Windows fornece suporte para clusters da Microsoft usando LUNs FC RDM em duas máquinas virtuais diferentes que pertencem a dois servidores ESX ou ESXi diferentes, também conhecidos como cluster entre caixas, quando você atende a requisitos de configuração específicos.

- As máquinas virtuais (VMs) devem estar executando a mesma versão do Windows Server.
- As versões do servidor ESX ou ESXi devem ser as mesmas para cada host pai VMware.
- Cada host pai deve ter pelo menos dois adaptadores de rede.
- Deve haver pelo menos um armazenamento de dados do VMware Virtual Machine File System (VMFS) compartilhado entre os dois servidores ESX ou ESXi.
- A VMware recomenda que o armazenamento de dados compartilhado seja criado em um FC SAN.

  Se necessário, o armazenamento de dados compartilhado também pode ser criado via iSCSI.

- O LUN RDM compartilhado deve estar no modo de compatibilidade física.
- O LUN RDM compartilhado deve ser criado manualmente fora do Plug-in para Windows.

  Você não pode usar discos virtuais para armazenamento compartilhado.

- Um controlador SCSI deve ser configurado em cada máquina virtual no cluster no modo de compatibilidade física:

  O Windows Server 2008 R2 exige que você configure o controlador LSI Logic SAS SCSI em cada máquina virtual. LUNs compartilhados não podem usar o controlador SAS LSI Logic existente se houver apenas um de seu tipo e ele já estiver conectado à unidade C:.

  Controladores SCSI do tipo paravirtual não são suportados em clusters VMware Microsoft.

  > Ao adicionar um controlador SCSI a um LUN compartilhado em uma máquina virtual no modo de compatibilidade física, você deve selecionar a opção **Raw Device Mappings** (RDM) e não a opção **Criar um novo disco** no VMware Infrastructure Client.

- Os clusters de máquinas virtuais da Microsoft não podem fazer parte de um cluster VMware.
- Você deve usar credenciais do vCenter e não credenciais do ESX ou ESXi ao instalar o Plug-in para Windows em máquinas virtuais que pertencem a um cluster da Microsoft.
- O Plug-in para Windows não pode criar um único igroup com iniciadores de vários hosts.

  O igroup contendo os iniciadores de todos os hosts ESXi deve ser criado no controlador de armazenamento antes de criar os LUNs RDM que serão usados como discos de cluster compartilhados.

- Certifique-se de criar um RDM LUN no ESXi 5.0 usando um iniciador FC.

  Quando você cria um RDM LUN, um grupo iniciador é criado com ALUA.

### Limitações

O plug-in para Windows oferece suporte a clusters da Microsoft usando LUNs RDM FC/iSCSI em diferentes máquinas virtuais pertencentes a diferentes servidores ESX ou ESXi.

> Este recurso não é suportado em versões anteriores ao ESX 5.5i.

- O plug-in para Windows não oferece suporte a clusters em datastores ESX iSCSI e NFS.
- O Plug-in para Windows não oferece suporte a iniciadores mistos em um ambiente de cluster.

  Os iniciadores devem ser FC ou Microsoft iSCSI, mas não ambos.

- Os iniciadores iSCSI e HBAs do ESX não são suportados em discos compartilhados em um cluster da Microsoft.
- O plug-in para Windows não oferece suporte à migração de máquina virtual com o vMotion se a máquina virtual fizer parte de um cluster da Microsoft.
- O plug-in para Windows não oferece suporte a MPIO em máquinas virtuais em um cluster da Microsoft.

#### Criar um FC RDM LUN compartilhado

Antes de poder usar LUNs FC RDM para compartilhar armazenamento entre nós em um cluster Microsoft, você deve primeiro criar o disco de quorum compartilhado e o disco de armazenamento compartilhado e, em seguida, adicioná-los às duas máquinas virtuais no cluster.

O disco compartilhado não é criado usando o Plug-in para Windows. Você deve criar e adicionar o LUN compartilhado a cada máquina virtual no cluster. Para obter informações, consulte "Agrupar máquinas virtuais em hosts físicos" .

## Adicionar licenças baseadas no controlador SnapCenter Standard

Uma licença baseada em controlador SnapCenter Standard será necessária se você estiver usando controladores de armazenamento FAS, AFF ou ASA .

A licença baseada em controlador tem as seguintes características:

- O direito ao SnapCenter Standard está incluído na compra do Premium ou Flash Bundle (não no pacote básico)
- Uso de armazenamento ilimitado
- Adicionado diretamente ao controlador de armazenamento FAS, AFF ou ASA usando o ONTAP System Manager ou o ONTAP CLI.

> Não insira nenhuma informação de licença na interface do usuário do SnapCenter para as licenças baseadas no controlador SnapCenter .

- Bloqueado no número de série do controlador

Para obter informações sobre as licenças necessárias, consulte"Licenças SnapCenter" .

#### Etapa 1: Verifique se a licença do SnapManager Suite está instalada

Você pode usar a interface de usuário do SnapCenter para verificar se uma licença do SnapManager Suite está instalada nos sistemas de armazenamento primário FAS, AFF ou ASA e identificar quais sistemas precisam de licenças. As licenças do SnapManager Suite se aplicam somente a SVMs FAS, AFF e ASA ou clusters em sistemas de armazenamento primário.

> Se você já tiver uma licença do SnapManager Suite no seu controlador, o SnapCenter fornecerá automaticamente o direito à licença baseada no controlador padrão. Os nomes licença SnapManagerSuite e licença baseada em controlador SnapCenter Standard são usados de forma intercambiável, mas se referem à mesma licença.

**Passos**

1. No painel de navegação esquerdo, selecione **Sistemas de armazenamento**.

2. Na página Sistemas de Armazenamento, no menu suspenso **Tipo**, selecione se deseja visualizar todos os SVMs ou clusters que foram adicionados:
   - Para visualizar todos os SVMs que foram adicionados, selecione * ONTAP SVMs*.
   - Para visualizar todos os clusters que foram adicionados, selecione * Clusters ONTAP *.

     Quando você seleciona o nome do cluster, todas as SVMs que fazem parte do cluster são exibidas na seção Máquinas Virtuais de Armazenamento.
3. Na lista Conexões de armazenamento, localize a coluna Licença do controlador.

   A coluna Licença do Controlador exibe o seguinte status:

   -  indica que uma licença do SnapManager Suite está instalada em um sistema de armazenamento primário FAS, AFF ou ASA .
   -  indica que uma licença do SnapManager Suite não está instalada em um sistema de armazenamento primário FAS, AFF ou ASA .
   - Não aplicável indica que uma licença do SnapManager Suite não é aplicável porque o controlador de armazenamento está no Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select ou secundário.

**Etapa 2: Identificar as licenças instaladas no controlador**

Você pode usar a linha de comando ONTAP para visualizar todas as licenças instaladas no seu controlador. Você deve ser um administrador de cluster no sistema FAS, AFF ou ASA .

O controlador exibe a licença baseada no controlador SnapCenter Standard como a licença SnapManagerSuite.

**Passos**

1. Efetue login no controlador NetApp usando a linha de comando ONTAP .
2. Digite o comando license show e visualize a saída para ver se a licença do SnapManagerSuite está instalada.

**Exemplo de saída**

```
cluster1::> license show
(system license show)

Serial Number: 1-80-0000xx
Owner: cluster1
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
Base              site     Cluster Base License     -

Serial Number: 1-81-0000000000000000000000000xx
Owner: cluster1-01
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
NFS               license  NFS License              -
CIFS              license  CIFS License             -
iSCSI             license  iSCSI License            -
FCP               license  FCP License              -
SnapRestore       license  SnapRestore License      -
SnapMirror        license  SnapMirror License       -
FlexClone         license  FlexClone License        -
SnapVault         license  SnapVault License        -
SnapManagerSuite  license  SnapManagerSuite License -
```

No exemplo, a licença SnapManagerSuite está instalada, portanto, nenhuma ação adicional de licenciamento do SnapCenter é necessária.

### Etapa 3: recuperar o número de série do controlador

Obtenha o número de série do controlador usando a linha de comando ONTAP . Você deve ser um administrador de cluster no sistema FAS, AFF ou ASA para obter seu número de série de licença baseado em controlador.

**Passos**

1. Efetue login no controlador usando a linha de comando ONTAP .
2. Digite o comando show -instance do sistema e revise a saída para localizar o número de série do controlador.

**Exemplo de saída**

```
cluster1::> system show -instance

Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

Node: fas8080-41-42-02
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234512
Asset Tag: -
Uptime: 144 days 00:08
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. Registre os números de série.

### Etapa 4: recuperar o número de série da licença baseada no controlador

Se estiver usando armazenamento FAS, ASA ou AFF , você poderá recuperar a licença baseada no controlador SnapCenter no site de suporte da NetApp antes de instalá-lo usando a linha de comando ONTAP .

**Antes de começar**

- Você deve ter credenciais de login válidas no site de suporte da NetApp .

  Se você não inserir credenciais válidas, o sistema não retornará nenhuma informação para sua pesquisa.

- Você deve ter o número de série do controlador.

**Passos**

1. Faça login no "Site de suporte da NetApp" .
2. Navegue até **Sistemas** > **Licenças de software**.
3. Na área Critérios de seleção, certifique-se de que o Número de série (localizado na parte traseira da unidade) esteja selecionado, insira o número de série do controlador e selecione **Ir!**.


Uma lista de licenças para o controlador especificado é exibida.

4. Localize e registre a licença do SnapCenter Standard ou SnapManagerSuite.

### Etapa 5: adicionar licença baseada em controlador

Você pode usar a linha de comando ONTAP para adicionar uma licença baseada no controlador SnapCenter quando estiver usando sistemas FAS, AFF ou ASA e tiver uma licença SnapCenter Standard ou SnapManagerSuite.

**Antes de começar**

- Você deve ser um administrador de cluster no sistema FAS, AFF ou ASA .
- Você deve ter a licença SnapCenter Standard ou SnapManagerSuite.

**Sobre esta tarefa**

Se você quiser instalar o SnapCenter em caráter de teste com armazenamento FAS, AFF ou ASA , poderá obter uma licença de avaliação do Premium Bundle para instalar no seu controlador.

Se você quiser instalar o SnapCenter em caráter de teste, entre em contato com seu representante de vendas para obter uma licença de avaliação do Premium Bundle para instalar no seu controlador.

**Passos**

1. Efetue login no cluster NetApp usando a linha de comando ONTAP .
2. Adicione a chave de licença do SnapManagerSuite:

   ```
   system license add -license-code license_key
   ```

   Este comando está disponível no nível de privilégio de administrador.

3. Verifique se a licença do SnapManagerSuite está instalada:

   ```
   license show
   ```

#### Etapa 6: Remova a licença de teste

Se você estiver usando uma licença SnapCenter Standard baseada em controlador e precisar remover a licença de teste baseada em capacidade (número de série terminando em “50”), use os comandos MySQL para remover a licença de teste manualmente. A licença de teste não pode ser excluída usando a interface de usuário do SnapCenter .

> A remoção manual de uma licença de avaliação só é necessária se você estiver usando uma licença baseada no controlador SnapCenter Standard.

**Passos**

1. No SnapCenter Server, abra uma janela do PowerShell para redefinir a senha do MySQL.
   a. Execute o cmdlet Open-SmConnection para estabelecer conexão com o SnapCenter Server para uma conta SnapCenterAdmin.
   b. Execute o Set-SmRepositoryPassword para redefinir a senha do MySQL.

      Para obter informações sobre os cmdlets, consulte "Guia de referência do cmdlet do software SnapCenter" .
2. Abra o prompt de comando e execute mysql -u root -p para efetuar login no MySQL.

   O MySQL solicita a senha. Insira as credenciais que você forneceu ao redefinir a senha.
3. Remova a licença de teste do banco de dados:

```
use nsm;DELETE FROM nsm_License WHERE nsm_License_Serial_Number='510000050';
```

## Configurar alta disponibilidade

### Configurar servidores SnapCenter para alta disponibilidade

Para oferecer suporte à Alta Disponibilidade (HA) no SnapCenter em execução no Windows ou no Linux, você pode instalar o balanceador de carga F5. O F5 permite que o SnapCenter Server suporte configurações ativas-passivas em até dois hosts que estão no mesmo local. Para usar o F5 Load Balancer no SnapCenter, você deve configurar os servidores SnapCenter e configurar o balanceador de carga F5.

Você também pode configurar o Balanceamento de Carga de Rede (NLB) para configurar a Alta Disponibilidade do SnapCenter . Você deve configurar manualmente o NLB fora da instalação do SnapCenter para alta disponibilidade.

Para o ambiente de nuvem, você pode configurar alta disponibilidade usando o Amazon Web Services (AWS) Elastic Load Balancing (ELB) e o balanceador de carga do Azure.

**Configurar alta disponibilidade usando F5**

Para obter instruções sobre como configurar os servidores SnapCenter para alta disponibilidade usando o balanceador de carga F5, consulte "Como configurar servidores SnapCenter para alta disponibilidade usando o balanceador de carga F5" .

Você deve ser membro do grupo Administradores locais nos servidores SnapCenter (além de ter a função SnapCenterAdmin atribuída) para usar os seguintes cmdlets para adicionar e remover clusters F5:

- Adicionar-SmServerCluster
- Adicionar-SmServer
- Remover-SmServerCluster

  Para obter mais informações, consulte "Guia de referência do cmdlet do software SnapCenter" .

Informações adicionais

- Depois de instalar e configurar o SnapCenter para alta disponibilidade, edite o atalho da área de trabalho do SnapCenter para apontar para o IP do cluster F5.
- Se ocorrer um failover entre os servidores SnapCenter e se também houver uma sessão SnapCenter existente, você deverá fechar o navegador e fazer logon no SnapCenter novamente.
- Na configuração do balanceador de carga (NLB ou F5), se você adicionar um host que é parcialmente resolvido pelo host NLB ou F5 e se o host SnapCenter não conseguir contatá-lo, a página do host SnapCenter alternará frequentemente entre os hosts inativos e em execução. Para resolver esse problema, você deve garantir que ambos os hosts do SnapCenter consigam resolver o host no NLB ou no host F5.
- Os comandos do SnapCenter para configurações de MFA devem ser executados em todos os hosts. A configuração da parte confiável deve ser feita no servidor dos Serviços de Federação do Active Directory (AD FS) usando detalhes do cluster F5. O acesso à interface de usuário do SnapCenter no nível do host será bloqueado após a ativação do MFA.
- Durante o failover, as configurações do log de auditoria não serão refletidas no segundo host. Portanto, você deve repetir manualmente as configurações do log de auditoria no host passivo F5 quando ele se tornar ativo.

**Configurar alta disponibilidade usando balanceamento de carga de rede (NLB)**

Você pode configurar o Balanceamento de Carga de Rede (NLB) para configurar a Alta Disponibilidade do SnapCenter . Você deve configurar manualmente o NLB fora da instalação do SnapCenter para alta disponibilidade.

Para obter informações sobre como configurar o balanceamento de carga de rede (NLB) com o SnapCenter , consulte "Como configurar o NLB com o SnapCenter" .

**Configurar alta disponibilidade usando o AWS Elastic Load Balancing (ELB)**

Você pode configurar o ambiente SnapCenter de alta disponibilidade na Amazon Web Services (AWS) configurando dois servidores SnapCenter em zonas de disponibilidade (AZs) separadas e configurando-os para failover automático. A arquitetura inclui endereços IP privados virtuais, tabelas de roteamento e sincronização entre bancos de dados MySQL ativos e em espera.

**Passos**

1. Configurar sobreposição de IP virtual privado na AWS. Para obter informações, consulte "Configurar sobreposição de IP virtual privado" .
2. Prepare seu host Windows
    a. Forçar o IPv4 a ser priorizado em relação ao IPv6:
        - Localização: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
        - Chave: DisabledComponents
        - Tipo: REG_DWORD
        - Valor: 0x20
    b. Certifique-se de que os nomes de domínio totalmente qualificados possam ser resolvidos via DNS ou via configuração de host local para endereços IPv4.
    c. Certifique-se de que você não tenha um proxy de sistema configurado.
    d. Certifique-se de que a senha do administrador seja a mesma no Windows Server ao usar uma configuração sem um Active Directory e que os servidores não estejam no mesmo domínio.
    e. Adicione IP virtual em ambos os servidores Windows.
3. Crie o cluster SnapCenter .
    a. Inicie o Powershell e conecte-se ao SnapCenter. `Open-SmConnection`
    b. Crie o cluster. `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`
    c. Adicione o servidor secundário. `Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator`
    d. Obtenha os detalhes de alta disponibilidade. `Get-SmServerConfig`
4. Crie a função Lamda para ajustar a tabela de roteamento caso o ponto de extremidade do IP privado virtual fique indisponível, monitorado pelo AWS CloudWatch. Para obter informações, consulte "Criar uma função Lambda" .
5. Crie um monitor no CloudWatch para monitorar a disponibilidade do endpoint do SnapCenter . Um alarme é configurado para acionar uma função Lambda se o ponto de extremidade estiver inacessível. A função Lambda ajusta a tabela de roteamento para redirecionar o tráfego para o servidor SnapCenter ativo. Para obter informações, consulte "Crie canários sintéticos" .
6. Implemente o fluxo de trabalho usando uma função de etapa como alternativa ao monitoramento do CloudWatch, proporcionando tempos de failover menores. O fluxo de trabalho inclui uma função de sonda Lambda para testar o URL do SnapCenter , uma tabela do DynamoDB para armazenar contagens de falhas e a própria função Step.
    a. Use uma função lambda para sondar o URL do SnapCenter . Para obter informações, consulte "Criar função Lambda" .
    b. Crie uma tabela do DynamoDB para armazenar a contagem de falhas entre duas iterações da Função de Etapa. Para obter informações, consulte "Comece a usar a tabela do DynamoDB" .
    c. Crie a função Step. Para obter informações, consulte "Documentação da função Step" .
    d. Teste uma única etapa.
    e. Teste a função completa.
    f. Crie uma função do IAM e ajuste as permissões para poder executar a função do Lambda.
    g. Crie uma programação para acionar a Step Function. Para obter informações, consulte "Usando

o Amazon EventBridge Scheduler para iniciar um Step Functions" .

**Configurar alta disponibilidade usando o balanceador de carga do Azure**

Você pode configurar o ambiente SnapCenter de alta disponibilidade usando o balanceador de carga do Azure.

**Passos**

1. Crie máquinas virtuais em um conjunto de dimensionamento usando o portal do Azure. O conjunto de dimensionamento de máquinas virtuais do Azure permite que você crie e gerencie um grupo de máquinas virtuais com balanceamento de carga. O número de instâncias de máquinas virtuais pode aumentar ou diminuir automaticamente em resposta à demanda ou a um cronograma definido. Para obter informações, consulte "Crie máquinas virtuais em um conjunto de dimensionamento usando o portal do Azure" .
2. Depois de configurar as máquinas virtuais, efetue login em cada máquina virtual no conjunto de VMs e instale o SnapCenter Server em ambos os nós.
3. Crie o cluster no host 1. `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>`
4. Adicione o servidor secundário. `Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>`
5. Obtenha os detalhes de alta disponibilidade. `Get-SmServerConfig`
6. Se necessário, reconstrua o host secundário. `Set-SmRepositoryConfig -RebuildSlave -Verbose`
7. Failover para o segundo host. `Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose`

== Mude de NLB para F5 para alta disponibilidade

Você pode alterar a configuração do SnapCenter HA do Network Load Balancing (NLB) para usar o F5 Load Balancer.

**Passos**

1. Configure os servidores SnapCenter para alta disponibilidade usando F5. "Saber mais" .
2. No host do SnapCenter Server, inicie o PowerShell.
3. Inicie uma sessão usando o cmdlet Open-SmConnection e insira suas credenciais.
4. Atualize o SnapCenter Server para apontar para o endereço IP do cluster F5 usando o cmdlet Update-SmServerCluster.

   As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

**Alta disponibilidade para o repositório SnapCenter MySQL**

A replicação do MySQL é um recurso do MySQL Server que permite replicar dados de um servidor de banco de dados MySQL (mestre) para outro servidor de banco de dados

MySQL (escravo). O SnapCenter oferece suporte à replicação do MySQL para alta disponibilidade somente em dois nós habilitados para balanceamento de carga de rede (NLB).

O SnapCenter executa operações de leitura ou gravação no repositório mestre e roteia sua conexão para o repositório escravo quando há uma falha no repositório mestre. O repositório escravo então se torna o repositório mestre. O SnapCenter também oferece suporte à replicação reversa, que é ativada somente durante o failover.

Se você quiser usar o recurso de alta disponibilidade (HA) do MySQL, deverá configurar o Network Load Balancer (NLB) no primeiro nó. O repositório MySQL é instalado neste nó como parte da instalação. Ao instalar o SnapCenter no segundo nó, você deve ingressar no F5 do primeiro nó e criar uma cópia do repositório MySQL no segundo nó.

O SnapCenter fornece os cmdlets *Get-SmRepositoryConfig* e *Set-SmRepositoryConfig* do PowerShell para gerenciar a replicação do MySQL.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Você deve estar ciente das limitações relacionadas ao recurso MySQL HA:

- NLB e MySQL HA não são suportados além de dois nós.
- Não há suporte para alternar de uma instalação autônoma do SnapCenter para uma instalação NLB ou vice-versa e alternar de uma configuração autônoma do MySQL para o MySQL HA.
- O failover automático não será suportado se os dados do repositório escravo não estiverem sincronizados com os dados do repositório mestre.

  Você pode iniciar um failover forçado usando o cmdlet *Set-SmRepositoryConfig*.

- Quando o failover é iniciado, os trabalhos em execução podem falhar.

  Se o failover ocorrer porque o MySQL Server ou o SnapCenter Server estiver inativo, todos os trabalhos em execução poderão falhar. Após a falha no segundo nó, todos os trabalhos subsequentes são executados com sucesso.

Para obter informações sobre como configurar alta disponibilidade, consulte "Como configurar NLB e ARR com SnapCenter" .

## Configurar o controle de acesso baseado em função (RBAC)

### Criar uma função

Além de usar as funções existentes do SnapCenter , você pode criar suas próprias funções e personalizar as permissões.

Para criar suas próprias funções, é necessário efetuar login como a função "SnapCenterAdmin".

**Passos**

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Funções**.

3. Clique + .
4. Especifique um nome e uma descrição para a nova função.

   Somente os seguintes caracteres especiais podem ser usados em nomes de usuários e grupos: espaço ( ), hífen (-), sublinhado (_) e dois pontos (:).

5. Selecione **Todos os membros desta função podem ver os objetos de outros membros** para permitir que outros membros da função vejam recursos como volumes e hosts depois de atualizarem a lista de recursos.

   Você deve desmarcar esta opção se não quiser que os membros desta função vejam objetos aos quais outros membros estão atribuídos.

   Quando esta opção está habilitada, não é necessário atribuir aos usuários acesso a objetos ou recursos se eles pertencerem à mesma função que o usuário que criou os objetos ou recursos.

6. Na página Permissões, selecione as permissões que deseja atribuir à função ou clique em **Selecionar tudo** para conceder todas as permissões à função.
7. Clique em **Enviar**.

#### Adicionar uma função NetApp ONTAP RBAC usando comandos de login de segurança

Você pode usar os comandos de login de segurança para adicionar uma função NetApp ONTAP RBAC quando seus sistemas de armazenamento estiverem executando o ONTAP em cluster.

**Antes de começar**

- Identifique a tarefa (ou tarefas) que você deseja executar e os privilégios necessários para executá-las.
- Conceda privilégios a comandos e/ou diretórios de comandos.

  Há dois níveis de acesso para cada comando/diretório de comando: acesso total e somente leitura.

  Você deve sempre atribuir os privilégios de acesso total primeiro.

- Atribuir funções aos usuários.
- Identifique sua configuração dependendo se seus plug-ins do SnapCenter estão conectados ao IP do administrador do cluster para todo o cluster ou diretamente conectados a uma SVM dentro do cluster.

**Sobre esta tarefa**

Para simplificar a configuração dessas funções em sistemas de armazenamento, você pode usar a ferramenta RBAC User Creator for NetApp ONTAP , publicada no Fórum de Comunidades da NetApp .

Esta ferramenta gerencia automaticamente a configuração correta dos privilégios do ONTAP . Por exemplo, a ferramenta RBAC User Creator for NetApp ONTAP adiciona automaticamente os privilégios na ordem correta para que os privilégios de acesso total apareçam primeiro. Se você adicionar primeiro os privilégios somente leitura e depois adicionar os privilégios de acesso total, o ONTAP marcará os privilégios de acesso total como duplicados e os ignorará.

Se você atualizar posteriormente o SnapCenter ou o ONTAP, execute novamente a ferramenta RBAC User Creator for NetApp ONTAP para atualizar as funções de usuário criadas anteriormente. Funções de usuário criadas para uma versão anterior do SnapCenter ou ONTAP não funcionam corretamente com versões atualizadas. Quando você executa a ferramenta novamente, ela realiza a atualização automaticamente. Você não precisa recriar as funções.

Para obter mais informações sobre como configurar funções ONTAP RBAC, consulte "Guia de autenticação de administrador do ONTAP 9 e RBAC Power" .

**Passos**

1. No sistema de armazenamento, crie uma nova função inserindo o seguinte comando:

   ```
   security login role create <role_name\> -cmddirname "command" -access all
   -vserver <svm_name\>
   ```

   - svm_name é o nome do SVM. Se você deixar em branco, o padrão será o administrador do cluster.
   - role_name é o nome que você especifica para a função.
   - comando é o recurso ONTAP .

     Você deve repetir este comando para cada permissão. Lembre-se de que os comandos de acesso total devem ser listados antes dos comandos somente leitura.

   Para obter informações sobre a lista de permissões, consulte"Comandos ONTAP CLI para criar funções e atribuir permissões" .

2. Crie um nome de usuário digitando o seguinte comando:

   ```
   security login create -username <user_name\> -application ontapi -authmethod
   <password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment
   "user_description"
   ```

   - user_name é o nome do usuário que você está criando.
   - <senha> é sua senha. Se você não especificar uma senha, o sistema solicitará uma.
   - svm_name é o nome do SVM.

3. Atribua a função ao usuário digitando o seguinte comando:

   ```
   security login modify username <user_name\> -vserver <svm_name\> -role
   <role_name\> -application ontapi -application console -authmethod <password\>
   ```

   - <user_name> é o nome do usuário que você criou na Etapa 2. Este comando permite que você modifique o usuário para associá-lo à função.
   - <svm_name> é o nome do SVM.
   - <role_name> é o nome da função que você criou na Etapa 1.
   - <senha> é sua senha. Se você não especificar uma senha, o sistema solicitará uma.

4. Verifique se o usuário foi criado corretamente digitando o seguinte comando:

   ```
   security login show -vserver <svm_name\> -user-or-group-name <user_name\>
   ```

   user_name é o nome do usuário que você criou na Etapa 3.

#### Crie funções SVM com privilégios mínimos

Há vários comandos ONTAP CLI que você deve executar ao criar uma função para um novo usuário SVM no ONTAP. Essa função é necessária se você configurar SVMs no ONTAP para usar com o SnapCenter e não quiser usar a função vsadmin.

**Passos**

1. No sistema de armazenamento, crie uma função e atribua todas as permissões a ela.

```
security login role create –vserver <svm_name\>- role <SVM_Role_Name\>
-cmddirname <permission\>
```

   Você deve repetir este comando para cada permissão.

2. Crie um usuário e atribua a função a ele.

```
security login create -user <user_name\> -vserver <svm_name\> -application
ontapi -authmethod password -role <SVM_Role_Name\>
```

3. Desbloqueie o usuário.

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

##### Comandos ONTAP CLI para criar funções SVM e atribuir permissões

Há vários comandos ONTAP CLI que você deve executar para criar funções SVM e atribuir permissões.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"lun igroup create" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"volume qtree show" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all`

#### Criar funções SVM para sistemas ASA r2

Há vários comandos ONTAP CLI que você deve executar para criar uma função para um novo usuário SVM em sistemas ASA r2. Essa função é necessária se você configurar SVMs em sistemas ASA r2 para usar com o SnapCenter e não quiser usar a função

vsadmin.

**Passos**

1. No sistema de armazenamento, crie uma função e atribua todas as permissões a ela.

```
security login role create –vserver <svm_name\>- role <SVM_Role_Name\>
-cmddirname <permission\>
```

   Você deve repetir este comando para cada permissão.

2. Crie um usuário e atribua a função a ele.

```
security login create -user <user_name\> -vserver <svm_name\> -application
http -authmethod password -role <SVM_Role_Name\>
```

3. Desbloqueie o usuário.

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

#### Comandos ONTAP CLI para criar funções SVM e atribuir permissões

Há vários comandos ONTAP CLI que você deve executar para criar funções SVM e atribuir permissões.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"snapmirror show" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname

"vserver iscsi connection show" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "storage-unit show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "consistency-group" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all

- `security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name`
- `security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name`

#### Crie funções de cluster ONTAP com privilégios mínimos

Você deve criar uma função de cluster ONTAP com privilégios mínimos para não precisar usar a função de administrador ONTAP para executar operações no SnapCenter. Você pode executar vários comandos ONTAP CLI para criar a função de cluster ONTAP e atribuir privilégios mínimos.

**Passos**

1. No sistema de armazenamento, crie uma função e atribua todas as permissões a ela.

   ```
   security login role create –vserver <cluster_name\>- role <role_name\>
   -cmddirname <permission\>
   ```

   Você deve repetir este comando para cada permissão.

2. Crie um usuário e atribua a função a ele.

   ```
   security login create -user <user_name\> -vserver <cluster_name\> -application
   ontapi http -authmethod password -role <role_name\>
   ```

3. Desbloqueie o usuário.

   ```
   security login unlock -user <user_name\> -vserver <cluster_name\>
   ```

##### Comandos ONTAP CLI para criar funções de cluster e atribuir permissões

Há vários comandos ONTAP CLI que você deve executar para criar funções de cluster e atribuir permissões.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"lun online" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly

- `security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all`
- `security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"system node show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```
"vserver create" -access all
```

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all`

#### Criar funções de cluster ONTAP para sistemas ASA r2

Você deve criar uma função de cluster ONTAP com privilégios mínimos para não precisar usar a função de administrador ONTAP para executar operações no SnapCenter. Você pode executar vários comandos ONTAP CLI para criar a função de cluster ONTAP e atribuir privilégios mínimos.

**Passos**

1. No sistema de armazenamento, crie uma função e atribua todas as permissões a ela.

   ```
   security login role create –vserver <cluster_name\>- role <role_name\>
   -cmddirname <permission\>
   ```

   Você deve repetir este comando para cada permissão.

2. Crie um usuário e atribua a função a ele.

   ```
   security login create -user <user_name\> -vserver <cluster_name\> -application
   http -authmethod password -role <role_name\>
   ```

3. Desbloqueie o usuário.

   ```
   security login unlock -user <user_name\> -vserver <cluster_name\>
   ```

#### Comandos ONTAP CLI para criar funções de cluster e atribuir permissões

Há vários comandos ONTAP CLI que você deve executar para criar funções de cluster e atribuir permissões.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all`

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"nvme subsystem modify" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"volume snapshot modify-snaplock-expiry-time" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "storage-unit show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"consistency-group" show" -access all

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror protect" show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume delete" show" -access all`

#### Adicionar um usuário ou grupo e atribuir função e ativos

Para configurar o controle de acesso baseado em função para usuários do SnapCenter , você pode adicionar usuários ou grupos e atribuir uma função. A função determina as opções que os usuários do SnapCenter podem acessar.

**Antes de começar**

- Você deve ter efetuado login com a função "SnapCenterAdmin".
- Você deve ter criado as contas de usuário ou grupo no Active Directory no sistema operacional ou banco de dados. Você não pode usar o SnapCenter para criar essas contas.

  Você pode incluir somente os seguintes caracteres especiais em nomes de usuários e grupos: espaço ( ), hífen (-), sublinhado (_) e dois pontos (:).

- O SnapCenter inclui várias funções predefinidas.

  Você pode atribuir essas funções ao usuário ou criar novas funções.

- Usuários e grupos do AD adicionados ao SnapCenter RBAC devem ter permissão de LEITURA no contêiner de usuários e no contêiner de computadores no Active Directory.
- Depois de atribuir uma função a um usuário ou grupo que contém as permissões apropriadas, você deve atribuir ao usuário acesso aos ativos do SnapCenter , como hosts e conexões de armazenamento.

  Isso permite que os usuários executem as ações para as quais têm permissão nos ativos atribuídos a eles.

- Você deve atribuir uma função ao usuário ou grupo em algum momento para aproveitar as permissões e eficiências do RBAC.
- Você pode atribuir ativos como host, grupos de recursos, política, conexão de armazenamento, plug-in e credencial ao usuário ao criar o usuário ou grupo.
- Os ativos mínimos que você deve atribuir a um usuário para executar determinadas operações são os seguintes:

| Operação | Atribuição de ativos |
|---|---|
| Proteja os recursos | anfitrião, política |
| Backup | host, grupo de recursos, política |
| Restaurar | host, grupo de recursos |
| Clone | host, grupo de recursos, política |

| Operação | Atribuição de ativos |
| --- | --- |
| Ciclo de vida do clone | hospedar |
| Criar um Grupo de Recursos | hospedar |

- Quando um novo nó é adicionado a um cluster do Windows ou a um ativo DAG (Exchange Server Database Availability Group) e se esse novo nó for atribuído a um usuário, você deve reatribuir o ativo ao usuário ou grupo para incluir o novo nó ao usuário ou grupo.

  Você deve reatribuir o usuário ou grupo RBAC ao cluster ou DAG para incluir o novo nó ao usuário ou grupo RBAC. Por exemplo, você tem um cluster de dois nós e atribuiu um usuário ou grupo RBAC ao cluster. Ao adicionar outro nó ao cluster, você deve reatribuir o usuário ou grupo RBAC ao cluster para incluir o novo nó para o usuário ou grupo RBAC.

- Se você estiver planejando replicar Snapshots, deverá atribuir a conexão de armazenamento para o volume de origem e de destino ao usuário que está executando a operação.

  Você deve adicionar ativos antes de atribuir acesso aos usuários.

Se estiver usando as funções do SnapCenter Plug-in for VMware vSphere para proteger VMs, VMDKs ou datastores, você deverá usar a GUI do VMware vSphere para adicionar um usuário do vCenter a uma função do SnapCenter Plug-in for VMware vSphere . Para obter informações sobre funções do VMware vSphere, consulte "Funções predefinidas incluídas no SnapCenter Plug-in for VMware vSphere" .

**Passos**

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Usuários e acesso** > * *.
3. Na página Adicionar usuários/grupos do Active Directory ou grupo de trabalho:

| Para este campo… | Faça isso… |
| --- | --- |
| Tipo de acesso | Selecione Domínio ou grupo de trabalho<br><br>Para o tipo de autenticação de domínio, você deve especificar o nome de domínio do usuário ou grupo ao qual deseja adicionar o usuário a uma função.<br><br>Por padrão, ele é pré-preenchido com o nome de domínio conectado.<br><br>Você deve registrar o domínio não confiável na página **Configurações** > **Configurações globais** > **Configurações de domínio**. |

| Para este campo… | Faça isso… |
| --- | --- |
| Tipo | Selecione Usuário ou Grupo<br><br>O SnapCenter suporta apenas o grupo de segurança e não o grupo de distribuição. |
| Nome de usuário | a. Digite o nome de usuário parcial e clique em **Adicionar**.<br><br>O nome de usuário diferencia maiúsculas de minúsculas.<br><br>b. Selecione o nome de usuário na lista de pesquisa.<br><br>Ao adicionar usuários de um domínio diferente ou de um domínio não confiável, você deve digitar o nome do usuário completo, pois não há lista de pesquisa para usuários de vários domínios.<br><br>Repita esta etapa para adicionar usuários ou grupos adicionais à função selecionada. |
| Funções | Selecione a função à qual você deseja adicionar o usuário. |

4. Clique em **Atribuir** e, em seguida, na página Atribuir ativos:
   a. Selecione o tipo de ativo na lista suspensa **Ativo**.
   b. Na tabela Ativos, selecione o ativo.

      Os ativos são listados somente se o usuário os tiver adicionado ao SnapCenter.

   c. Repita esse procedimento para todos os ativos necessários.
   d. Clique em **Salvar**.
5. Clique em **Enviar**.

Depois de adicionar usuários ou grupos e atribuir funções, atualize a lista de recursos.

## Configurar definições de log de auditoria

Os logs de auditoria são gerados para cada atividade do SnapCenter Server. Por padrão, os logs de auditoria são protegidos no local de instalação padrão *C:\Arquivos de Programas\ NetApp\ SnapCenter WebApp\audit*.

Os logs de auditoria são protegidos por meio da geração de um resumo assinado digitalmente para cada evento de auditoria para protegê-lo de modificações não autorizadas. Os resumos gerados são mantidos no arquivo de soma de verificação de auditoria separado e passam por verificações periódicas de integridade para garantir a integridade do conteúdo.

Você deve ter efetuado login com a função "SnapCenterAdmin".

**Sobre esta tarefa**

- Os alertas são enviados nos seguintes cenários:
  - A verificação da integridade do log de auditoria ou o servidor Syslog está habilitado ou desabilitado
  - Verificação de integridade do log de auditoria, log de auditoria ou falha do log do servidor Syslog
  - Pouco espaço em disco
- O e-mail é enviado somente quando a verificação de integridade falha.
- Você deve modificar os caminhos do diretório do log de auditoria e do diretório do log de soma de verificação de auditoria juntos. Você não pode modificar apenas um deles.
- Quando os caminhos do diretório do log de auditoria e do diretório do log de soma de verificação de auditoria são modificados, a verificação de integridade não pode ser executada nos logs de auditoria presentes no local anterior.
- Os caminhos do diretório do log de auditoria e do diretório do log de soma de verificação de auditoria devem estar na unidade local do SnapCenter Server.

  Unidades compartilhadas ou montadas em rede não são suportadas.

- Se o protocolo UDP for usado nas configurações do servidor Syslog, erros devido a porta inativa ou indisponível não poderão ser capturados como um erro ou um alerta no SnapCenter.
- Você pode usar os comandos Set-SmAuditSettings e Get-SmAuditSettings para configurar os logs de auditoria.

  As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando Get-Help command_name. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

**Passos**

1. Na página **Configurações**, navegue até **Configurações** > **Configurações globais** > **Configurações do log de auditoria**.
2. Na seção Log de auditoria, insira os detalhes.
3. Entre no **diretório de log de auditoria** e no **diretório de log de soma de verificação de auditoria**
   a. Digite o tamanho máximo do arquivo
   b. Insira o máximo de arquivos de log
   c. Insira a porcentagem de uso do espaço em disco para enviar um alerta
4. (Opcional) Habilite **Registrar hora UTC**.
5. (Opcional) Habilite **Agendamento de verificação de integridade do log de auditoria** e clique em **Iniciar verificação de integridade** para verificação de integridade sob demanda.

   Você também pode executar o comando **Start-SmAuditIntegrityCheck** para iniciar a verificação de integridade sob demanda.

6. (Opcional) Habilite Logs de auditoria encaminhados para o servidor syslog remoto e insira os detalhes do servidor syslog.

   Você deve importar o certificado do servidor Syslog para a 'Raiz Confiável' para o protocolo TLS 1.2.

   a. Digite o host do servidor Syslog
   b. Digite a porta do servidor Syslog
   c. Digite o protocolo do servidor Syslog
   d. Insira o formato RFC
7. Clique em **Salvar**.
8. Você pode ver as verificações de integridade de auditoria e as verificações de espaço em disco clicando em **Monitor** > **Tarefas**.

## Configurar conexões MySQL seguras com o SnapCenter Server

Você pode gerar certificados Secure Sockets Layer (SSL) e arquivos de chave se quiser proteger a comunicação entre o SnapCenter Server e o MySQL Server em configurações autônomas ou configurações de balanceamento de carga de rede (NLB).

### Configurar conexões MySQL seguras para configurações autônomas do SnapCenter Server

Você pode gerar certificados Secure Sockets Layer (SSL) e arquivos de chave se quiser proteger a comunicação entre o SnapCenter Server e o MySQL Server. Você deve configurar os certificados e arquivos de chave no MySQL Server e no SnapCenter Server.

Os seguintes certificados são gerados:

- Certificado CA
- Certificado público do servidor e arquivo de chave privada
- Certificado público do cliente e arquivo de chave privada

**Passos**

1. Configure os certificados SSL e os arquivos de chave para servidores e clientes MySQL no Windows usando o comando openssl.

   Para obter informações, consulte "MySQL Versão 5.7: Criando Certificados e Chaves SSL Usando o OpenSSL"

   > O valor do nome comum usado para o certificado do servidor, o certificado do cliente e os arquivos de chave deve ser diferente do valor do nome comum usado para o certificado da CA. Se os valores de nome comum forem os mesmos, os arquivos de certificado e chave falharão para servidores compilados usando OpenSSL.

   **Melhores práticas:** você deve usar o nome de domínio totalmente qualificado (FQDN) do servidor como o nome comum para o certificado do servidor.
2. Copie os certificados SSL e os arquivos de chave para a pasta MySQL Data.

   O caminho padrão da pasta de dados do MySQL é `C:\ProgramData\NetApp\SnapCenter\MySQL`

`Data\Data\` .

3. Atualize o certificado da CA, o certificado público do servidor, o certificado público do cliente, a chave privada do servidor e os caminhos da chave privada do cliente no arquivo de configuração do servidor MySQL (my.ini).

   O caminho padrão do arquivo de configuração do servidor MySQL (my.ini) é `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini` .

   > Você deve especificar os caminhos do certificado CA, do certificado público do servidor e da chave privada do servidor na seção [mysqld] do arquivo de configuração do servidor MySQL (my.ini).

   Você deve especificar os caminhos do certificado CA, do certificado público do cliente e da chave privada do cliente na seção [cliente] do arquivo de configuração do servidor MySQL (my.ini).

   O exemplo a seguir mostra os certificados e arquivos de chave copiados para a seção [mysqld] do arquivo my.ini na pasta padrão `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data` .

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
   ```

   ```
   ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
   ```

   O exemplo a seguir mostra os caminhos atualizados na seção [client] do arquivo my.ini.

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
   ```

   ```
   ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
   ```

4. Pare o aplicativo Web SnapCenter Server no Internet Information Server (IIS).
5. Reinicie o serviço MySQL.
6. Atualize o valor da chave MySQLProtocol no arquivo SnapManager.Web.UI.dll.config.

   O exemplo a seguir mostra o valor da chave MySQLProtocol atualizada no arquivo

SnapManager.Web.UI.dll.config.

```
<add key="MySQLProtocol" value="SSL" />
```

7. Atualize o arquivo SnapManager.Web.UI.dll.config com os caminhos fornecidos na seção [client] do arquivo my.ini.

   O exemplo a seguir mostra os caminhos atualizados na seção [client] do arquivo my.ini.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

8. Inicie o aplicativo web SnapCenter Server no IIS.

**Configurar conexões MySQL seguras para configurações de HA**

Você pode gerar certificados Secure Sockets Layer (SSL) e arquivos de chave para os nós de Alta Disponibilidade (HA) se quiser proteger a comunicação entre o SnapCenter Server e os servidores MySQL. Você deve configurar os certificados e arquivos de chave nos servidores MySQL e nos nós HA.

Os seguintes certificados são gerados:

- Certificado CA

  Um certificado CA é gerado em um dos nós HA e esse certificado CA é copiado para o outro nó HA.

- Arquivos de certificado público do servidor e de chave privada do servidor para ambos os nós HA
- Arquivos de certificado público do cliente e de chave privada do cliente para ambos os nós HA

**Passos**

1. Para o primeiro nó HA, configure os certificados SSL e os arquivos de chave para servidores e clientes MySQL no Windows usando o comando openssl.

   Para obter informações, consulte "MySQL Versão 5.7: Criando Certificados e Chaves SSL Usando o OpenSSL"

O valor do nome comum usado para o certificado do servidor, o certificado do cliente e os arquivos de chave deve ser diferente do valor do nome comum usado para o certificado da CA. Se os valores de nome comum forem os mesmos, os arquivos de certificado e chave falharão para servidores compilados usando OpenSSL.

**Melhores práticas:** você deve usar o nome de domínio totalmente qualificado (FQDN) do servidor como o nome comum para o certificado do servidor.

2. Copie os certificados SSL e os arquivos de chave para a pasta MySQL Data.

   O caminho padrão da pasta de dados do MySQL é C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\Data\.

3. Atualize o certificado da CA, o certificado público do servidor, o certificado público do cliente, a chave privada do servidor e os caminhos da chave privada do cliente no arquivo de configuração do servidor MySQL (my.ini).

   O caminho padrão do arquivo de configuração do servidor MySQL (my.ini) é C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\my.ini.

   Você deve especificar os caminhos do certificado CA, do certificado público do servidor e da chave privada do servidor na seção [mysqld] do arquivo de configuração do servidor MySQL (my.ini).

   Você deve especificar os caminhos do certificado CA, do certificado público do cliente e da chave privada do cliente na seção [cliente] do arquivo de configuração do servidor MySQL (my.ini).

   O exemplo a seguir mostra os certificados e arquivos de chave copiados para a seção [mysqld] do arquivo my.ini na pasta padrão C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

   O exemplo a seguir mostra os caminhos atualizados na seção [client] do arquivo my.ini.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-
key.pem"
```

4. Para o segundo nó HA, copie o certificado CA e gere o certificado público do servidor, os arquivos de chave privada do servidor, o certificado público do cliente e os arquivos de chave privada do cliente. Execute as seguintes etapas:

   a. Copie o certificado CA gerado no primeiro nó HA para a pasta MySQL Data do segundo nó NLB.

      O caminho padrão da pasta de dados do MySQL é C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\Data\.

      > Você não deve criar um certificado de CA novamente. Você deve criar apenas o certificado público do servidor, o certificado público do cliente, o arquivo de chave privada do servidor e o arquivo de chave privada do cliente.

   b. Para o primeiro nó HA, configure os certificados SSL e os arquivos de chave para servidores e clientes MySQL no Windows usando o comando openssl.

      "MySQL Versão 5.7: Criando Certificados e Chaves SSL Usando o OpenSSL"

      > O valor do nome comum usado para o certificado do servidor, o certificado do cliente e os arquivos de chave deve ser diferente do valor do nome comum usado para o certificado da CA. Se os valores de nome comum forem os mesmos, os arquivos de certificado e chave falharão para servidores compilados usando OpenSSL.

      É recomendável usar o FQDN do servidor como o nome comum para o certificado do servidor.

   c. Copie os certificados SSL e os arquivos de chave para a pasta MySQL Data.

   d. Atualize o certificado da CA, o certificado público do servidor, o certificado público do cliente, a chave privada do servidor e os caminhos da chave privada do cliente no arquivo de configuração do servidor MySQL (my.ini).

      > Você deve especificar os caminhos do certificado CA, do certificado público do servidor e da chave privada do servidor na seção [mysqld] do arquivo de configuração do servidor MySQL (my.ini).

      Você deve especificar os caminhos do certificado CA, do certificado público do cliente e da chave privada do cliente na seção [cliente] do arquivo de configuração do servidor MySQL (my.ini).

      O exemplo a seguir mostra os certificados e arquivos de chave copiados para a seção [mysqld] do arquivo my.ini na pasta padrão C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data.

      ```
      ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
      ```

      ```
      ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-
      cert.pem"
      ```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-
key.pem"
```

O exemplo a seguir mostra os caminhos atualizados na seção [client] do arquivo my.ini.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

+

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-
cert.pem"
```

+

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-
key.pem"
```

5. Pare o aplicativo Web SnapCenter Server no Internet Information Server (IIS) em ambos os nós HA.
6. Reinicie o serviço MySQL em ambos os nós HA.
7. Atualize o valor da chave MySQLProtocol no arquivo SnapManager.Web.UI.dll.config para ambos os nós HA.

   O exemplo a seguir mostra o valor da chave MySQLProtocol atualizada no arquivo SnapManager.Web.UI.dll.config.

   ```
   <add key="MySQLProtocol" value="SSL" />
   ```

8. Atualize o arquivo SnapManager.Web.UI.dll.config com os caminhos que você especificou na seção [client] do arquivo my.ini para ambos os nós HA.

   O exemplo a seguir mostra os caminhos atualizados na seção [client] dos arquivos my.ini.

   ```
   <add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
   Data/Data/client-cert.pem" />
   ```

   ```
   <add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
   Data/Data/client-key.pem" />
   ```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

9. Inicie o aplicativo Web SnapCenter Server no IIS em ambos os nós HA.
10. Use o cmdlet Set-SmRepositoryConfig -RebuildSlave -Force do PowerShell com a opção -Force em um dos nós HA para estabelecer a replicação segura do MySQL em ambos os nós HA.

    Mesmo que o status da replicação seja saudável, a opção -Force permite reconstruir o repositório escravo.

# Configurar autenticação baseada em certificado

A autenticação baseada em certificado aumenta a segurança ao verificar a identidade do SnapCenter Server e dos hosts de plug-in, garantindo uma comunicação segura e criptografada.

## Habilitar autenticação baseada em certificado

Para habilitar a autenticação baseada em certificado para o SnapCenter Server e os hosts de plug-in do Windows, execute o seguinte cmdlet do PowerShell. Para os hosts de plug-in do Linux, a autenticação baseada em certificado será habilitada quando você habilitar o SSL bidirecional.

- Para habilitar a autenticação baseada em certificado de cliente:

  ```
  Set-SmConfigSettings -Agent –configSettings
  @{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
  ```

- Para desabilitar a autenticação baseada em certificado de cliente:

  ```
  Set-SmConfigSettings -Agent –configSettings
  @{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
  ```

## Exportar certificados de Autoridade Certificadora (CA) do SnapCenter Server

Você deve exportar os certificados de CA do SnapCenter Server para os hosts de plug-in usando o console de gerenciamento da Microsoft (MMC).

**Antes de começar**

Você deve ter configurado o SSL bidirecional.

**Passos**

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela Snap-in de Certificados, selecione a opção **Conta de Computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados - Computador local** > **Pessoal** > **Certificados**.
5. Clique com o botão direito do mouse no certificado CA adquirido, que é usado para o SnapCenter Server

e selecione **Todas as tarefas** > **Exportar** para iniciar o assistente de exportação.

6. Execute as seguintes ações no assistente.

| Para esta opção… | Faça o seguinte… |
|---|---|
| Exportar chave privada | Selecione **Não, não exportar a chave privada** e clique em **Avançar**. |
| Formato de arquivo de exportação | Clique em **Avançar**. |
| Nome do arquivo | Clique em **Procurar** e especifique o caminho do arquivo para salvar o certificado e clique em **Avançar**. |
| Concluindo o Assistente de Exportação de Certificados | Revise o resumo e clique em **Concluir** para iniciar a exportação. |

A autenticação baseada em certificado não é suportada para configurações do SnapCenter HA e do SnapCenter Plug-in for VMware vSphere.

## Importar certificado CA para hosts de plug-in do Windows

Para usar o certificado CA do SnapCenter Server exportado, você deve importar o certificado relacionado para os hosts do plug-in do SnapCenter Windows usando o console de gerenciamento da Microsoft (MMC).

**Passos**

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela Snap-in de Certificados, selecione a opção **Conta de Computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados - Computador local** > **Pessoal** > **Certificados**.
5. Clique com o botão direito do mouse na pasta “Pessoal” e selecione **Todas as Tarefas** > **Importar** para iniciar o assistente de importação.
6. Execute as seguintes ações no assistente.

| Para esta opção… | Faça o seguinte… |
|---|---|
| Localização da loja | Clique em **Avançar**. |
| Arquivo para importar | Selecione o certificado do SnapCenter Server que termina com a extensão .cer. |
| Loja de Certificados | Clique em **Avançar**. |
| Concluindo o Assistente de Exportação de Certificados | Revise o resumo e clique em **Concluir** para iniciar a importação. |

## Importar certificado CA para hosts de plug-in UNIX

Você deve importar o certificado da CA para os hosts do plug-in UNIX.

### Sobre esta tarefa

- Você pode gerenciar a senha do keystore SPL e o alias do par de chaves assinadas pela CA em uso.
- A senha para o keystore SPL e para todas as senhas de alias associadas da chave privada devem ser as mesmas.

### Passos

1. Você pode recuperar a senha padrão do keystore SPL a partir do arquivo de propriedades SPL. É o valor correspondente à chave `SPL_KEYSTORE_PASS` .
2. Alterar a senha do keystore: `$ keytool -storepasswd -keystore keystore.jks`
3. Altere a senha de todos os aliases de entradas de chave privada no keystore para a mesma senha usada para o keystore: `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. Atualize o mesmo para a chave SPL_KEYSTORE_PASS em `spl.properties` arquivo.
5. Reinicie o serviço após alterar a senha.

### Configurar certificados raiz ou intermediários para armazenamento confiável SPL

Você deve configurar os certificados raiz ou intermediários para o armazenamento confiável SPL. Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

### Passos

1. Navegue até a pasta que contém o keystore SPL: `/var/opt/snapcenter/spl/etc` .
2. Localize o arquivo `keystore.jks` .
3. Listar os certificados adicionados no keystore: `$ keytool -list -v -keystore keystore.jks`
4. Adicione um certificado raiz ou intermediário: `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. Reinicie o serviço após configurar os certificados raiz ou intermediários para o armazenamento confiável SPL.

### Configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL

Você deve configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL.

### Passos

1. Navegue até a pasta que contém o keystore do SPL `/var/opt/snapcenter/spl/etc` .
2. Localize o arquivo `keystore.jks` .
3. Listar os certificados adicionados no keystore: `$ keytool -list -v -keystore keystore.jks`
4. Adicione o certificado da CA com chave privada e pública. `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore`

`keystore.jks -deststoretype JKS`

5. Listar os certificados adicionados no keystore. `$ keytool -list -v -keystore keystore.jks`
6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

   A senha padrão do keystore SPL é o valor da chave SPL_KEYSTORE_PASS em `spl.properties` arquivo.

   `$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`

8. Se o nome do alias no certificado da CA for longo e contiver espaços ou caracteres especiais ("*",","), altere o nome do alias para um nome simples: `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
9. Configure o nome do alias do keystore localizado em `spl.properties` arquivo. Atualize este valor em relação à chave SPL_CERTIFICATE_ALIAS.
10. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL.

## Exportar certificados SnapCenter

Você deve exportar os certificados do SnapCenter no formato .pfx.

**Passos**

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snap-in**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Minha conta de usuário** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados - Usuário atual** > **Autoridades de certificação raiz confiáveis** > **Certificados**.
5. Clique com o botão direito do mouse no certificado que tem o Nome amigável do SnapCenter e selecione **Todas as tarefas** > **Exportar** para iniciar o assistente de exportação.
6. Conclua o assistente da seguinte forma:

| Nesta janela do assistente… | Faça o seguinte… |
|---|---|
| Exportar chave privada | Selecione a opção **Sim, exportar a chave privada** e clique em **Avançar**. |
| Formato de arquivo de exportação | Não faça alterações; clique em **Avançar**. |
| Segurança | Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**. |

| Nesta janela do assistente… | Faça o seguinte… |
| --- | --- |
| Arquivo para Exportar | Especifique um nome de arquivo para o certificado exportado (você deve usar .pfx) e clique em **Avançar**. |
| Concluindo o Assistente de Exportação de Certificados | Revise o resumo e clique em **Concluir** para iniciar a exportação. |

# Configurar certificado CA para host Windows

## Gerar arquivo CSR de certificado CA

Você pode gerar uma Solicitação de Assinatura de Certificado (CSR) e importar o certificado que pode ser obtido de uma Autoridade de Certificação (CA) usando o CSR gerado. O certificado terá uma chave privada associada a ele.

CSR é um bloco de texto codificado que é fornecido a um fornecedor de certificado autorizado para obter o certificado de CA assinado.

O comprimento mínimo da chave RSA do certificado CA deve ser de 3072 bits.

Para obter informações sobre como gerar um CSR, consulte "Como gerar um arquivo CSR de certificado CA" .

Se você possui o certificado CA para seu domínio (*.domain.company.com) ou seu sistema (machine1.domain.company.com), você pode pular a geração do arquivo CSR do certificado CA. Você pode implantar o certificado CA existente com o SnapCenter.

Para configurações de cluster, o nome do cluster (FQDN do cluster virtual) e os respectivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome Alternativo do Assunto (SAN) antes de adquirir o certificado. Para um certificado curinga (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

## Importar certificados de CA

Você deve importar os certificados de CA para o SnapCenter Server e os plug-ins do host do Windows usando o console de gerenciamento da Microsoft (MMC).

**Passos**

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados – Computador local** > **Autoridades de certificação raiz confiáveis** > **Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione

**Todas as Tarefas** > **Importar** para iniciar o assistente de importação.

6. Conclua o assistente da seguinte forma:

| Nesta janela do assistente… | Faça o seguinte… |
|---|---|
| Importar chave privada | Selecione a opção **Sim**, importe a chave privada e clique em **Avançar**. |
| Formato de arquivo de importação | Não faça alterações; clique em **Avançar**. |
| Segurança | Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**. |
| Concluindo o Assistente de Importação de Certificados | Revise o resumo e clique em **Concluir** para iniciar a importação. |

O certificado de importação deve ser agrupado com a chave privada (os formatos suportados são: *.pfx, *.p12 e *.p7b).

7. Repita a Etapa 5 para a pasta “Pessoal”.

## Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma sequência hexadecimal que identifica um certificado. Uma impressão digital é calculada a partir do conteúdo do certificado usando um algoritmo de impressão digital.

**Passos**

1. Execute o seguinte na GUI:
   a. Clique duas vezes no certificado.
   b. Na caixa de diálogo Certificado, clique na guia **Detalhes**.
   c. Percorra a lista de campos e clique em **Impressão digital**.
   d. Copie os caracteres hexadecimais da caixa.
   e. Remova os espaços entre os números hexadecimais.

      Por exemplo, se a impressão digital for: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:
   a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

      *Get-ChildItem -Path Cert:\LocalMachine\My*

   b. Copie a impressão digital.

## Configurar certificado CA com serviços de plug-in de host do Windows

Você deve configurar o certificado CA com os serviços de plug-in do host do Windows para ativar o certificado digital instalado.

Execute as seguintes etapas no SnapCenter Server e em todos os hosts de plug-in onde os certificados CA já estão implantados.

**Passos**

1. Remova a vinculação de certificado existente com a porta padrão 8145 do SMCore, executando o seguinte comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Por exemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Vincule o certificado recém-instalado aos serviços de plug-in do host
   do Windows, executando os seguintes comandos:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Por exemplo:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

## Configurar certificado CA com o site SnapCenter

Você deve configurar o certificado CA com o site SnapCenter no host Windows.

**Passos**

1. Abra o Gerenciador do IIS no Windows Server onde o SnapCenter está instalado.
2. No painel de navegação esquerdo, clique em **Conexões**.
3. Expanda o nome do servidor e **Sites**.
4. Selecione o site do SnapCenter no qual você deseja instalar o Certificado SSL.
5. Navegue até **Ações** > **Editar site** e clique em **Vinculações**.
6. Na página Ligações, selecione **ligação para https**.

7. Clique em **Editar**.
8. Na lista suspensa do certificado SSL, selecione o certificado SSL importado recentemente.
9. Clique em **OK**.

> O site do SnapCenter Scheduler (porta padrão: 8154, HTTPS) é configurado com certificado autoassinado. Esta porta está se comunicando dentro do host do SnapCenter Server e não é obrigatório configurá-la com um certificado CA. No entanto, se o seu ambiente exigir que você use um Certificado CA, repita as etapas 5 a 9 usando o site SnapCenter Scheduler.

> Se o certificado CA implantado recentemente não estiver listado no menu suspenso, verifique se o certificado CA está associado à chave privada.

> Certifique-se de que o certificado seja adicionado usando o seguinte caminho: **Raiz do console > Certificados – Computador local > Autoridades de certificação raiz confiáveis > Certificados**.

## Habilitar certificados CA para SnapCenter

Você deve configurar os certificados CA e habilitar a validação do certificado CA para o SnapCenter Server.

**Antes de começar**

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet Set-SmCertificateSettings.
- Você pode exibir o status do certificado do SnapCenter Server usando o cmdlet Get-SmCertificateSettings.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

**Passos**

1. Na página Configurações, navegue até **Configurações** > **Configurações globais** > **Configurações do certificado CA**.
2. Selecione **Ativar validação de certificado**.
3. Clique em **Aplicar**.

**Depois que você terminar**

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- * * indica que não há nenhum certificado CA habilitado ou atribuído ao host do plug-in.
- * * indica que o certificado CA foi validado com sucesso.
- * * indica que o certificado CA não pôde ser validado.
- * * indica que as informações de conexão não puderam ser recuperadas.

Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

# Configurar certificado CA para host Linux

Após instalar o SnapCenter Server no Linux, o instalador cria o certificado autoassinado. Se quiser usar o certificado CA, você deve configurar os certificados para o proxy reverso nginx, registro de auditoria e serviços do SnapCenter .

## Configurar certificado nginx

**Passos**

1. Navegue até */etc/nginx/conf.d*: `cd /etc/nginx/conf.d`
2. Abra **snapcenter.conf** usando o vi ou qualquer editor de texto.
3. Navegue até a seção do servidor no arquivo de configuração.
4. Modifique os caminhos de *ssl_certificate* e *ssl_certificate_key* para apontar para o certificado CA.
5. Salve e feche o arquivo.
6. Recarregue o nginx: `$nginx -s reload`

## Configurar certificado de log de auditoria

**Passos**

1. Abra *INSTALL_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config* usando o vi ou qualquer editor de texto.

   O valor padrão de *INSTALL_DIR* é */opt*.

2. Edite as chaves **AUDILOG_CERTIFICATE_PATH** e **AUDILOG_CERTIFICATE_PASSWORD** para incluir o caminho do certificado CA e a senha, respectivamente.

   Somente o formato *.pfx* é suportado para certificado de log de auditoria.

3. Salve e feche o arquivo.
4. Reinicie o serviço **snapmanagerweb**: `$ systemctl restart snapmanagerweb`

## Configurar certificado de serviços do SnapCenter

**Passos**

1. Abra os seguintes arquivos de configuração usando o vi ou qualquer editor de texto.
   - *INSTALL_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config*
   - *INSTALL_DIR/ NetApp/snapcenter/SMCore/SMCoreServiceHost.dll.config*
   - *INSTALL_DIR/ NetApp/snapcenter/Scheduler/Scheduler.Api.dll.config*

   O valor padrão de *INSTALL_DIR* é */opt*.

2. Edite as chaves **SERVICE_CERTIFICATE_PATH** e **SERVICE_CERTIFICATE_PASSWORD** para incluir o caminho do certificado da CA e a senha, respectivamente.

Somente o formato *.pfx* é suportado para o certificado de serviços do SnapCenter .

3. Salve e feche os arquivos.
4. Reinicie todos os serviços.
   - `$ systemctl restart snapmanagerweb`
   - `$ systemctl restart smcore`
   - `$ systemctl restart scheduler`

# Configurar e habilitar a comunicação SSL bidirecional no host Windows

## Configurar comunicação SSL bidirecional no host Windows

Você deve configurar a comunicação SSL bidirecional para proteger a comunicação mútua entre o SnapCenter Server no host Windows e os plug-ins.

**Antes de começar**

- Você deve ter gerado o arquivo CSR do certificado CA com o comprimento mínimo de chave suportado de 3072.
- O certificado da CA deve oferecer suporte à autenticação do servidor e à autenticação do cliente.
- Você deve ter um certificado de CA com chave privada e detalhes de impressão digital.
- Você deve ter habilitado a configuração SSL unidirecional.

  Para mais detalhes, veja "Seção Configurar certificado CA."

- Você deve ter habilitado a comunicação SSL bidirecional em todos os hosts de plug-in e no SnapCenter Server.

  Ambientes com alguns hosts ou servidores não habilitados para comunicação SSL bidirecional não são suportados.

**Passos**

1. Para vincular a porta, execute as seguintes etapas no host do SnapCenter Server para a porta 8146 do servidor web SnapCenter IIS (padrão) e novamente para a porta 8145 do SMCore (padrão) usando comandos do PowerShell.

   a. Remova a vinculação de porta do certificado autoassinado existente do SnapCenter usando o seguinte comando do PowerShell.

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
      ```

      Por exemplo,

      ```
      > netsh http delete sslcert ipport=0.0.0.0:8145

      > netsh http delete sslcert ipport=0.0.0.0:8146
      ```

   b. Vincule o certificado CA recém-adquirido ao servidor SnapCenter e à porta SMCore.

```
> $cert = "<CA_certificate thumbprint>"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>
certhash=$cert appid="$guid" clientcertnegotiation=enable
verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

Por exemplo,

```
> $cert = "abc123abc123abc123abc123"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8146

> netsh http show sslcert ipport=0.0.0.0:8145
```

2. Para acessar a permissão para o certificado da CA, adicione o usuário do servidor web IIS padrão do SnapCenter "**IIS AppPool\ SnapCenter**" na lista de permissões de certificado executando as seguintes etapas para acessar o certificado da CA recém-adquirido.
   a. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover SnapIn**.
   b. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
   c. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
   d. Clique em **Console Root** > **Certificados – Computador local** > **Pessoal** > **Certificados**.
   e. Selecione o certificado SnapCenter .
   f. Para iniciar o assistente para adicionar usuário/permissão, clique com o botão direito do mouse no certificado da CA e selecione **Todas as tarefas** > **Gerenciar chaves privadas**.
   g. Clique em **Adicionar**, no assistente Selecionar usuários e grupos altere o local para o nome do computador local (o mais alto na hierarquia)
   h. Adicione o usuário IIS AppPool\ SnapCenter e conceda permissões de controle total.
3. Para **permissão do certificado CA IIS**, adicione a nova entrada de chaves de registro DWORD no SnapCenter Server a partir do seguinte caminho:

   No editor de registro do Windows, navegue até o caminho mencionado abaixo,

   ```
   HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv ders\SCHANNEL
   ```

4. Crie uma nova entrada de chave de registro DWORD no contexto da configuração do registro SCHANNEL.

```
SendTrustedIssuerList = 0

ClientAuthTrustMode = 2
```

### Configurar o plug-in SnapCenter do Windows para comunicação SSL bidirecional

Você deve configurar o plug-in SnapCenter do Windows para comunicação SSL bidirecional usando comandos do PowerShell.

#### Antes de começar

Certifique-se de que a impressão digital do certificado da CA esteja disponível.

#### Passos

1. Para vincular a porta, execute as seguintes ações no host do plug-in do Windows para a porta 8145 do SMCore (padrão).

   a. Remova a vinculação de porta do certificado autoassinado existente do SnapCenter usando o seguinte comando do PowerShell.

   ```
   > netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
   ```

   Por exemplo,

   ```
   > netsh http delete sslcert ipport=0.0.0.0:8145
   ```

   b. Vincule o certificado CA recém-adquirido à porta SMCore.

   ```
   > $cert = "<CA_certificate thumbprint>"

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
   appid="$guid" clientcertnegotiation=enable
   verifyclientcertrevocation=disable

   > netsh http show sslcert ipport=0.0.0.0:<SMCore Port>
   ```

   Por exemplo,

   ```
   > $cert = "abc123abc123abc123abc123"

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
   clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8145
```

## Habilitar comunicação SSL bidirecional no host Windows

Você pode habilitar a comunicação SSL bidirecional para proteger a comunicação mútua entre o SnapCenter Server no host Windows e os plug-ins usando comandos do PowerShell.

### Antes de começar

Execute os comandos para todos os plug-ins e o agente SMCore primeiro e depois para o servidor.

### Passos

1. Para habilitar a comunicação SSL bidirecional, execute os seguintes comandos no SnapCenter Server para os plug-ins, o servidor e para cada um dos agentes para os quais a comunicação SSL bidirecional é necessária.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName <Plugin_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. Execute a operação de reciclagem do pool de aplicativos do IIS SnapCenter usando o seguinte comando.
   `> Restart-WebAppPool -Name "SnapCenter"`
3. Para plug-ins do Windows, reinicie o serviço SMCore executando o seguinte comando do PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

### Desabilitar comunicação SSL bidirecional

Você pode desabilitar a comunicação SSL bidirecional usando comandos do PowerShell.

### Sobre esta tarefa

- Execute os comandos para todos os plug-ins e o agente SMCore primeiro e depois para o servidor.
- Quando você desabilita a comunicação SSL bidirecional, o certificado da CA e sua configuração não são removidos.
- Para adicionar um novo host ao SnapCenter Server, você deve desabilitar o SSL bidirecional para todos os hosts de plug-in.
- NLB e F5 não são suportados.

### Passos

1. Para desabilitar a comunicação SSL bidirecional, execute os seguintes comandos no SnapCenter Server para todos os hosts de plug-in e o host SnapCenter .

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName <Agent_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. Execute a operação de reciclagem do pool de aplicativos do IIS SnapCenter usando o seguinte comando.
   `> Restart-WebAppPool -Name "SnapCenter"`
3. Para plug-ins do Windows, reinicie o serviço SMCore executando o seguinte comando do PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

# Configurar e habilitar comunicação SSL bidirecional no host Linux

## Configurar comunicação SSL bidirecional no host Linux

Você deve configurar a comunicação SSL bidirecional para proteger a comunicação mútua entre o SnapCenter Server no host Linux e os plug-ins.

**Antes de começar**

- Você deve ter configurado o certificado CA para o host Linux.
- Você deve ter habilitado a comunicação SSL bidirecional em todos os hosts de plug-in e no SnapCenter Server.

**Passos**

1. Copie **certificate.pem** para */etc/pki/ca-trust/source/anchors/*.
2. Adicione os certificados na lista de confiança do seu host Linux.
   - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
   - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
   - `update-ca-trust extract`
3. Verifique se os certificados foram adicionados à lista de confiança. `trust list | grep "<CN of your certificate>"`
4. Atualize **ssl_certificate** e **ssl_certificate_key** no arquivo SnapCenter **nginx** e reinicie.
   - `vim /etc/nginx/conf.d/snapcenter.conf`
   - `systemctl restart nginx`
5. Atualize o link da GUI do SnapCenter Server.
6. Atualize os valores das seguintes chaves em * SnapManager.Web.UI.dll.config* localizado em _ /<caminho de instalação>/ NetApp/snapcenter/SnapManagerWeb_ e **SMCoreServiceHost.dll.config** localizado em */<caminho de instalação>/ NetApp/snapcenter/SMCore*.
   - <add key="SERVICE_CERTIFICATE_PATH" value="<caminho do certificado.pfx>" />
   - <adicionar chave="SENHA_DO_CERTIFICADO_DE_SERVIÇO" valor="<senha>"/>
7. Reinicie os seguintes serviços.
   - `systemctl restart smcore.service`

- `systemctl restart snapmanagerweb.service`

8. Verifique se o certificado está anexado à porta da web do SnapManager . `openssl s_client -connect localhost:8146 -brief`
9. Verifique se o certificado está anexado à porta smcore. `openssl s_client -connect localhost:8145 -brief`
10. Gerenciar senha para keystore e alias SPL.
    a. Recupere a senha padrão do keystore SPL atribuída à chave **SPL_KEYSTORE_PASS** no arquivo de propriedades SPL.
    b. Alterar a senha do keystore. `keytool -storepasswd -keystore keystore.jks`
    c. Altere a senha de todos os aliases de entradas de chave privada. `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
    d. Atualize a mesma senha para a chave **SPL_KEYSTORE_PASS** em *spl.properties*.
    e. Reinicie o serviço.
11. No host Linux do plug-in, adicione os certificados raiz e intermediário no keystore do plug-in SPL.
    - `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`
    - `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`
        i. Verifique as entradas em keystore.jks. `keytool -list -v -keystore <path to keystore.jks>`
        ii. Renomeie qualquer alias, se necessário. `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`
12. Atualize o valor de **SPL_CERTIFICATE_ALIAS** no arquivo *spl.properties* com o alias de **certificate.pfx** armazenado em *keystore.jks* e reinicie o serviço SPL: `systemctl restart spl`
13. Verifique se o certificado está anexado à porta smcore. `openssl s_client -connect localhost:8145 -brief`

## Habilitar comunicação SSL no host Linux

Você pode habilitar a comunicação SSL bidirecional para proteger a comunicação mútua entre o SnapCenter Server no host Linux e os plug-ins usando comandos do PowerShell.

**Etapa**

1. Execute o seguinte para habilitar a comunicação SSL unidirecional.
    a. Efetue login na interface gráfica do usuário do SnapCenter .
    b. Clique em **Configurações** > **Configurações globais** e selecione **Ativar validação de certificado no SnapCenter Server**.
    c. Clique em **Hosts** > **Hosts gerenciados** e selecione o host do plug-in para o qual você deseja habilitar o SSL unidirecional.

d. Clique ícone e clique em **Ativar validação de certificado**.

2. Habilite a comunicação SSL bidirecional do host Linux do SnapCenter Server.
   - `Open-SmConnection`
   - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>`
   - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost`
   - `Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}`

# Configurar Active Directory, LDAP e LDAPS

## Registrar domínios não confiáveis do Active Directory

Você deve registrar o Active Directory com o SnapCenter Server para gerenciar hosts, usuários e grupos de vários domínios não confiáveis do Active Directory.

**Antes de começar**

**Protocolos LDAP e LDAPS**

- Você pode registrar domínios não confiáveis do Active Directory usando o protocolo LDAP ou LDAPS.
- Você deve ter habilitado a comunicação bidirecional entre os hosts do plug-in e o SnapCenter Server.
- A resolução de DNS deve ser configurada do SnapCenter Server para os hosts de plug-in e vice-versa.

**Protocolo LDAP**

- O nome de domínio totalmente qualificado (FQDN) deve ser resolvível no SnapCenter Server.

  Você pode registrar um domínio não confiável com o FQDN. Se o FQDN não puder ser resolvido no SnapCenter Server, você poderá registrar com um endereço IP de controlador de domínio, e isso poderá ser resolvido no SnapCenter Server.

**Protocolo LDAPS**

- Os certificados CA são necessários para que o LDAPS forneça criptografia de ponta a ponta durante a comunicação do diretório ativo.

  "Configurar certificado de cliente CA para LDAPS"

- Os nomes de host do controlador de domínio (DCHostName) devem ser acessíveis pelo SnapCenter Server.

**Sobre esta tarefa**

- Você pode usar a interface de usuário do SnapCenter , os cmdlets do PowerShell ou a API REST para registrar um domínio não confiável.

**Passos**

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Configurações globais**.
3. Na página Configurações globais, clique em **Configurações de domínio**.
4. Clique + para registrar um novo domínio.
5. Na página Registrar novo domínio, selecione **LDAP** ou **LDAPS**.
   a. Se você selecionar **LDAP**, especifique as informações necessárias para registrar o domínio não confiável para LDAP:

| Para este campo… | Faça isso… |
|---|---|
| Nome de domínio | Especifique o nome NetBIOS para o domínio. |
| FQDN de domínio | Especifique o FQDN e clique em **Resolver**. |
| Endereços IP do controlador de domínio | Se o FQDN do domínio não puder ser resolvido no SnapCenter Server, especifique um ou mais endereços IP do controlador de domínio.<br><br>Para obter mais informações, consulte "Adicionar IP do controlador de domínio para domínio não confiável da GUI" . |

   b. Se você selecionar **LDAPS**, especifique as informações necessárias para registrar o domínio não confiável para LDAPS:

| Para este campo… | Faça isso… |
|---|---|
| Nome de domínio | Especifique o nome NetBIOS para o domínio. |
| FQDN de domínio | Especifique o FQDN. |
| Nomes de controladores de domínio | Especifique um ou mais nomes de controladores de domínio e clique em **Resolver**. |
| Endereços IP do controlador de domínio | Se os nomes dos controladores de domínio não puderem ser resolvidos pelo SnapCenter Server, você deverá retificar as resoluções de DNS. |

6. Clique em **OK**.

## Configurar pools de aplicativos do IIS para habilitar permissões de leitura do Active Directory

Você pode configurar o Internet Information Services (IIS) no seu Windows Server para criar uma conta personalizada do Application Pool quando precisar habilitar permissões de leitura do Active Directory para o SnapCenter.

**Passos**

1. Abra o Gerenciador do IIS no Windows Server onde o SnapCenter está instalado.
2. No painel de navegação esquerdo, clique em **Pools de aplicativos**.
3. Selecione SnapCenter na lista Pools de aplicativos e clique em **Configurações avançadas** no painel Ações.
4. Selecione Identidade e clique em **…** para editar a identidade do pool de aplicativos do SnapCenter .
5. No campo Conta personalizada, insira um nome de conta de usuário ou administrador de domínio com permissão de leitura do Active Directory.
6. Clique em OK.

   A conta personalizada substitui a conta ApplicationPoolIdentity interna para o pool de aplicativos SnapCenter .

## Configurar certificado de cliente CA para LDAPS

Você deve configurar o certificado do cliente CA para LDAPS no SnapCenter Server quando o Windows Active Directory LDAPS estiver configurado com os certificados CA.

**Passos**

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados – Computador local** > **Autoridades de certificação raiz confiáveis** > **Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas** > **Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

| Nesta janela do assistente… | Faça o seguinte… |
| --- | --- |
| Na segunda página do assistente | Clique em **Procurar**, selecione o *Certificado Raiz* e clique em **Avançar**. |
| Concluindo o Assistente de Importação de Certificados | Revise o resumo e clique em **Concluir** para iniciar a importação. |

7. Repita as etapas 5 e 6 para os certificados intermediários.

## Informações sobre direitos autorais



## Informações sobre marcas comerciais