Instalar e configurar o SnapCenter Server

SnapCenter software

NetApp
October 06, 2025

This PDF was generated from https://docs.netapp.com/pt-br/snapcenter/install/requirements-to-install-snapcenter-server.html on October 06, 2025. Always check docs.netapp.com for the latest.

Índice

Instalar e configurar o SnapCenter Server . . . 1
- Prepare-se para instalar o servidor SnapCenter . . . 1
  - Requisitos para instalar o servidor SnapCenter . . . 1
  - Registe-se para aceder ao software SnapCenter . . . 7
  - Autenticação multifator (MFA) . . . 8
- Instale o servidor SnapCenter . . . 18
  - Instale o servidor SnapCenter no host Windows . . . 18
  - Instale o servidor SnapCenter no host Linux . . . 22
  - Registre o SnapCenter . . . 26
  - Faça login no SnapCenter usando a autorização RBAC . . . 26
- Configurar o SnapCenter Server . . . 30
  - Adicionar e provisionar o sistema de armazenamento . . . 30
  - Adicione licenças padrão baseadas em controladora SnapCenter . . . 51
  - Configurar alta disponibilidade . . . 56
  - Configurar controles de acesso baseados em função (RBAC) . . . 60
  - Configurar as definições do registo de auditoria . . . 89
  - Configure conexões MySQL seguras com o servidor SnapCenter . . . 90
- Configurar autenticação baseada em certificado . . . 96
  - Ativar autenticação baseada em certificado . . . 96
  - Exportar certificados de autoridade de certificação (CA) do servidor SnapCenter . . . 96
  - Importar certificado CA para os hosts de plug-in do Windows . . . 97
  - Importar certificado CA para os hosts de plug-in UNIX . . . 98
  - Exportar certificados SnapCenter . . . 99
- Configurar o certificado CA para o host Windows . . . 100
  - Gerar arquivo CSR do certificado CA . . . 100
  - Importar certificados CA . . . 100
  - Obtenha a impressão digital do certificado CA . . . 101
  - Configure o certificado CA com os serviços de plug-in do host do Windows . . . 102
  - Configure o certificado CA com o site SnapCenter . . . 102
  - Ativar certificados de CA para SnapCenter . . . 103
- Configure o certificado CA para o host Linux . . . 104
  - Configure o certificado nginx . . . 104
  - Configurar o certificado de log de auditoria . . . 104
  - Configurar certificado SnapCenter . . . 104
- Configure e ative a comunicação SSL bidirecional no host Windows . . . 105
  - Configurar comunicação SSL bidirecional no host Windows . . . 105
  - Ative a comunicação SSL bidirecional no host Windows . . . 108
- Configure e habilite a comunicação SSL bidirecional no host Linux . . . 109
  - Configurar comunicação SSL bidirecional no host Linux . . . 109
  - Ative a comunicação SSL no host Linux . . . 110
- Configure o ative Directory, LDAP e LDAPS . . . 111
  - Registre domínios não confiáveis do ative Directory . . . 111
  - Configure pools de aplicativos do IIS para habilitar permissões de leitura do ative Directory . . . 113

Configure o certificado de cliente CA para LDAPS 113

Instalar e configurar o SnapCenter Server

Prepare-se para instalar o servidor SnapCenter

Requisitos para instalar o servidor SnapCenter

Antes de instalar o servidor SnapCenter no Windows ou no host Linux, você deve analisar e garantir que todos os requisitos sejam atendidos para o seu ambiente.

Requisitos de domínio e grupo de trabalho para host Windows

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

O usuário que tem Privileges de administrador pode instalar o servidor SnapCenter.

- Domínio do ative 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 do Windows.
- Grupos de trabalho: Você deve usar uma conta local que tenha direitos de administrador local.

Embora as trusts de domínio, florestas de vários domínios e trusts de vários domínios sejam suportados, os domínios de floresta cruzada não são suportados. A documentação da Microsoft sobre domínios e trusts do ative Directory contém mais informações.

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

Requisitos de espaço e dimensionamento

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

Item	Requisitos de host do Windows	Requisitos de host do Linux
Sistemas operacionais	Microsoft Windows Apenas as versões em inglês, alemão, japonês e chinês simplificado dos sistemas operacionais são suportadas. Para obter as informações mais recentes sobre versões suportadas, "Ferramenta de Matriz de interoperabilidade do NetApp"consulte .	• Red Hat Enterprise Linux (RHEL) 8 e 9 • SUSE Linux Enterprise Server (SLES) 15 Para obter as informações mais recentes sobre versões suportadas, "Ferramenta de Matriz de interoperabilidade do NetApp"consulte .
Contagem mínima de CPU	4 núcleos	4 núcleos

Item	Requisitos de host do Windows	Requisitos de host do Linux
RAM mínima	8 GB O pool de buffers do MySQL Server usa 20% do total de RAM.	8 GB
Espaço mínimo no disco rígido para o software e logs do servidor SnapCenter	7 GB Se você tiver o repositório SnapCenter na mesma unidade em que o servidor SnapCenter está instalado, então é recomendável ter 15 GB.	15 GB
Espaço mínimo no disco rígido para o repositório SnapCenter	8 GB OBSERVAÇÃO: Se você tiver o servidor SnapCenter na mesma unidade em que o repositório SnapCenter está instalado, então é recomendável ter 15 GB.	Não aplicável

Item	Requisitos de host do Windows	Requisitos de host do Linux
Pacotes de software necessários	• Pacote de Hospedagem ASP.NET Core Runtime 8.0.12 (e todos os patches 8,0.x subsequentes) • PowerShell 7.4.2 ou posterior Para obter informações específicas de solução de problemas .NET, "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet" consulte .	• .NET Framework 8.0.12 (e todos os patches 8,0.x subsequentes) • PowerShell 7.4.2 ou posterior • O nginx é um servidor web que pode ser usado como proxy reverso • PAM-devel PAM (Pluggable Authentication Modules) é uma ferramenta de segurança do sistema que permite que os administradores de sistema definam a política de autenticação sem ter que recompilar programas que fazem a autenticação.

O núcleo ASP.NET precisa IIS_IUSRS para acessar o sistema de arquivos temporários no servidor SnapCenter no Windows.

Requisitos de 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 servidor SnapCenter.

- Utilitários de host: Os Utilitários de host são compatíveis com FC e iSCSI e permitem que você use MPIO em seus servidores Windows. "Saiba mais".
- Microsoft DSM para Windows MPIO: Este software funciona com drivers MPIO Windows para gerenciar vários caminhos entre computadores host NetApp e Windows. É necessário um DSM para configurações de alta disponibilidade.

Se estiver a utilizar o ONTAP DSM, deve migrar para o Microsoft DSM. Para obter mais informações, "Como migrar do ONTAP DSM para o Microsoft DSM"consulte .

Requisitos do navegador

O software SnapCenter suporta Chrome 125 e posterior e Microsoft Edge 110.0.1587.17 e posterior.

Requisitos portuários

O software SnapCenter 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, adicione uma regra de firewall no host do plug-in para essa porta para o Loader de plug-ins do SnapCenter.

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

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

Nome da porta	Números das portas	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 dentro do host do servidor SnapCenter de maneira centralizada. Você pode personalizar o número da porta.
Porto RabbitMQ	5672	TCP		Esta é a porta padrão em que o RabbitMQ escuta e é usada para comunicação entre o serviço de Agendador e o SnapCenter.
Porta MySQL	3306	HTTPS		A porta é usada para se comunicar com o banco de dados do repositório do SnapCenter. Você pode criar conexões seguras do servidor SnapCenter para o servidor MySQL. "Saiba mais"
Hosts de plug-in do Windows	135, 445	TCP		Esta porta é usada para comunicação entre o servidor SnapCenter e o host no qual o plug-in está sendo instalado. O intervalo de portas dinâmico adicional especificado pela Microsoft também deve estar aberto.

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

Nome da porta	Números das portas	Protocolo	Direção	Descrição
Porta de comunicação do cluster ONTAP ou SVM	• 443 (HTTPS) • 80 (HTTP)	• HTTPS • HTTP	Bidirecional	A porta é usada pela sal (camada de abstração de storage) para comunicação entre o host que executa o servidor SnapCenter e o SVM. Atualmente, a porta também é usada pelo sal em hosts plug-in do SnapCenter para Windows para comunicação entre o host do plug-in do SnapCenter e o SVM.
Plug-in do SnapCenter para banco de dados SAP HANA	• 3instance_number13 • 3instance_number15	• HTTPS • HTTP	Bidirecional	Para um locatário único de contentor de banco de dados multitenant (MDC), o número da porta termina com 13; para não MDC, o número da porta termina com 15. Você pode personalizar o número da porta.
Plug-in SnapCenter para PostgreSQL	5432			Esta porta é a porta PostgreSQL padrão usada para comunicação pelo plug-in para PostgreSQL para o cluster PostgreSQL. Você pode personalizar o número da porta.

Registe-se para aceder ao software SnapCenter

Você deve se Registrar para acessar o software SnapCenter se você é novo no Amazon FSX for NetApp ONTAP ou Azure NetApp Files e não tem uma conta NetApp existente.

Antes de começar

- Você deve ter acesso ao ID de e-mail corporativo.
- Se você usa o Azure NetApp Files, você deve ter o ID de assinatura do Azure.
- Se você estiver usando o Amazon FSX for NetApp ONTAP, você deve ter o ID do sistema de arquivos do seu sistema de arquivos FSX for 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 site de suporte da NetApp (NSS) para acesso **completo** a partir do acesso **convidado**.

Passos

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

> Você pode levantar um ticket em https://mysupport.netapp.com/site/help se você enfrentar qualquer problema durante o Registro ou para saber o status.

Autenticação multifator (MFA)

Gerenciamento da autenticação multifator (MFA)

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

Habilitar a autenticação multifator (MFA)

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

Sobre esta tarefa

- O SnapCenter suporta logins baseados em SSO quando outros aplicativos são configurados no mesmo AD FS. Em certas configurações do AD FS, o SnapCenter pode exigir autenticação de 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`o . Alternativamente, você também pode "Guia de referência de cmdlet do software SnapCenter"ver .

Antes de começar

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

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

  O certificado CA é obrigatório pelos seguintes motivos:

  - Garante que as comunicações ADFS-F5 não quebrem porque os certificados autoassinados são exclusivos no nível do nó.
  - Garante que durante a atualização, reparo ou 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, "Gerar arquivo CSR do certificado CA"consulte .

Passos

1. Conete-se ao host dos Serviços de Federação do ative Directory (AD FS).
2. Faça download do arquivo de metadados de federação do AD FS de "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml".
3. Copie o arquivo baixado para o servidor SnapCenter para ativar o recurso MFA.
4. Faça login no servidor SnapCenter como o usuário Administrador do SnapCenter através 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 servidor SnapCenter.

6. Copie o arquivo gerado para o host do AD FS para configurar o SnapCenter como a entidade cliente.
7. Habilite o MFA para servidor SnapCenter usando `Set-SmMultiFactorAuthentication` o cmdlet.
8. (Opcional) Verifique o status e as configurações do MFA usando `Get-SmMultiFactorAuthentication` o cmdlet.
9. Vá para o console de gerenciamento da Microsoft (MMC) e execute as seguintes etapas:
   a. Clique em **File** > **Add/Remove Snapin**.
   b. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
   c. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
   d. Clique em **raiz da consola** > **certificados – computador local** > **Pessoal** > **certificados**.
   e. Clique com o botão direito do rato no certificado CA vinculado ao SnapCenter e selecione **todas as tarefas** > **gerir chaves privadas**.
   f. No assistente de permissões, execute as seguintes etapas:
      i. Clique em **Add**.
      ii. Clique em **locais** e selecione o host em questão (topo da hierarquia).
      iii. Clique em **OK** na janela pop-up **Locations**.
      iv. No campo Nome do objeto, digite 'IIS_IUSRS' e 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 do rato em **confiar em parte** > **Adicionar confiança de parte dependente** > **Iniciar**.
    b. Selecione a segunda opção e navegue no arquivo de metadados do SnapCenter MFA e clique em **Avançar**.
    c. Especifique um nome de exibição e clique em **Next**.
    d. Escolha uma política de controle de acesso conforme necessário e clique em **Next**.
    e. Selecione as configurações na próxima guia como padrão.
    f. Clique em **Finish**.

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

11. Selecione o nome e execute as seguintes etapas:
    a. Clique em **Editar Política de emissão de reclamação**.
    b. Clique em **Adicionar regra** e clique em **seguinte**.
    c. Especifique um nome para a regra de reclamação.
    d. Selecione **ative Directory** como o armazenamento de atributos.
    e. Selecione o atributo como **User-Principal-Name** e o tipo de reclamação enviada como **Name-ID**.
    f. Clique em **Finish**.
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 etapas a seguir para confirmar se os metadados foram importados com êxito.
    a. Clique com o botão direito do rato na confiança da parte dependente e selecione **Propriedades**.
    b. Certifique-se de que os campos Endpoints, Identificadores e assinatura estão preenchidos.
14. Feche todas as guias do navegador e reabra um navegador para limpar os cookies de sessão existentes ou ativos e faça login novamente.

A funcionalidade de MFA do SnapCenter também pode ser ativada usando APIS REST.

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

Atualizar metadados MFA do AD FS

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

Passos

1. Faça download do arquivo de metadados de federação do AD FS de "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"

2. Copie o arquivo baixado para o servidor SnapCenter para atualizar a configuração 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 guias do navegador e reabra um navegador para limpar os cookies de sessão existentes ou ativos e faça login novamente.

Atualizar os 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 da CA, DR, etc.

Passos

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

      O nome definido pelo utilizador da confiança da parte dependente será apresentado.

   c. Habilite a autenticação multifator (MFA).

      "Ativar a autenticação multifator"Consulte .

2. Feche todas as guias do navegador e reabra um navegador para limpar os cookies de sessão existentes ou ativos e faça login novamente.

Desativar a autenticação multifator (MFA)

Passos

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

Gerencie a autenticação multifator (MFA) usando API REST, PowerShell e SCCLI

O login no MFA é compatível com navegador, API REST, PowerShell e SCCLI. O MFA é suportado por um gerenciador de identidade do AD FS. Você pode ativar o MFA, desativar o MFA e configurar o MFA a partir de GUI, API REST, PowerShell e SCCLI.

Configurar o AD FS como OAuth/OIDC

- Configurar o AD FS usando o assistente GUI do Windows*
  1. Navegue até **Painel do Gestor do servidor** > **Ferramentas** > **Gestão ADFS**.
  2. Navegue até **ADFS** > **grupos de aplicativos**.
     a. Clique com o botão direito do rato em **grupos de aplicações**.
     b. Selecione **Adicionar grupo de aplicativos** e digite **Nome do aplicativo**.

   c. Selecione **aplicação de servidor**.
   d. Clique em **seguinte**.
3. Copiar **Identificador do cliente**.

   Esta é a ID do cliente. .. Adicionar URL de retorno de chamada (URL do servidor SnapCenter) em URL de redirecionamento. .. Clique em **seguinte**.

4. Selecione **Generate shared secret** (gerar segredo partilhado).

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

5. Na página **Summary**, clique em **Next**.
   a. Na página **Complete**, clique em **Close**.
6. Clique com o botão direito no recém-adicionado **Application Group** e selecione **Properties**.
7. Selecione **Adicionar aplicativo** nas Propriedades do aplicativo.
8. Clique em **Adicionar aplicativo**.

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

9. Na página Configurar API da Web, digite o URL do servidor SnapCenter e o identificador do cliente criados na etapa anterior na seção Identificador.
   a. Clique em **Add**.
   b. Clique em **seguinte**.
10. Na página **escolha Política de Controle de Acesso**, selecione a política de controle com base em sua exigência (por exemplo, permitir todos e exigir MFA) e clique em **Avançar**.
11. Na página **Configurar permissão de aplicativo**, por padrão openid é selecionado como um escopo, clique em **Avançar**.
12. Na página **Summary**, clique em **Next**.

    Na página **Complete**, clique em **Close**.

13. Na página **Sample Application Properties**, clique em **OK**.
14. Token JWT emitido por um servidor de autorização (AD FS) e destinado a ser consumido pelo recurso.

    A reivindicação 'aud' ou audiência 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 servidor SnapCenter) e o identificador do cliente foram adicionados corretamente.

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

16. Abra a ferramenta **AD FS Management** localizada no menu **Tools** no canto superior direito do Gerenciador de servidores.
    a. Selecione a pasta **grupos de aplicativos** na barra lateral esquerda.
    b. Selecione a API Web e clique em **edit**.
    c. Ir para a guia regras de transformação de emissão

17. Clique em **Adicionar regra**.
    a. Selecione **Enviar atributos LDAP como reclamações** no menu suspenso modelo de regra de reclamação.
    b. Clique em **seguinte**.
18. Introduza o nome **regra de reclamação**.
    a. Selecione **ative Directory** no menu suspenso Attribute store.
    b. Selecione **User-Principal-Name** no menu suspenso **LDAP Attribute** e **UPN** no menu suspenso o*utgoing Claim Type*.
    c. Clique em **Finish**.

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 reivindicações usando comandos do PowerShell. Esses comandos estão disponíveis em formato de script automatizado. Para obter mais informações, consulte o artigo da KB>.

1. Crie o novo grupo de aplicativos no AD FS usando o seguinte comamnd.

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

   `ClientRoleIdentifier` nome do seu grupo de aplicações

   `redirectURL` URL válido para redirecionamento após autorização

2. Crie o aplicativo AD FS Server 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 a partir da saída dos seguintes comandos porque, ele é mostrado 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 Transform rules.

```
$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 o tempo de expiração do token de acesso

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

Sobre esta tarefa

- Um token de acesso pode ser usado apenas para uma combinação específica de usuário, cliente e recurso. Os tokens de acesso não podem ser revogados e são válidos até sua expiração.
- Por padrão, o tempo de expiração de um token de acesso é de 60 minutos. Este tempo de expiração mínimo é suficiente e dimensionado. Você deve fornecer valor suficiente para evitar qualquer trabalho crítico contínuo dos negócios.

Passo

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

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

Obtenha o token portador do AD FS

Você deve preencher os parâmetros abaixo mencionados em qualquer cliente REST (como Postman) e ele solicita 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 portador.

A validade do token portador é configurável a partir do servidor AD FS por aplicativo e o período de validade padrão é de 60 minutos.

Campo	Valor
Tipo de concessão	Código de autorização
URL de retorno de chamada	Insira o URL base do aplicativo se você não tiver um URL de retorno de chamada.
URL de autenticação	[adfs-domain-name]/adfs/oauth2/autorize
Acesse o URL do token	[adfs-domain-name]/adfs/oauth2/token
ID do cliente	Introduza a ID de cliente do AD FS
Segredo do cliente	Insira o segredo do cliente do AD FS
Âmbito de aplicação	OpenID
Autenticação do cliente	Enviar como cabeçalho AUTH básico
Recurso	Na guia **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 servidor SnapCenter usando PowerShell, SCCLI e API REST

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

Autenticação de CLI de MFA do SnapCenter

No PowerShell e 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>]
```

Depois que o cmdlet acima é executado, uma sessão é criada para que o respetivo usuário execute outros cmdlets SnapCenter.

Autenticação da API REST do SnapCenter MFA

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

Fluxo de trabalho da API REST 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 (API REST do SnapCenter) para executar qualquer operação.

Passos

Para autenticar através do AD FS MFA

1. Configure o CLIENTE REST para chamar o endpoint do AD FS para obter o token de acesso.

   Quando você pressiona o botão para obter um token de acesso para um aplicativo, você será redirecionado para a página SSO do AD FS, onde você deve fornecer suas credenciais do AD e autenticar com 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 de domínio ou domínio/usuário.

2. Na caixa de texto Senha, digite sua senha.
3. Clique em **Log in**.
4. Na seção **Opções de login**, selecione uma opção de autenticação e autentique (dependendo da configuração).
   - Push: Aprove a notificação de envio que é enviada para o telefone.
   - Código QR: Use o aplicativo móvel AUTH Point para digitalizar o código QR e, em seguida, digite o código de verificação mostrado no aplicativo
   - Senha de uso único: Digite a senha de uso único do token.
5. Após a autenticação bem-sucedida, um pop-up será aberto que contém o Access, ID e Atualizar Token.

   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 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.

Ative ou desative a funcionalidade SnapCenter MFA para API REST, CLI e GUI

GUI

Passos

1. Inicie sessão no servidor SnapCenter como Administrador do SnapCenter.
2. Clique em **Configurações** > **Configurações globais** > **Configurações MultiFactorAuthentication(MFA)**
3. Selecione a interface (GUI/RST API/CLI) para ativar ou desativar o login MFA.
    - Interface do PowerShell*

Passos

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

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

   O parâmetro PATH especifica a localização do arquivo xml de metadados MFA do AD FS.

   Habilita o MFA para GUI do SnapCenter, API REST, PowerShell e SCCLI configurados com 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.

SCCLI Interface

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 POST para ativar MFA para GUI, API REST, PowerShell e SCCLI.

Parâmetro	Valor
URL solicitada	/api/4,9/settings/multifactorauthentication
Método HTTP	Post
Solicitar corpo	"IsGuiMFAEnabled": False, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSConfigFilePath": "C: ADFS_metadata.abc.xml"

Corpo de resposta	"IGuiMFAEnabled": False, "ADFSConfigFilePath": NULL, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "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/multifactorauthentication
Método HTTP	Obter
Corpo de resposta	"IGuiMFAEnabled": False, "ADFSConfigFilePath": NULL, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSHostName": "win-adfs-sc49.winscedom2.com"

Instale o servidor SnapCenter

Instale o servidor SnapCenter no host Windows

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

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

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

Antes de começar

- O host do servidor SnapCenter deve estar atualizado com as atualizações do Windows sem reiniciar o sistema pendente.
- Você deve ter assegurado que o servidor MySQL não está instalado no host onde você pretende instalar o servidor SnapCenter.
- Você deve ter habilitado a depuração do instalador do Windows.

  Consulte o site da Microsoft para obter informações sobre como ativar "Registo do instalador do Windows"o .

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

Passos

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

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

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

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

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

   > O caráter especial "`"%" is not supported in the custom path for the repository database. If you include "%"` no caminho, falha na instalação.

4. Clique em **Instalar agora**.

   Se você tiver especificado quaisquer valores inválidos, as mensagens de erro apropriadas serão exibidas. Você deve reinserir os valores e, em seguida, iniciar a instalação.

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

   No entanto, se você clicar em **Cancelar** quando as operações "SnapCenter Server site Restart" ou "Waiting for SnapCenter Server to start" estiverem sendo executadas, a instalação continuará sem cancelar a operação.

   Os ficheiros de registo estão sempre listados (o mais antigo primeiro) na pasta %temp% do utilizador admin. Se você quiser redirecionar os locais de log, inicie a instalação do servidor SnapCenter a partir do prompt de comando executando:`C:\installer_location\installer_name.exe /log"C:\"`

Recursos habilitados no host Windows durante a instalação

O instalador do servidor SnapCenter permite os recursos e funções do Windows em 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 informações da Internet
	• Serviços Web mundiais
	• Recursos HTTP comuns
	  ◦ Documento padrão
	  ◦ Navegação de diretório
	  ◦ Erros HTTP
	  ◦ Redirecionamento HTTP
	  ◦ Conteúdo estático
	  ◦ Publicação WebDAV
	• Saúde e Diagnóstico
	  ◦ Registo personalizado
	  ◦ Registo HTTP
	  ◦ Ferramentas de registo
	  ◦ Monitorização de pedidos
	  ◦ Traçado
	• Recursos de desempenho
	  ◦ Compressão de conteúdo estático
	• Segurança
	  ◦ Segurança IP
	  ◦ Autenticação básica
	  ◦ Suporte centralizado a certificados SSL
	  ◦ Autenticação Mapeamento certificado Cliente
	  ◦ Autenticação de mapeamento de certificados do cliente IIS
	  ◦ Restrições de IP e domínio
	  ◦ Filtragem de solicitação
	  ◦ Autorização de URL
	  ◦ Autenticação do Windows
	• Recursos de desenvolvimento de aplicativos
	  ◦ Extensão .NET 4,5
	  ◦ Inicialização da aplicação
	  ◦ Pacote de Hospedagem ASP.NET Core Runtime 8.0.12 (e todos os patches 8,0.x subsequentes)
	  ◦ O lado do servidor inclui
	  ◦ Protocolo WebSocket
	• Ferramentas de gerenciamento
	  Console de gerenciamento do IIS

Categoria	Recurso
Scripts e ferramentas de gerenciamento do IIS	• Serviço de Gestão do IIS • Ferramentas de gerenciamento da Web

O NET Framework 8.0.12 é um dos nossos selecionados Jogos de Plataforma	• Pacote de Hospedagem ASP.NET Core Runtime 8.0.12 (e todos os patches 8,0.x subsequentes)
	• Windows Communication Foundation (WCF) HTTP Activation45
	  ◦ Ativação TCP
	  ◦ Ativação HTTP
	
	Para obter informações específicas de solução de problemas .NET, "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet" consulte .

Fila de mensagens	• Serviços de enfileiramento de mensagens Certifique-se de que nenhum outro aplicativo use o serviço MSMQ que o SnapCenter cria e gerencia. • RabbitMQ • Erlang
Serviço de ativação do processo do Windows	• Modelo do processo
APIs de configuração	Tudo

Instale o servidor SnapCenter no host Linux

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

Antes de começar

- Se você quiser instalar o servidor SnapCenter usando um usuário não-root que não tenha Privileges suficiente para instalar o SnapCenter, obtenha o arquivo de checksum de sudoers no site de suporte da NetApp. Você deve usar o arquivo de checksum apropriado baseado na versão Linux.
- Se o pacote sudo não estiver disponível no SUSE Linux, instale o pacote sudo para evitar falha de autenticação.
- Para o SUSE Linux, configure o nome do host para evitar a falha de instalação.
- Verifique o status seguro do Linux executando o comando `sestatus`. Se o status *SELinux* estiver "ativado" e o modo *atual* estiver "aplicando", 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 a partir do 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 novamente o comando após instalar o servidor SnapCenter.

  - Se o comando criar *my-nginx.PP*, execute o comando para tornar o pacote de políticas ativo: `sudo semodule -i my-nginx.pp`
- O caminho usado para o diretório PID do MySQL é */var/opt/mysqld*. Execute os seguintes comandos para definir as permissões para a 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 MySQL é */install_DIR/NetApp/SnapCenter/SnapManagerWeb/Repositório/MySQL/*. Execute os seguintes comandos para definir as permissões para o diretório de dados 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 servidor SnapCenter é instalado no host Linux, serviços de terceiros como MySQL, RabbitMq, Errlang são instalados. Você não deve desinstalá-los.
- O servidor SnapCenter instalado no host Linux não suporta:
  - Alta disponibilidade
  - Plug-ins do Windows
  - Ative Directory (suporta apenas os utilizadores locais, tanto o utilizador raiz como o utilizador não-raiz com creds)
  - Autenticação baseada em chave para fazer login no SnapCenter
- Durante a instalação do runtime .NET, se a instalação não conseguir resolver as dependências da biblioteca *libicu*, então instale *libicu* executando o comando: `yum install -y libicu`
- Se a instalação do servidor SnapCenter falhar devido à não disponibilidade de *Perl*, então instale *Perl* executando o comando: `yum install -y perl`

Passos

1. Faça o download do seguinte de "Site de suporte da NetApp" para */home Directory*.

- Pacote de instalação do servidor SnapCenter - **SnapCenter-linux-server-(el8/el9/sles15).bin**
- Arquivo de chave pública - **SnapCenter_public_key.pub**
- Respetivo arquivo de assinatura - **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 usuários que não sejam root, adicione o conteúdo visualizado especificado em **SnapCenter_Server_checksum_(el8/el9/sles15).txt** disponível junto com o instalador .bin.
4. Atribua a permissão executar para o instalador .bin. `chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`
5. Execute uma das ações para instalar o servidor SnapCenter.

Se você quiser executar…	Faça isso…
Instalação interativa	`./snapcenter-linux-server-(el8/el9/sles15).bin` Ser-lhe-á pedido que introduza os seguintes detalhes: • A porta externa do webapp usada para acessar o servidor SnapCenter fora do host Linux. O valor padrão é 8146. • O usuário do servidor SnapCenter que instalará o servidor SnapCenter. • 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>` 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 Os registos serão armazenados em */var/opt/SnapCenter/logs*. Parâmetros a serem passados para a instalação do servidor SnapCenter: • DWEBAPP_EXTERNAL_port: Porta externa webapp usada para acessar o servidor SnapCenter fora do host Linux. O valor padrão é 8146. • DWEBAPP_INTERNAL_port: Porta interna do webapp usada para acessar o servidor SnapCenter dentro do host Linux. O valor padrão é 8147. • DSMCORE_port: Porta SMCore na qual os serviços smcore estão sendo executados. O valor padrão é 8145. • DSCHEDULER_port: Porta do Agendador na qual os serviços do agendador estão sendo executados. O valor padrão é 8154. • DSNAPCENTER_Server_User: Usuário do servidor SnapCenter que instalará o servidor SnapCenter. Para *DSNAPCENTER_SERVER_USER*, o padrão é o usuário que executa o instalador. • DUSER_install_DIR: Diretório de instalação onde os pacotes serão instalados. Para *DUSER_install_DIR*, o diretório de instalação padrão é */opt*. • 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 esse parâmetro, os logs serão exibidos no console e também armazenados no arquivo de log padrão.

O que se segue?

- Se o status *SELinux* estiver "habilitado" e o modo *atual* estiver "impondo", o serviço **nginx** não será iniciado. Você deve executar os seguintes comandos:
  a. Vá para o diretório inicial.
  b. Executar o comando: `journalctl -x|grep nginx`.
  c. Se a porta interna do Webapp (8147) não tiver permissão para ouvir, execute os seguintes comandos:
     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
     - `semodule -i my-nginx.pp`
  d. Executar `setsebool -P httpd_can_network_connect on`
- DSELINUX: Se o status *SELinux* estiver "habilitado", o *current mode* está "impondo", e você executou os comandos mencionados na seção antes de começar, você deve especificar esse parâmetro e atribuir o valor como 1. O valor padrão é 0.
- DUPGRADE: O valor padrão é 0. Especifique este parâmetro e seu valor como qualquer inteiro diferente de 0 para atualizar o servidor SnapCenter.

Recursos ativados 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

Registre o SnapCenter

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

Passos

1. Depois de 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.comem .
4. Clique em **Eu não sou um Cliente NetApp registrado**.
5. Especifique os seus dados para se registar.
6. Deixe o campo NetApp Reference SN em branco.
7. Selecione **SnapCenter** na lista suspensa linha de produtos.
8. Selecione o fornecedor de faturação.
9. Insira o ID da instância do SnapCenter de 20 dígitos.
10. Clique em **Enviar**.

Faça login no SnapCenter usando a autorização RBAC

O SnapCenter é compatível com controles de acesso baseados em função (RBAC). O administrador do SnapCenter atribui funções e recursos por meio do SnapCenter RBAC a um usuário no grupo de trabalho ou diretório ativo ou a grupos no diretório ativo. O usuário RBAC agora pode fazer login no SnapCenter com as funções atribuídas.

Antes de começar

- Você deve ativar o Serviço de ativação do processo do Windows (WAS) no Gerenciador do Windows Server.
- Se pretender utilizar o Internet Explorer como browser para iniciar sessão no servidor SnapCenter, deve certificar-se de que o modo protegido no Internet Explorer está desativado.
- Se o servidor SnapCenter estiver instalado no host Linux, você deve fazer login usando a conta de usuário que foi usada para instalar o servidor SnapCenter.

Sobre esta tarefa

Durante a instalação, o assistente de instalação do servidor SnapCenter 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 navegador da Web, fechar apenas a guia do navegador do SnapCenter não fará o logout do SnapCenter. Para terminar sua conexão com o SnapCenter, você deve sair do SnapCenter clicando no botão **Sair** ou fechando todo o navegador da Web.

Prática recomendada: por motivos de segurança, recomenda-se que não ative o seu navegador para guardar a sua palavra-passe do SnapCenter.

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

Para a implantação de alta disponibilidade (HA), você deve acessar o SnapCenter usando o IP *https://Virtual_Cluster_IP_or_FQDN:8146*. do cluster virtual Se você não vir a IU do SnapCenter ao navegar para *https://Virtual_Cluster_IP_or_FQDN:8146* no Internet Explorer (IE), você deve adicionar o endereço IP do cluster virtual ou FQDN como um site confiável no IE em cada host de plug-in ou desativar a Segurança aprimorada do IE em cada host de plug-in. Para obter mais informações, "Não é possível acessar o endereço IP do cluster a partir da rede externa"consulte .

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 sido alterados com cada versão do SnapCenter. O "Guia de referência de cmdlet do software SnapCenter" tem os detalhes.

> Se estiver a iniciar sessão no SnapCenter pela primeira vez, tem de iniciar sessão utilizando 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 do URL fornecido no final da instalação, ou a partir do URL fornecido pelo administrador do SnapCenter.
2. Introduza as credenciais do utilizador.

Para especificar o seguinte…	Use um destes formatos…
Administrador de domínio	• NetBIOS/nome de usuário • Sufixo UPN Por exemplo, NetApp.com • Nome de usuário do domínio
Administrador local	Nome de utilizador

3. Se lhe for atribuída mais de uma função, na caixa função, selecione a função que pretende utilizar para esta sessão de início de sessão.

   Seu usuário atual e sua função associada são mostrados no canto superior direito do SnapCenter depois que você estiver conetado.

Resultado

É apresentada a página Painel de instrumentos.

Se o log falhar com o erro de que o site não pode ser alcançado, você deve mapear o certificado SSL para o SnapCenter. "Saiba mais"

Depois de terminar

Depois de efetuar login no servidor SnapCenter como usuário RBAC pela primeira vez, atualize a lista de recursos.

Se você tiver domínios não confiáveis do ative Directory que deseja que o SnapCenter ofereça suporte, Registre esses domínios no SnapCenter antes de configurar as funções dos usuários em domínios não confiáveis. "Saiba mais".

Se você quiser adicionar o host do plug-in no SnapCenter em execução no host Linux, você deve obter o arquivo de checksum do 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.

Faça login no SnapCenter usando autenticação multifator (MFA)

O servidor SnapCenter suporta MFA para conta de domínio, que faz parte do diretório ativo.

Antes de começar

Você deve ter habilitado o MFA. Para obter informações sobre como ativar o MFA, consulte "Ativar a autenticação multifator"

Sobre esta tarefa

- Apenas o FQDN é suportado
- Os usuários de grupos de trabalho e entre domínios não podem fazer login usando MFA

Passos

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

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

   - Se o nome de usuário ou senha é válido

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

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

Modifique o tempo limite padrão da sessão da GUI 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 um recurso de segurança, após um período padrão de 15 minutos de inatividade, o SnapCenter avisa que você será desconetado da sessão da GUI em 5 minutos. Por padrão, o SnapCenter faz o logout da sessão da GUI após 20 minutos de inatividade e você deve fazer login novamente.

Passos

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

Proteja o servidor web SnapCenter desativando o SSL 3,0

Para fins de segurança, você deve desativar o protocolo SSL (Secure Socket Layer) 3,0 no Microsoft IIS se ele estiver ativado no servidor da Web SnapCenter.

Há falhas no protocolo SSL 3,0 que um invasor pode usar para causar falhas de conexão, ou para executar ataques man-in-the-middle e observar o tráfego de criptografia entre seu site e seus visitantes.

Passos

1. Para iniciar o Editor de Registro no host do servidor web do SnapCenter, clique em **Iniciar** > **Executar** e, em seguida, digite regedit.
2. No Editor de 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 ativado 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, em seguida, nomeie o servidor de chaves.
ii. Com a nova chave de servidor selecionada, clique em **Edit** > **New** > **DWORD**.
iii. Nomeie o novo DWORD habilitado e insira 0 como o valor.

3. Feche o Editor de Registro.

Configurar o SnapCenter Server

Adicionar e provisionar o sistema de armazenamento

Adicione sistemas de storage

Você deve configurar o sistema de armazenamento que dá acesso à SnapCenter 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 independente ou um cluster composto de vários SVMs. Se você estiver usando o Amazon FSX para NetApp ONTAP, você pode adicionar o FSX admin LIF composto por várias SVMs usando a conta fsxadmin ou adicionar o FSX SVM no SnapCenter.

Antes de começar

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

  As instalações de plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento, pois 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 do sistema de armazenamento devem ser exclusivos.

  O SnapCenter não é compatível com vários sistemas de storage com o mesmo nome em clusters diferentes. Cada sistema de storage com suporte do SnapCenter deve ter um nome exclusivo e um endereço IP de LIF de dados exclusivo.

Sobre esta tarefa

- Ao configurar sistemas de armazenamento, também pode ativar as funcionalidades do sistema de Gestão de Eventos (EMS) e do AutoSupport. A ferramenta AutoSupport coleta dados sobre a integridade do seu sistema e envia automaticamente os dados para o suporte técnico da NetApp, permitindo que eles solucionem o problema do seu sistema.

  Se você habilitar esses recursos, o SnapCenter enviará informações do AutoSupport para o sistema de armazenamento e mensagens do EMS para o syslog do sistema de armazenamento quando um recurso estiver protegido, uma operação de restauração ou clone terminar com êxito ou uma operação falhar.

- Se você está planejando replicar snapshots para um destino da SnapMirror ou destino da SnapVault, configure as conexões do sistema de storage para o SVM ou cluster de destino, bem como para o SVM ou cluster de origem.

Se alterar a palavra-passe do sistema de armazenamento, os trabalhos agendados, as operações de cópia de segurança a pedido e restauro poderão falhar. Depois de alterar a palavra-passe do sistema de armazenamento, pode atualizar a palavra-passe clicando em **Modificar** no separador armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Storage Systems**.
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 storage	Introduza o nome do sistema de armazenamento ou o endereço IP. Os nomes de sistemas de storage, que não incluem o nome de domínio, devem ter 15 ou menos carateres e os nomes devem ser solucionáveis. Para criar conexões do sistema de armazenamento com nomes com mais de 15 carateres, você pode usar o cmdlet Add-SmStorageConnectionPowerShell. Para sistemas de storage com configuração MetroCluster (MCC), recomenda-se Registrar clusters locais e de pares para operações sem interrupções. O SnapCenter não é compatível com vários SVMs com o mesmo nome em clusters diferentes. Cada SVM que seja compatível com o SnapCenter precisa ter um nome exclusivo. Depois de adicionar a conexão de storage ao SnapCenter, você não deve renomear o SVM ou o cluster usando o ONTAP. Se o SVM for adicionado com um nome curto ou FQDN, então ele precisa ser resolvido a partir do SnapCenter e do host do plug-in.

Para este campo…	Faça isso…
Nome de utilizador/Palavra-passe	Insira as credenciais do usuário de storage que tem o Privileges necessário para acessar o sistema de storage.
Sistema de Gestão de Eventos (EMS) e Definições do AutoSupport	Se você quiser enviar mensagens EMS para o syslog do sistema de armazenamento ou se quiser enviar mensagens AutoSupport para o sistema de armazenamento para proteção aplicada, operações de restauração concluídas ou operações com falha, marque a caixa de seleção apropriada. Quando você seleciona a caixa de seleção **Enviar notificação AutoSupport para operações com falha no sistema de armazenamento**, a caixa de seleção **Log SnapCenter eventos para syslog** também está selecionada porque mensagens EMS são necessárias para habilitar notificações 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 storage secundário em um relacionamento de backup, marque a caixa de seleção **secundário**. Quando a opção **secundário** está selecionada, o SnapCenter não executa uma verificação de licença imediatamente.

   Se você tiver adicionado SVM no SnapCenter, o usuário precisará selecionar o tipo de plataforma no menu suspenso manualmente.

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

      A porta padrão 443 normalmente funciona.

   c. Introduza o tempo em segundos que deve decorrer antes de as tentativas de comunicação serem interrompidas.

      O valor padrão é de 60 segundos.

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

Resultado

Na página sistemas de armazenamento, na lista suspensa **Type**, execute uma das seguintes ações:

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

  Se você adicionou FSX SVMs, os FSX SVMs são listados aqui.

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

  Se você adicionou clusters FSX usando fsxadmin, os clusters FSX são listados aqui.

  Quando você clica no nome do cluster, todos os SVMs que fazem parte do cluster são exibidos na seção máquinas virtuais de armazenamento.

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

Depois de terminar

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

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

O administrador da máquina virtual de storage (SVM) não tem acesso ao AutoSupport.

Conexões e credenciais de storage

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

Conexões de armazenamento

As conexões de armazenamento dão aos plug-ins do servidor SnapCenter e do SnapCenter acesso ao armazenamento do ONTAP. A configuração dessas conexões também envolve a configuração de 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 no qual você está instalando o plug-in do SnapCenter. Formatos válidos para o campo Nome de usuário são:

  - *NetBIOS_username*
  - *Domain FQDN_username*
  - *upn*

- Administrador local (apenas para grupos de trabalho)

  Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o

recurso de controle de acesso do usuário estiver desativado no sistema host.

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

- Credenciais para grupos de recursos individuais

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

Provisione storage em hosts do Windows

Crie e gerencie grupos

Você cria grupos de iniciadores (grupos de iniciadores) 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 grupo em um host do Windows.

Crie um grupo

Você pode usar o SnapCenter para criar um grupo em um host do Windows. O grupo estará disponível no assistente criar disco ou conetar disco quando você mapear o grupo 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 grupo, defina o grupo:

Neste campo…	Faça isso…
Sistema de storage	Selecione o SVM para o LUN que você mapeará para o grupo.
Host	Selecione o host no qual você deseja criar o grupo.
Nome do grupo	Introduza o nome do grupo.
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 grupo no sistema de armazenamento.

Renomeie um grupo

Você pode usar o SnapCenter para renomear um grupo 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 **Storage Virtual Machine** para exibir uma lista de SVMs disponíveis e selecione o SVM para o grupo que deseja renomear.
4. Na lista de grupos para o SVM, selecione o grupo que deseja renomear e clique em **Renomear**.
5. Na caixa de diálogo Renomear grupo, digite o novo nome para o grupo e clique em **Renomear**.

Modifique um grupo

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

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 **Storage Virtual Machine** para exibir uma lista suspensa de SVMs disponíveis e, em seguida, selecione o SVM para o grupo que deseja modificar.
4. Na lista de grupos, selecione um grupo e clique em **Adicionar iniciador ao grupo**.
5. Selecione um host.
6. Selecione os iniciadores e clique em **OK**.

Exclua um igroup

Você pode usar o SnapCenter para excluir um iggroup 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 **Storage Virtual Machine** para exibir uma lista suspensa de SVMs disponíveis e, em seguida, selecione o SVM para o grupo que deseja excluir.
4. Na lista de grupos para o SVM, selecione o grupo que deseja excluir e clique em **Excluir**.
5. Na caixa de diálogo Excluir grupo, clique em **OK**.

   O SnapCenter exclui o grupo.

Criar e gerenciar discos

O host do Windows vê LUNs no seu sistema de armazenamento como discos virtuais. Pode utilizar o SnapCenter para criar e configurar um LUN ligado a FC ou ligado a iSCSI.

- O SnapCenter suporta apenas discos básicos. Os discos dinâmicos não são suportados.
- Para GPT apenas é permitida uma partição de dados e para MBR uma partição primária que tenha um volume formatado com NTFS ou CSVFS e tenha um caminho de montagem.
- Estilos de partição suportados: GPT, MBR; em uma VM UEFI VMware, 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.

Exibir os discos em um host

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

Passos

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

   Os discos são listados.

Exibir discos em cluster

É possível exibir discos em cluster no cluster que você gerencia com o SnapCenter. Os discos em cluster são exibidos somente quando você seleciona o cluster na lista suspensa hosts.

Passos

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

   Os discos são listados.

Estabeleça uma sessão iSCSI

Se estiver a utilizar iSCSI para ligar a um LUN, tem de estabelecer uma sessão iSCSI antes de criar o LUN para ativar a comunicação.

Antes de começar

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

Sobre esta tarefa

Pode estabelecer uma sessão iSCSI apenas entre as mesmas versões IP, de IPv6 a IPv6, ou de IPv4 a IPv4.

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

Se alterar o nome de um iniciador iSCSI, o acesso a iSCSI Targets é afetado. Depois de alterar o nome, você pode precisar reconfigurar os destinos acessados pelo iniciador para que eles possam reconhecer o novo nome. Tem de se certificar de que reinicia o anfitrião depois de alterar o nome de um iniciador iSCSI.

Se o seu host tiver mais de uma interface iSCSI, depois de estabelecer uma sessão iSCSI para SnapCenter usando um endereço IP na primeira interface, não será possível 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 **iSCSI Session**.
3. Na lista suspensa **Storage Virtual Machine**, selecione a máquina virtual de armazenamento (SVM) para o destino iSCSI.
4. Na lista suspensa **Host**, selecione o host para a sessão.
5. Clique em **estabelecer sessão**.

   É apresentado o assistente estabelecer sessão.

6. No assistente estabelecer sessão, identifique o alvo:

Neste campo…	Digite…
Nome do nó de destino	O nome do nó do destino iSCSI Se houver um nome de nó de destino existente, o nome será exibido no formato somente leitura.
Endereço do portal de destino	O endereço IP do portal de rede de destino
Porta do portal de destino	A porta TCP do portal de rede de destino
Endereço do portal do iniciador	O endereço IP do portal de rede do iniciador

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

   O SnapCenter estabelece a sessão iSCSI.

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

Crie LUNs ou discos conectados a FC ou iSCSI

O host do Windows vê os LUNs no seu sistema de armazenamento como discos virtuais. Pode utilizar o SnapCenter para criar e configurar um LUN ligado a FC ou ligado a iSCSI.

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

Antes de começar

- Você deve ter criado um volume para o LUN em seu sistema de storage.

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

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

- Você deve ter iniciado o serviço FC ou iSCSI no sistema de storage.
- Se estiver a utilizar iSCSI, tem de 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 conetar 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 cluster.

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **Disks**.
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 storage	Selecione o SVM para o LUN.
Caminho de LUN	Clique em **Browse** para selecionar o caminho completo da pasta que contém o LUN.
Nome LUN	Introduza o nome do LUN.
Tamanho do cluster	Selecione o tamanho da alocação do bloco LUN para o cluster. O tamanho do cluster depende do sistema operacional e dos aplicativos.
Etiqueta LUN	Opcionalmente, insira 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. Ignore o campo **Grupo de recursos**.
Disco compartilhado	O LUN é compartilhado por hosts em um cluster de failover do Windows Server. Digite 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 de cluster (CSV)	O LUN é compartilhado por hosts em um cluster de failover do Windows Server que usa CSV. Digite 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 é o proprietário do grupo de cluster.

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

Propriedade	Descrição
Atribuir automaticamente o ponto de montagem	O SnapCenter atribui automaticamente um ponto de montagem de volume com base na unidade do sistema. Por exemplo, se a unidade do sistema for C:, a atribuição automática cria um ponto de montagem de volume sob a unidade C: (C:). A atribuição automática não é suportada para discos partilhados.
Atribua a letra da unidade	Monte o disco na unidade selecionada na lista suspensa adjacente.
Utilize o ponto de montagem do volume	Monte o disco no caminho da unidade especificado no campo adjacente. A raiz do ponto de montagem de volume deve ser propriedade do host no qual você está criando o disco.
Não atribua a letra da unidade ou o ponto de montagem do volume	Escolha esta opção se preferir montar o disco manualmente no Windows.

Propriedade	Descrição
Tamanho da LUN	Especifique o tamanho do LUN; mínimo de 150 MB. Selecione MB, GB ou TB na lista suspensa adjacente.
Use thin Provisioning para o volume que hospeda este LUN	Thin Provisioning o LUN. O thin Provisioning aloca apenas o espaço de armazenamento necessário de uma só vez, permitindo que o LUN cresça eficientemente até à capacidade máxima disponível. Certifique-se de que há espaço suficiente disponível no volume para acomodar todo o armazenamento LUN que você acha que vai precisar.
Escolha o tipo de partição	Selecione partição GPT para uma Tabela de partição GUID ou partição MBR para um Registro de inicialização mestre. As partições MBR podem causar problemas de desalinhamento nos clusters de failover do Windows Server. Os discos de partição UEFI (Unified Extensible firmware Interface) não são suportados.

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

Neste campo…	Faça isso…
Host	Clique duas vezes no nome do grupo de cluster para exibir uma lista suspensa que mostra os hosts que pertencem ao cluster e, em seguida, selecione o host para o iniciador. Este campo é 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. Você pode selecionar vários iniciadores FC se estiver usando FC com e/S multipath (MPIO).

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

grupo:

Selecione…	Se…
Crie um novo grupo para iniciadores selecionados	Você deseja criar um novo grupo para os iniciadores selecionados.
Escolha um grupo existente ou especifique um novo grupo para iniciadores selecionados	Você deseja especificar um grupo existente para os iniciadores selecionados ou criar um novo grupo com o nome que você especificar. Digite o nome do grupo no campo **Nome do grupo**. Digite as primeiras letras do nome do grupo existente para preencher automaticamente o campo.

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

    O SnapCenter cria o LUN e o coneta à unidade especificada ou ao caminho da unidade no host.

Redimensione um disco

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

Sobre esta tarefa

- Para LUN com provisionamento reduzido, o tamanho da geometria do lun ONTAP é mostrado como o tamanho máximo.
- Para LUN provisionado grosso, o tamanho expansível (tamanho disponível no volume) é mostrado como o tamanho máximo.
- Os LUNs com partições de estilo MBR têm um limite de tamanho de 2 TB.
- Os LUNs com partições de estilo GPT têm um limite de tamanho de sistema de armazenamento de 16 TB.
- É uma boa ideia fazer um instantâneo antes de redimensionar um LUN.
- Se você precisar restaurar um LUN de uma captura Instantânea feita antes que o LUN fosse redimensionado, o SnapCenter redimensionará automaticamente o LUN para o tamanho da captura Instantânea.

  Após a operação de restauração, os dados adicionados ao LUN após o dimensionamento devem ser restaurados a partir de uma captura Instantânea feita após o dimensionamento.

Passos

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

   Os discos são 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, será necessário clicar fora do campo tamanho antes que o botão diminuir ou expandir esteja 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 **Shrink** ou **Expand**, conforme apropriado.

   O SnapCenter redimensiona o disco.

Conete um disco

Você pode usar o assistente conetar disco para conetar um LUN existente a um host ou para reconetar um LUN que foi desconetado.

Antes de começar

- Você deve ter iniciado o serviço FC ou iSCSI no sistema de storage.
- Se estiver a utilizar iSCSI, tem de ter estabelecido uma sessão iSCSI com o sistema de armazenamento.
- Não é possível conetar 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), será necessário conetar o disco no host que possui o grupo de cluster.
- O plug-in para Windows precisa ser instalado apenas no host no qual você está conetando o disco.

Passos

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

   O assistente Connect Disk (ligar disco) é aberto.

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

Neste campo…	Faça isso…
Sistema de storage	Selecione o SVM para o LUN.
Caminho de LUN	Clique em **Procurar** para selecionar o caminho completo do volume que contém o LUN.
Nome LUN	Introduza o nome do LUN.

Neste campo…	Faça isso…
Tamanho do cluster	Selecione o tamanho da alocação do bloco LUN para o cluster. O tamanho do cluster depende do sistema operacional e dos aplicativos.
Etiqueta LUN	Opcionalmente, insira 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. Você só precisa conetar o disco a um host no cluster de failover.
Volume compartilhado de cluster (CSV)	O LUN é compartilhado por hosts em um cluster de failover do Windows Server que usa CSV. Certifique-se de que o host no qual você está se conetando ao disco é o proprietário do grupo de cluster.

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

Propriedade	Descrição
Atribuição automática	Permita que o SnapCenter atribua automaticamente um ponto de montagem de volume com base na unidade do sistema. Por exemplo, se a unidade do sistema for C:, a propriedade de atribuição automática cria um ponto de montagem de volume sob a unidade C: (C:). A propriedade atribuição automática não é suportada para discos compartilhados.
Atribua a letra da unidade	Monte o disco na unidade selecionada na lista suspensa adjacente.

Propriedade	Descrição
Utilize o ponto de montagem do volume	Monte o disco no caminho da unidade especificado no campo adjacente. A raiz do ponto de montagem de volume deve ser propriedade do host no qual você está criando o disco.
Não atribua a letra da unidade ou o ponto de montagem do volume	Escolha esta opção se preferir montar o disco manualmente no Windows.

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

Neste campo…	Faça isso…
Host	Clique duas vezes no nome do grupo de cluster para exibir uma lista suspensa que mostra os hosts que pertencem ao cluster e, em seguida, selecione o host para o iniciador. Este campo é 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. Você pode selecionar vários iniciadores FC se estiver usando FC com MPIO.

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

Selecione…	Se…
Crie um novo grupo para iniciadores selecionados	Você deseja criar um novo grupo para os iniciadores selecionados.
Escolha um grupo existente ou especifique um novo grupo para iniciadores selecionados	Você deseja especificar um grupo existente para os iniciadores selecionados ou criar um novo grupo com o nome que você especificar. Digite o nome do grupo no campo **Nome do grupo**. Digite as primeiras letras do nome do grupo existente para completar automaticamente o campo.

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

    O SnapCenter coneta o LUN à unidade especificada ou ao caminho da unidade no host.

Desconete um disco

Você pode desconetar um LUN de um host sem afetar o conteúdo do LUN, com uma exceção: Se você desconetar um clone antes que ele tenha sido dividido, você perderá o conteúdo do clone.

Antes de começar

- Certifique-se de que o LUN não está a ser utilizado por qualquer aplicação.
- Certifique-se de que o LUN não está a ser monitorizado com o software de monitorização.
- Se o LUN for compartilhado, remova as dependências de recursos do cluster do LUN e verifique se todos os nós do cluster estão ligados, funcionando corretamente e disponíveis para o SnapCenter.

Sobre esta tarefa

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

Para evitar a eliminação automática do volume FlexClone, deve mudar o nome do volume antes de desligar o último LUN. Ao renomear o volume, certifique-se de alterar vários carateres do que apenas o último caractere no nome.

Passos

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

   Os discos são listados.

4. Selecione o disco que deseja desconetar e clique em **Disconnect**.
5. Na caixa de diálogo Disconnect Disk (Desligar disco), clique em **OK**.

   O SnapCenter desliga o disco.

Eliminar um disco

Você pode excluir um disco quando não precisar mais dele. Depois de eliminar um disco, não pode anular a sua eliminação.

Passos

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

   Os discos são 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.

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.

Prática recomendada: o uso dos cmdlets é recomendado porque permite que você aproveite os modelos fornecidos com o SnapCenter para automatizar a configuração de compartilhamento.

Os modelos encapsulam as práticas recomendadas 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 fazendo isso, você pode criar seus próprios modelos seguindo os modelos fornecidos. Você deve revisar os parâmetros na documentação do cmdlet antes de criar um modelo personalizado.

Crie um compartilhamento SMB

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

Não é possível usar o SnapCenter para fazer backup de bancos de dados em compartilhamentos SMB. O suporte a SMB está limitado apenas ao provisionamento.

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **shares**.
3. Selecione o SVM na lista suspensa **Storage Virtual Machine**.
4. Clique em **novo**.

   Abre-se a caixa de diálogo New Share (Nova partilha).

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

Neste campo…	Faça isso…
Descrição	Introduza texto descritivo para a partilha.

Neste campo…	Faça isso…
Nome da partilha	Introduza o nome da partilha, por exemplo, test_share. O nome introduzido para a partilha também será utilizado como o nome do volume. O nome da partilha: • Deve ser uma string UTF-8. • Não deve incluir os seguintes carateres: Controlar carateres de 0x00 a 0x1F (ambos incluídos), 0X22 (aspas duplas) e os carateres especiais `\ / [ ] : (vertical bar) < > + = ; , ?`
Compartilhar caminho	• Clique no campo para introduzir um novo caminho do sistema de ficheiros, por exemplo, /. • Clique duas vezes no campo para selecionar a partir de 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 na 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 **shares**.
3. Na página compartilhamentos, clique no campo **Storage Virtual Machine** para exibir uma lista suspensa com uma lista de máquinas virtuais de armazenamento disponíveis (SVMs) e selecione o SVM para o compartilhamento que 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 storage

Embora o NTFS rastreie o espaço disponível em um LUN quando os arquivos são excluídos ou modificados, ele não relata as novas informações para o sistema de

armazenamento. Você pode executar o cmdlet PowerShell de recuperação de espaço no host Plug-in para Windows para garantir que os blocos recém-liberados sejam marcados como disponíveis no storage.

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

Antes de começar

- Você deve garantir que o processo de recuperação de espaço foi 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 cluster.
- Para um desempenho de armazenamento ideal, você deve executar a recuperação de espaço o mais frequentemente possível.

  Você deve garantir que todo o sistema de arquivos NTFS foi digitalizado.

Sobre esta tarefa

- A recuperação de espaço é demorada e intensiva na CPU, por isso geralmente é melhor executar a operação quando o sistema de armazenamento e o uso de host do Windows são baixos.
- A recuperação de espaço recupera quase todo o espaço disponível, mas não 100%.
- Você não deve executar a desfragmentação do disco ao mesmo tempo que está executando a recuperação de espaço.

  Fazer isso pode retardar o processo de recuperação.

Passo

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.

Provisione o 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 você estiver executando os cmdlets em um host de plug-in remoto, será necessário executar o cmdlet SnapCenter Open-SMConnection para abrir uma conexão com o servidor SnapCenter.

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

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

Provisione storage em ambientes VMware

Você pode usar o plug-in do SnapCenter para Microsoft Windows em ambientes VMware para criar e gerenciar LUNs e snapshots.

Plataformas VMware Guest os compatíveis

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

  Suporte para até um máximo de 16 nós com suporte no VMware ao usar o iniciador de software iSCSI da Microsoft ou até dois nós usando FC

- LUNs RDM

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

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

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

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.
- Quando você cria um LUN RDM fora do plug-in para Windows, você deve reiniciar o serviço de plug-in para permitir que ele reconheça o disco recém-criado.
- Não é possível usar iniciadores iSCSI e FC ao mesmo tempo em um SO convidado VMware.

Mínimo do vCenter Privileges necessário para operações do SnapCenter RDM

Você deve ter o seguinte vCenter Privileges no host para executar operações RDM em um SO convidado:

- Datastore: Remover Arquivo
- Host: Configuração > Configuração da partição de armazenamento
- Máquina virtual: Configuração

Você deve atribuir esses Privileges a uma função no nível do servidor do Centro Virtual. A função à qual você atribui esses Privileges não pode ser atribuída a nenhum usuário sem root Privileges.

Depois de atribuir esses Privileges, você pode instalar o plug-in para Windows no SO convidado.

Gerenciar LUNs FC RDM em um cluster da Microsoft

Você pode usar o Plug-in para Windows para gerenciar um cluster da Microsoft usando LUNs FC RDM, mas primeiro você deve criar o quórum 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 o 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 oferece suporte a 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 de 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 datastore 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 uma SAN FC.

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

  Não é possível 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 requer que você configure o controlador SCSI SAS LSI Logic em cada máquina virtual. Os LUNs compartilhados não podem usar o controlador SAS LSI Logic existente se apenas um de seu tipo existir e já estiver conetado à unidade C:.

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

  > Quando você adiciona 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 **Create a new disk** no VMware Infrastructure Client.

- Os clusters de máquinas virtuais da Microsoft não podem fazer parte de um cluster VMware.
- Você deve usar as credenciais do vCenter e não as credenciais do ESX ou do 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 grupo com iniciadores de vários hosts.

  O grupo que contém 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 LUN RDM no ESXi 5,0 usando um iniciador FC.

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

Limitações

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

> Esse recurso não é suportado em versões anteriores ao ESX 5,5i.

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

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

- Iniciadores iSCSI ESX e HBAs não são suportados em discos compartilhados em um cluster Microsoft.
- O Plug-in para Windows não suporta migração de máquina virtual com o vMotion se a máquina virtual fizer parte de um cluster da Microsoft.
- O plug-in para Windows não suporta MPIO em máquinas virtuais em um cluster da Microsoft.

Crie um LUN FC RDM compartilhado

Antes de usar LUNs FC RDM para compartilhar o storage entre nós em um cluster da Microsoft, primeiro você deve criar o disco de quorum compartilhado e o disco de storage compartilhado e adicioná-los a ambas as 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, "Cluster de máquinas virtuais em hosts físicos"consulte .

Adicione licenças padrão baseadas em controladora SnapCenter

Se você estiver usando controladores de storage FAS, AFF ou ASA, é necessária uma licença baseada em controlador padrão da SnapCenter.

A licença baseada no controlador tem as seguintes caraterísticas:

- Direito padrão da SnapCenter incluído na compra de pacote Premium ou Flash (não com o pacote básico)
- Uso ilimitado de armazenamento
- 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, "Licenças SnapCenter"consulte .

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 **Storage Systems**.
2. Na página sistemas de armazenamento, na lista suspensa **tipo**, selecione se deseja exibir todos os SVMs ou clusters que foram adicionados:
   - Para visualizar todos os SVMs que foram adicionados, selecione **SVMs ONTAP**.
   - Para visualizar todos os clusters que foram adicionados, selecione **clusters ONTAP**.

     Quando você seleciona o nome do cluster, todos os SVMs que fazem parte do cluster são exibidos 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 storage primário FAS, AFF ou ASA.
   - ⊘ Indica que uma licença do SnapManager Suite não está instalada em um sistema de storage 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 para NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select ou plataformas de armazenamento secundário.

Passo 2: Identifique 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. Faça 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 é instalada, portanto, nenhuma ação adicional de licenciamento SnapCenter é necessária.

Passo 3: Recupere 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. Faça login no controlador usando a linha de comando ONTAP.
2. Digite o comando system show -instance e, em seguida, 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. Registe os números de série.

Passo 4: Recupere 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

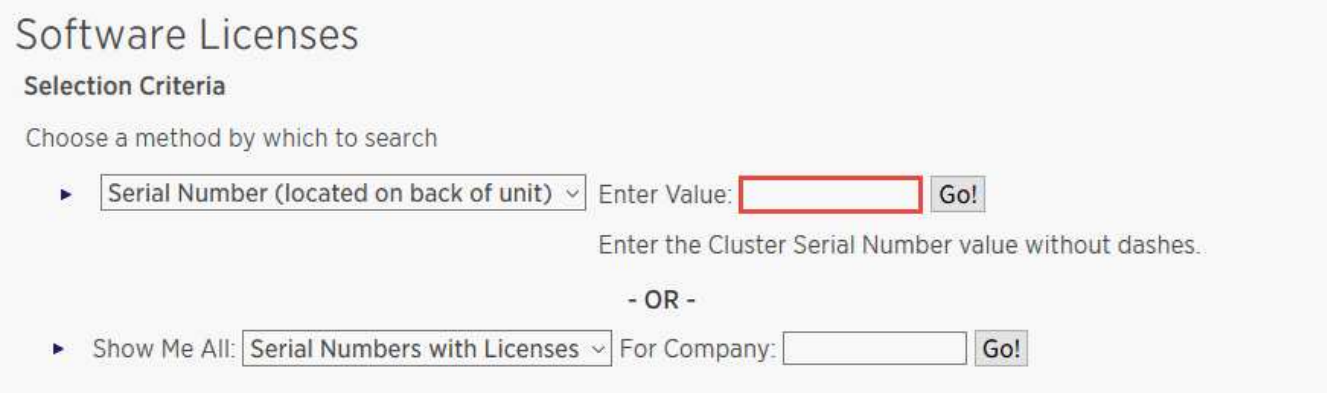
- Você deve ter credenciais de login válidas no site de suporte da NetApp.

  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. Inicie sessão 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) está selecionado, introduza o número de série do controlador e, em seguida, selecione **Go!**.



   É apresentada uma lista de licenças para o controlador especificado.

4. Localize e Registre a licença padrão ou SnapManagerSuite do SnapCenter.

Passo 5: Adicione licença baseada no controlador

Você pode usar a linha de comando ONTAP para adicionar uma licença baseada em controladora SnapCenter quando estiver usando sistemas FAS, AFF ou ASA e tiver uma licença padrão ou SnapManagerSuite do SnapCenter.

Antes de começar

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

Sobre esta tarefa

Se você quiser instalar o SnapCenter de avaliação com o storage FAS, AFF ou ASA, obtenha uma licença de avaliação do pacote Premium para instalar no controlador.

Se você quiser instalar o SnapCenter em uma base de avaliação, entre em Contato com seu representante de vendas para obter uma licença de avaliação do pacote Premium para instalar em seu controlador.

Passos

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

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

   Este comando está disponível no nível de privilégios de administrador.

3. Verifique se a licença SnapManagerSuite está instalada:

   ```
   license show
   ```

Passo 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 teste só é necessária se estiver a utilizar uma licença baseada em controlador padrão da SnapCenter.

Passos

1. No servidor SnapCenter, 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 de cmdlet do software SnapCenter" .

2. Abra o prompt de comando e execute mysql -u root -p para fazer login no MySQL.

   O MySQL solicita a senha. Introduza as credenciais fornecidas durante a reposição da palavra-passe.

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 a alta disponibilidade (HA) no SnapCenter executado no Windows ou no Linux, você pode instalar o balanceador de carga F5. O F5 permite que o servidor SnapCenter suporte configurações ativo-passivo em até dois hosts que estão no mesmo local. Para usar o balanceador de carga F5 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 o SnapCenter High Availability. Você deve configurar manualmente o NLB fora da instalação do SnapCenter para alta disponibilidade.

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

Configure a alta disponibilidade usando o 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 ser atribuído à função SnapCenterAdmin) para usar os seguintes cmdlets para adicionar e remover clusters F5:

- Add-SmServerCluster
- Add-SmServer
- Remover-SmServerCluster

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

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 servidores SnapCenter e houver também uma sessão do 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 parcialmente resolvido pelo NLB ou host F5 e se o host SnapCenter não conseguir entrar em Contato com esse host, a página do host SnapCenter alternará entre hosts inativos e o estado em execução com frequência. Para resolver esse problema, você deve garantir que ambos os hosts do SnapCenter sejam capazes de resolver o host no NLB ou no host F5.
- Os comandos SnapCenter para configurações de MFA devem ser executados em todos os hosts. A configuração do grupo dependente deve ser feita no servidor AD FS (Serviços de Federação do ative Directory) usando os detalhes do cluster F5. O acesso à IU 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 de log de auditoria no host passivo F5 quando ele se tornar ativo.

Configurar a alta disponibilidade usando o balanceamento de carga de rede (NLB)

Você pode configurar o balanceamento de carga de rede (NLB) para configurar o SnapCenter High Availability. Você deve configurar manualmente o NLB fora da instalação do SnapCenter para alta disponibilidade.

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

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

Você pode configurar o ambiente de SnapCenter de alta disponibilidade no 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 IP de sobreposição virtual privada na AWS. Para obter informações, "Configurar IP de sobreposição virtual privada" consulte .
2. Prepare seu host Windows
   a. Força IPv4 a ser priorizada acima de 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 podem ser resolvidos via DNS ou através da configuração de host local para os endereços IPv4.
   c. Certifique-se de que não tem um proxy do sistema configurado.
   d. Certifique-se de que a palavra-passe de administrador seja a mesma no Windows Server quando utilizar uma configuração sem um ative Directory e que os servidores não estejam num domínio.
   e. Adicione IP virtual em ambos os servidores Windows.
3. Crie o cluster SnapCenter.
   a. Inicie o PowerShell e conete-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 endpoint IP privado virtual fique indisponível, monitorado pelo AWS CloudWatch. Para obter informações, "Crie uma função do Lambda" consulte .
5. Crie um monitor no CloudWatch para monitorar a disponibilidade do endpoint do SnapCenter. Um alarme é configurado para acionar uma função do Lambda se o endpoint estiver inacessível. A função do Lambda ajusta a tabela de roteamento para redirecionar o tráfego para o servidor SnapCenter ativo. Para obter informações, "Crie canários sintéticos" consulte .
6. Implemente o fluxo de trabalho usando uma função de etapa como alternativa ao monitoramento do CloudWatch, fornecendo tempos de failover menores. O fluxo de trabalho inclui uma função de sonda do Lambda para testar o URL do SnapCenter, uma tabela do DynamoDB para armazenar contagens de falhas e a própria função Etapa.
   a. Use uma função lambda para verificar a URL do SnapCenter. Para obter informações, "Crie a função Lambda" consulte .
   b. Crie uma tabela do DynamoDB para armazenar a contagem de falhas entre duas iterações de função de passo. Para obter informações, "Comece a usar a tabela DynamoDB" consulte .
   c. Crie a função Step (passo). Para obter informações, "Documentação da função de passos" consulte .
   d. Teste uma única etapa.
   e. Teste a função completa.
   f. Crie a função do IAM e ajuste as permissões para poder executar a função do Lambda.

g. Criar agendamento para acionar a função Step. Para obter informações, "Usando o Amazon EventBridge Scheduler para iniciar uma função de passo" consulte .

Configure a alta disponibilidade usando o balanceador de carga do Azure

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

Passos

1. Crie máquinas virtuais em um conjunto de escala usando o portal do Azure. O conjunto de escala de máquina virtual do Azure permite criar e gerenciar um grupo de máquinas virtuais balanceadas de carga. O número de instâncias de máquina virtual pode aumentar ou diminuir automaticamente em resposta à demanda ou a um cronograma definido. Para obter informações, "Crie máquinas virtuais em um conjunto de escala usando o portal do Azure" consulte .
2. Depois de configurar as máquinas virtuais, faça login em cada máquina virtual no VM Set e instale o servidor SnapCenter 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 sua configuração do SnapCenter HA de balanceamento de carga de rede (NLB) para usar o balanceador de carga F5.

Passos

1. Configurar servidores SnapCenter para alta disponibilidade usando o F5. "Saiba mais".
2. No host do servidor SnapCenter, inicie o PowerShell.
3. Inicie uma sessão usando o cmdlet Open-SmConnection e insira suas credenciais.
4. Atualize o servidor SnapCenter 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Alta disponibilidade para o repositório SnapCenter MySQL

Replicação MySQL é um recurso do MySQL Server que permite replicar dados de um servidor de banco de dados MySQL (master) para outro servidor de banco de dados

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

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 slave então se torna o repositório master. O SnapCenter também dá suporte à replicação reversa, que é ativada somente durante o failover.

Para usar o recurso de alta disponibilidade (HA) do MySQL, você deve 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 se juntar ao 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

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

- NLB e MySQL HA não são suportados além de dois nós.
- Mudar de uma instalação autônoma do SnapCenter para uma instalação NLB ou vice-versa e mudar de uma configuração autônoma do MySQL para o MySQL HA não são suportados.
- O failover automático não é suportado se os dados do repositório secundário não forem sincronizados com os dados do repositório principal.

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

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

  Se o failover acontecer porque o servidor MySQL ou o servidor SnapCenter estão inoperantes, os trabalhos que estão em execução podem falhar. Após o failover para o segundo nó, todos os trabalhos subsequentes são executados com êxito.

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

Configurar controles de acesso baseados em função (RBAC)

Crie 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 + em .
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 objetos de outros membros** para permitir que outros membros da função vejam recursos como volumes e hosts depois que eles atualizarem a lista de recursos.

   Você deve desmarcar essa opção se não quiser que os membros dessa função vejam objetos aos quais outros membros são atribuídos.

> Quando essa opção está ativada, a atribuição de acesso aos usuários a objetos ou recursos não é necessária se os usuários pertencerem à mesma função que o usuário que criou os objetos ou recursos.

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

Adicione uma função NetApp ONTAP RBAC usando comandos de login de segurança

Use os comandos de login de segurança para adicionar uma função RBAC do NetApp ONTAP quando seus sistemas de storage estiverem executando o Clustered ONTAP.

Antes de começar

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

  Existem dois níveis de acesso para cada diretório de comando/comando: All-Access e somente leitura.

  Você deve sempre atribuir primeiro o All-Access Privileges.

- Atribua funções aos usuários.
- Identifique sua configuração dependendo se seus plug-ins 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 lida automaticamente com a configuração correta do ONTAP Privileges. Por exemplo, a ferramenta Criador de Usuário RBAC para NetApp ONTAP adiciona automaticamente o Privileges na ordem correta para que o Privileges de Acesso total apareça primeiro. Se você adicionar primeiro o Privileges somente leitura e depois adicionar o Privileges All-Access, o ONTAP marca o Privileges All-Access como duplicatas e os ignora.

> Se você atualizar mais tarde o SnapCenter ou o ONTAP, execute novamente a ferramenta Criador de usuários do RBAC para NetApp ONTAP para atualizar as funções de usuário criadas anteriormente. As funções de usuário criadas para uma versão anterior do SnapCenter ou do ONTAP não funcionam corretamente com versões atualizadas. Quando você executa novamente a ferramenta, ela manipula automaticamente a atualização. Você não precisa recriar os papéis.

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

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 isso em branco, o padrão será administrador do cluster.
   - role_name é o nome que você especifica para a função.
   - Comando é a capacidade ONTAP.

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

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

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.
   - <password> é a sua palavra-passe. Se você não especificar uma senha, o sistema solicitará uma.
   - SVM_name é o nome do SVM.

3. Atribua a função ao utilizador introduzindo 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 modificar 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.
   - <password> é a sua palavra-passe. 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.

Criar funções do SVM com Privileges mínimo

Há vários comandos de CLI do ONTAP que você deve executar ao criar uma função para um novo usuário do 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 storage, crie uma função e atribua todas as permissões à função.

   ```
   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 esse usuário.

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

3. Desbloquear o utilizador.

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

Comandos CLI do ONTAP para criar funções SVM e atribuir permissões

Existem vários comandos de CLI do ONTAP 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 do 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 storage, crie uma função e atribua todas as permissões à função.

   ```
   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 esse usuário.

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

3. Desbloquear o utilizador.

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

Comandos CLI do ONTAP para criar funções SVM e atribuir permissões

Existem vários comandos de CLI do ONTAP 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

Criar funções de cluster do ONTAP com Privileges mínimo

Você deve criar uma função de cluster do ONTAP com Privileges mínimo para que você não precise usar a função de administrador do ONTAP para executar operações no SnapCenter. Você pode executar vários comandos de CLI do ONTAP para criar a função de cluster do ONTAP e atribuir Privileges mínimo.

Passos

1. No sistema de storage, crie uma função e atribua todas as permissões à função.

   ```
   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 esse usuário.

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

3. Desbloquear o utilizador.

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

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

Há vários comandos de CLI do ONTAP 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 do ONTAP para sistemas ASA R2

Você deve criar uma função de cluster do ONTAP com Privileges mínimo para que você não precise usar a função de administrador do ONTAP para executar operações no SnapCenter. Você pode executar vários comandos de CLI do ONTAP para criar a função de cluster do ONTAP e atribuir Privileges mínimo.

Passos

1. No sistema de storage, crie uma função e atribua todas as permissões à função.

   ```
   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 esse usuário.

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

3. Desbloquear o utilizador.

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

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

Há vários comandos de CLI do ONTAP 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

Adicione um usuário ou grupo e atribua funções e ativos

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

Antes de começar

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

> Você pode incluir apenas os seguintes carateres especiais em nomes de usuário e nomes de grupo: Espaço ( ), hífen (-), sublinhado (_) e dois pontos (:).

- O SnapCenter inclui várias funções predefinidas.

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

- Os usuários DE ANÚNCIOS e grupos de AD adicionados ao RBAC do SnapCenter devem ter a permissão DE LEITURA no contentor usuários e no contentor computadores no ative Directory.
- Depois de atribuir uma função a um usuário ou grupo que contenha as permissões apropriadas, você deve atribuir o acesso do usuário aos ativos do SnapCenter, como hosts e conexões de armazenamento.

  Isso permite que os usuários executem as ações para as quais eles têm permissões nos ativos que são 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
Proteger recursos	host, política
Backup	host, grupo de recursos, política
Restaurar	host, grupo de recursos
Clone	host, grupo de recursos, política
Ciclo de vida do clone	host
Crie um Grupo de recursos	host

- 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, atribua a conexão de armazenamento para o volume de origem e destino ao usuário que executa a operação.

  Você deve adicionar ativos antes de atribuir acesso aos usuários.

> Se você estiver usando o plug-in do SnapCenter para funções do VMware vSphere para proteger VMs, VMDKs ou datastores, use a GUI do VMware vSphere para adicionar um usuário do vCenter a uma função do SnapCenter Plug-in para VMware vSphere. Para obter informações sobre as funções do VMware vSphere, "Funções predefinidas empacotadas com o plug-in SnapCenter para VMware vSphere" consulte .

Passos

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

Para este campo…	Faça isso…
Tipo de acesso	Selecione domínio ou grupo de trabalho 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. Por padrão, ele é pré-preenchido com o nome de domínio conetado. Tem de registar o domínio não fidedigno na na página **Definições** > **Definições globais** > **Definições de domínio**.
Tipo	Selecione Usuário ou Grupo O SnapCenter suporta apenas o grupo de segurança e não o grupo de distribuição.
Nome de utilizador	a. Digite o nome de usuário parcial e clique em **Add**. O nome de usuário diferencia maiúsculas de minúsculas. b. Selecione o nome de utilizador na lista de pesquisa. Quando você adiciona usuários de um domínio diferente ou de um domínio não confiável, você deve digitar o nome de usuário totalmente porque não há lista de pesquisa para usuários de vários domínios. Repita esta etapa para adicionar usuários ou grupos adicionais à função selecionada.
Funções	Selecione a função à qual deseja adicionar o usuário.

4. Clique em **Assign** e, em seguida, na página Assign Assets (atribuir ativos):
   a. Selecione o tipo de ativo na lista suspensa **Ativo**.
   b. Na tabela Ativo, selecione o ativo.

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

c. Repita este 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 recursos.

Configurar as definições do registo de auditoria

Os logs de auditoria são gerados para cada atividade do servidor SnapCenter. Por padrão, os logs de auditoria são protegidos no local instalado padrão *C: Arquivos de programas/NetApp/SnapCenter WebApp/audit*.

Os logs de auditoria são protegidos por meio da geração de resumos assinados digitalmente para cada evento de auditoria para protegê-lo da modificação não autorizada. Os resumos gerados são mantidos no arquivo de checksum de auditoria separado e em seguida são verificações periódicas de integridade para garantir a integridade do conteúdo.

Você deve ter feito login como a função "SnapCenterAdmin".

Sobre esta tarefa

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

  Unidades compartilhadas ou montadas em rede não são suportadas.

- Se o protocolo UDP for usado nas configurações do servidor Syslog, os erros devido à porta estão inativos ou não podem 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 de cmdlet do software SnapCenter".

Passos

1. Na página **Configurações**, navegue até **Configurações** > **Configurações globais** > **Configurações do log de auditoria**.

2. Na secção Registo de auditoria, introduza os detalhes.
3. Digite o diretório **Audit log** e o diretório de log de checksum* de auditoria
   a. Introduza o tamanho máximo do ficheiro
   b. Introduza o máximo de ficheiros de registo
   c. Insira a porcentagem de uso do espaço em disco para enviar um alerta
4. (Opcional) Ativar **Log UTC Time**.
5. (Opcional) ative **Audit Log Integrity Check Schedule** e clique em **Start Integrity Check** para verificação de integridade sob demanda.

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

6. (Opcional) ative os 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 o protocolo 'Trusted Root' para TLS 1,2.

   a. Introduza o sistema anfitrião do servidor Syslog
   b. Introduza a porta do servidor Syslog
   c. Introduza o protocolo Syslog Server
   d. Introduza o formato RFC
7. Clique em **Salvar**.
8. Você pode ver verificações de integridade de auditoria e verificações de espaço em disco clicando em **Monitor** > **jobs**.

Configure conexões MySQL seguras com o servidor SnapCenter

Você pode gerar certificados SSL (Secure Sockets Layer) e arquivos de chave se quiser proteger a comunicação entre o servidor SnapCenter e o servidor MySQL em configurações autônomas ou configurações NLB (Network Load Balancing).

Configurar conexões MySQL seguras para configurações autônomas do servidor SnapCenter

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

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 arquivos de chave para servidores e clientes MySQL no Windows usando o comando openssl.

Para obter informações, consulte "MySQL versão 5,7: Criando certificados SSL e chaves usando openssl"

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

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

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

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

3. Atualize o certificado CA, o certificado público do servidor, o certificado público do cliente, a chave privada do servidor e os caminhos de chave privada do cliente no ficheiro 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 o certificado CA, o certificado público do servidor e os caminhos de chave privada do servidor na seção [mysqld] do arquivo de configuração do servidor MySQL (my.ini).

   Você deve especificar o certificado CA, o certificado público do cliente e os caminhos de 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 [cliente] 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 da Web do servidor SnapCenter no servidor de informações da Internet (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 [cliente] do arquivo my.ini.

   O exemplo a seguir mostra os caminhos atualizados na seção [cliente] 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 da Web do servidor SnapCenter no IIS.

Configurar conexões MySQL seguras para configurações HA

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

Os seguintes certificados são gerados:

- Certificado CA

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

de HA.

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

Passos

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

   Para obter informações, consulte "MySQL versão 5,7: Criando certificados SSL e chaves usando openssl"

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

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

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

   O caminho padrão da pasta de dados MySQL é C:/// NetApp/ SnapCenter/ dados MySQL.

3. Atualize o certificado CA, o certificado público do servidor, o certificado público do cliente, a chave privada do servidor e os caminhos de chave privada do cliente no ficheiro 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 o certificado CA, o certificado público do servidor e os caminhos de chave privada do servidor na seção [mysqld] do arquivo de configuração do servidor MySQL (my.ini).

   Você deve especificar o certificado CA, o certificado público do cliente e os caminhos de 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 dados/dados.

   ```
   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 [cliente] 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 da 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.

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

      O caminho padrão da pasta de dados MySQL é C:/// NetApp/ SnapCenter/ dados MySQL.

      > 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 arquivos de chave para servidores MySQL e clientes no Windows usando o comando openssl.

      "MySQL versão 5,7: Criando certificados SSL e chaves usando openssl"

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

      Recomenda-se usar o FQDN do servidor como o nome comum para o certificado do servidor.

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

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

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

Você deve especificar o certificado CA, o certificado público do cliente e os caminhos de 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 dados/dados.

```
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 [cliente] 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 da Web do servidor SnapCenter no servidor de informações da Internet (IIS) em ambos os nós de HA.
6. Reinicie o serviço MySQL em ambos os nós de HA.
7. Atualize o valor da chave MySQLProtocol no arquivo SnapManager.Web.UI.dll.config para ambos os nós de 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 especificados na seção [cliente] do arquivo my.ini para ambos os nós de HA.

O exemplo a seguir mostra os caminhos atualizados na seção [cliente] 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 da Web do servidor SnapCenter no IIS em ambos os nós de HA.
10. Use o cmdlet Set-SmRepositoryConfig -RebuildSlave -Force PowerShell com a opção -Force em um dos nós de HA para estabelecer replicação MySQL segura em ambos os nós de HA.

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

Configurar autenticação baseada em certificado

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

Ativar autenticação baseada em certificado

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

- Para ativar a autenticação baseada em certificado de cliente:

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

- Para desativar a autenticação baseada em certificado de cliente:

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

Exportar certificados de autoridade de certificação (CA) do servidor SnapCenter

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

Antes de começar

Você deve ter configurado o SSL bidirecional.

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela certificados Snap-in, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados - computador local** > **Pessoal** > **certificados**.
5. Clique com o botão direito do rato no certificado CA adquirido, que é utilizado para o servidor SnapCenter 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 exporte a chave privada** e, em seguida, clique em **seguinte**.
Exportar formato de ficheiro	Clique em **seguinte**.
Nome do ficheiro	Clique em **Procurar** e especifique o caminho do arquivo para salvar o certificado e clique em **Avançar**.
Concluir o Assistente de exportação de certificados	Revise o resumo e clique em **Finish** para iniciar a exportação.

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

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

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

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela certificados Snap-in, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados - computador local** > **Pessoal** > **certificados**.
5. Clique com o botão direito 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 **seguinte**.
Ficheiro a importar	Selecione o certificado do servidor SnapCenter que termina com a extensão .cer.
Armazenamento de certificados	Clique em **seguinte**.
Concluir o Assistente de exportação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

Importar certificado CA para os hosts de plug-in UNIX

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

Sobre esta tarefa

- Você pode gerenciar a senha do armazenamento de chaves SPL e o alias do par de chaves assinadas CA em uso.
- A senha para o keystore SPL e para toda a senha de alias associada da chave privada deve ser a mesma.

Passos

1. Você pode recuperar a senha padrão do keystore SPL do arquivo de propriedade SPL. É o valor correspondente à chave `SPL_KEYSTORE_PASS`.
2. Altere a senha do keystore: `$ keytool -storepasswd -keystore keystore.jks`
3. Altere a senha para 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 no `spl.properties` arquivo.
5. Reinicie o serviço depois de alterar a senha.

Configure certificados raiz ou intermediários para o armazenamento de confiança SPL

Você deve configurar os certificados raiz ou intermediários para o SPL Trust-store. Você deve adicionar o certificado de CA raiz e, em seguida, os certificados de CA intermediários.

Passos

1. Navegue até a pasta que contém o keystore SPL: `/var/opt/snapcenter/spl/etc`.
2. Localize o arquivo `keystore.jks`.
3. Liste 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 depois de configurar os certificados raiz ou intermédios para o armazenamento de

confiança SPL.

Configure o par de chaves assinadas da CA para o armazenamento de confiança SPL

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança 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. Liste 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. Liste os certificados adicionados no keystore. `$ keytool -list -v -keystore keystore.jks`
6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

   A senha padrão do keystore SPL é o valor da chave SPL_KEYSTORE_PASS no `spl.properties` arquivo.

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

8. Se o nome do alias no certificado da CA for longo e contiver espaço ou carateres 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 a partir do keystore localizado no `spl.properties` arquivo. Atualize este valor com a chave SPL_CERTIFICATE_ALIAS.
10. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança SPL.

Exportar certificados SnapCenter

Você deve exportar os certificados SnapCenter no formato .pfx.

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snap-in**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **minha conta de usuário** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados - Utilizador atual** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato 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, exporte a chave privada** e clique em **Avançar**.
Exportar formato de ficheiro	Não faça alterações; clique em **seguinte**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Ficheiro a exportar	Especifique um nome de arquivo para o certificado exportado (você deve usar .pfx) e clique em **Next**.
Concluir o Assistente de exportação de certificados	Revise o resumo e clique em **Finish** para iniciar a exportação.

Configurar o certificado CA para o host Windows

Gerar arquivo CSR do 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 a CSR gerada. O certificado terá uma chave privada associada a ele.

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

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

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

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

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

Importar certificados CA

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

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.

2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados – computador local** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" 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 **Yes**, importe a chave privada e clique em **Next**.
Importar formato de ficheiro	Não faça alterações; clique em **seguinte**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluir o Assistente de importação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

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

7. Repita o passo 5 para a pasta "Pessoal".

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma cadeia 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 **thumbprint**.
   d. Copie os carateres 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", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

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.

Configure o certificado CA com os serviços de plug-in do host do Windows

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

Execute as etapas a seguir no servidor SnapCenter e em todos os hosts de plug-in em que os certificados de CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão SMCore 8145, 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"
   ```

Configure o 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 servidor Windows em que o SnapCenter está instalado.
2. No painel de navegação esquerdo, clique em **Connections** (ligações).
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**, clique em **ligações**.
6. Na página ligações, selecione **encadernação para https**.
7. Clique em **Editar**.
8. Na lista suspensa certificado SSL, selecione o certificado SSL recentemente importado.
9. Clique em **OK**.

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

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

> Certifique-se de que o certificado é adicionado usando o seguinte caminho: **Raiz da consola > certificados – computador local > autoridades de certificação raiz fidedignas > certificados**.

Ativar certificados de CA para SnapCenter

Você deve configurar os certificados da CA e ativar a validação do certificado da CA para o servidor SnapCenter.

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet Set-SmCertificateSettings.
- Você pode exibir o status do certificado para o servidor SnapCenter 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*. Em alternativa, pode consultar a "Guia de referência de 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 de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

- 🔒* * Indica que não há certificado CA habilitado ou atribuído ao host do plug-in.

- * * Indica que o certificado da CA foi validado com êxito.
- * * Indica que o certificado da 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 são concluídas com êxito.

Configure o certificado CA para o host Linux

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

Configure o certificado nginx

Passos

1. Navegue para */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. Recarregar nginx: `$nginx -s reload`

Configurar o 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 respetivamente.

   Apenas o formato *.pfx* é suportado para o certificado de registo de auditoria.

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

Configurar certificado 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 e a senha do certificado da CA, respetivamente.

   Somente o formato *.pfx* é suportado para o certificado SnapCenter .

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

Configure e ative 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 servidor SnapCenter 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 CA deve suportar autenticação de servidor e autenticação de cliente.
- Você deve ter um certificado CA com chave privada e detalhes de impressão digital.
- Você deve ter habilitado a configuração SSL unidirecional.

  Para obter mais detalhes, consulte "Configurar a seção certificado CA."

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

  O ambiente com alguns hosts ou servidor não habilitado para comunicação SSL bidirecional não é suportado.

Passos

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

   a. Remova a vinculação de porta de certificado auto-assinada do SnapCenter existente usando o seguinte comando 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 com o servidor SnapCenter e a 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 ao certificado da CA, adicione o usuário padrão do servidor Web IIS "**SnapCenter**" do SnapCenter na lista de permissões do certificado executando as etapas a seguir para acessar o certificado da CA recém-adquirida.
   a. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove SnapIn**.
   b. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
   c. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
   d. Clique em **raiz da consola** > **certificados – computador local** > **Pessoal** > **certificados**.
   e. Selecione o certificado SnapCenter.
   f. Para iniciar o assistente 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 **Add**, no assistente Select Users and Groups (Selecionar usuários e grupos) altere o local para o nome do computador local (mais importante na hierarquia)
   h. Adicione o usuário do AppPool/SnapCenter do IIS, dê permissões de controle total.

3. Para **permissão IIS de certificado CA**, adicione a nova entrada de chaves de Registro DWORD no servidor SnapCenter a partir do seguinte caminho:

   No editor de Registro do Windows, percorra para o caminho abaixo mencionado,

   ```
   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
   ```

Configure o plug-in do SnapCenter para comunicação SSL bidirecional

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

Antes de começar

Verifique se a impressão digital do certificado CA está disponível.

Passos

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

   a. Remova a vinculação de porta de certificado auto-assinada do SnapCenter existente usando o seguinte comando 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 com a 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
```

Ative a comunicação SSL bidirecional no host Windows

Você pode habilitar a comunicação SSL bidirecional para proteger a comunicação mútua entre o servidor SnapCenter 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 ativar a comunicação SSL bidirecional, execute os seguintes comandos no servidor SnapCenter para os plug-ins, 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 PowerShell:

   ```
   > Restart-Service -Name SnapManagerCoreService
   ```

Desative a comunicação SSL bidirecional

Você pode desativar 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 desativa a comunicação SSL bidirecional, o certificado da CA e sua configuração não são removidos.
- Para adicionar um novo host ao servidor SnapCenter, você deve desativar o SSL bidirecional para todos os hosts de plug-in.
- NLB e F5 não são suportados.

Passos

1. Para desativar a comunicação SSL bidirecional, execute os seguintes comandos no servidor SnapCenter 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 PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

Configure e habilite a 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 servidor SnapCenter 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 servidor SnapCenter.

Passos

1. Copiar **certificate.pem** para */etc/pki/CA-trust/source/ancors/*.
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 servidor SnapCenter.
6. Atualize os valores das seguintes chaves em **SnapManager.Web.UI.dll.config** localizado em _ /<installation path>/NetApp/SnapCenter/SnapManagerWeb_ e **SMCoreServiceHost.dll.config** localizado em */<installation path>/NetApp/SnapCenter/SMCore*.

- <add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />
- <add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>"/>

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 o keystore SPL e alias.
    a. Recupere a senha padrão do keystore SPL atribuída à chave **SPL_KEYSTORE_PASS** no arquivo de propriedades SPL.
    b. Altere a senha do keystore. `keytool -storepasswd -keystore keystore.jks`
    c. Altere a senha para 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 plug-in, adicione os certificados raiz e intermediários 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 no 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`

Ative a comunicação SSL no host Linux

Você pode habilitar a comunicação SSL bidirecional para proteger a comunicação mútua entre o servidor SnapCenter no host Linux e os plug-ins usando comandos do PowerShell.

Passo

1. Execute o seguinte para ativar a comunicação SSL unidirecional.

a. Entre na GUI do SnapCenter.

b. Clique em **Configurações** > **Configurações globais** e selecione **Ativar validação de certificado no servidor SnapCenter**.

c. Clique em **hosts** > **hosts gerenciados** e selecione o host do plug-in para o qual você deseja habilitar o SSL unidirecional.

d. Clique no ícone e, em seguida, clique em **Ativar validação de certificado**.

2. Ative a comunicação SSL bidirecional a partir do host Linux do servidor SnapCenter.

   - `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"}`

Configure o ative Directory, LDAP e LDAPS

Registre domínios não confiáveis do ative Directory

Você deve Registrar o ative Directory com o servidor SnapCenter para gerenciar hosts, usuários e grupos de vários domínios não confiáveis do ative Directory.

Antes de começar

Protocolos LDAP e LDAPS

- Você pode Registrar os domínios de diretório ativo não confiáveis usando o protocolo LDAP ou LDAPS.
- Você deve ter habilitado a comunicação bidirecional entre os hosts do plug-in e o servidor SnapCenter.
- A resolução DNS deve ser configurada do servidor SnapCenter para os hosts plug-in e vice-versa.

Protocolo LDAP

- O nome de domínio totalmente qualificado (FQDN) deve ser resolvido a partir do servidor SnapCenter.

  Você pode Registrar um domínio não confiável com o FQDN. Se o FQDN não for resolvido a partir do servidor SnapCenter, você pode se Registrar com um endereço IP do controlador de domínio e isso deve ser resolvido a partir do servidor SnapCenter.

Protocolo LDAPS

- Os certificados CA são necessários para que o LDAPS forneça criptografia de ponta a ponta durante a comunicação do diretório ativo.

  "Configure o certificado de cliente CA para LDAPS"

- Os nomes de host do controlador de domínio (DCHostName) devem ser acessíveis a partir do servidor SnapCenter.

Sobre esta tarefa

- Você pode usar a interface de usuário do SnapCenter, cmdlets do PowerShell ou 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 selecionar **LDAP**, especifique as informações necessárias para registar o domínio não fidedigno 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 domínio FQDN não for resolvido a partir do servidor SnapCenter, especifique um ou mais endereços IP do controlador de domínio. Para obter mais informações, "Adicione IP do controlador de domínio para domínio não confiável da GUI"consulte .

   b. Se selecionar **LDAPS**, especifique as informações necessárias para registar o domínio não fidedigno 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 controlador de domínio	Especifique um ou mais nomes de controlador de domínio e clique em **resolver**.
Endereços IP do controlador de domínio	Se os nomes do controlador de domínio não forem solucionáveis a partir do servidor SnapCenter, você deve corrigir as resoluções DNS.

6. Clique em **OK**.

Configure pools de aplicativos do IIS para habilitar permissões de leitura do ative Directory

Você pode configurar os Serviços de informações da Internet (IIS) no servidor Windows para criar uma conta de pool de aplicativos personalizada quando precisar ativar as permissões de leitura do ative Directory para o SnapCenter.

Passos

1. Abra o Gerenciador do IIS no servidor Windows em que 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, em seguida, clique em **…** para editar a identidade do conjunto de aplicações SnapCenter.
5. No campo conta personalizada, insira um nome de usuário de domínio ou conta de administrador de domínio com permissão de leitura do ative Directory.
6. Clique em OK.

   A conta personalizada substitui a conta ApplicationPoolIdentity incorporada para o pool de aplicativos do SnapCenter.

Configure o certificado de cliente CA para LDAPS

Você deve configurar o certificado de cliente CA para LDAPS no servidor SnapCenter quando o LDAPS do ative Directory do Windows estiver configurado com os certificados de CA.

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados – computador local** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" 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 **Browse**, selecione o *root Certificate* e clique em **Next**.
Concluir o Assistente de importação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

7. Repita os passos 5 e 6 para os certificados intermédios.

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em http://www.netapp.com/TM são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.