Instalação do servidor SnapCenter

SnapCenter Software 4.8

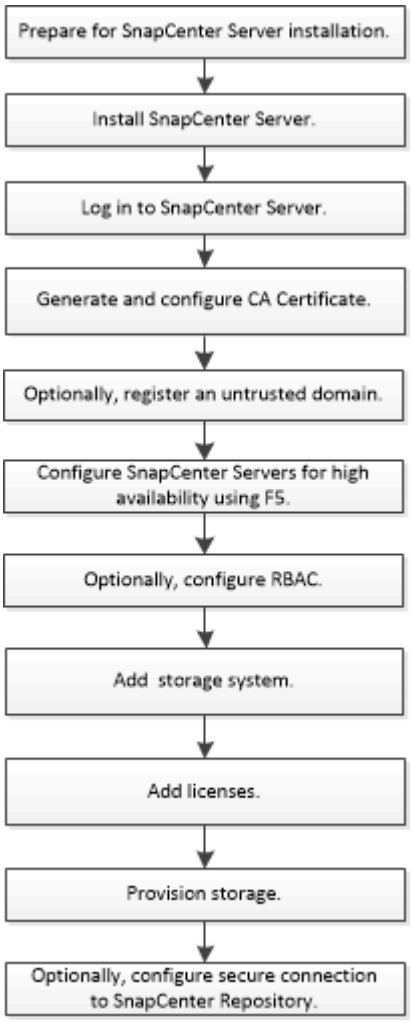
NetApp
September 26, 2025

Índice

Instalação do servidor SnapCenter

Fluxo de trabalho de instalação

O fluxo de trabalho mostra as diferentes tarefas necessárias para instalar e configurar o servidor SnapCenter.



Prepare-se para instalar o servidor SnapCenter

Requisitos de domínio e grupo de trabalho

O servidor SnapCenter pode ser instalado em sistemas que estejam em um domínio ou em um grupo de trabalho. O usuário usado para instalação deve ter Privileges de administrador na máquina no caso de grupo de trabalho e domínio.

Para instalar plug-ins do servidor SnapCenter e do SnapCenter em hosts Windows, você deve usar um dos seguintes:

- **Domínio 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

Antes de instalar o servidor SnapCenter, você deve estar familiarizado com os requisitos de espaço e dimensionamento. Você também deve aplicar as atualizações de sistema e segurança disponíveis.

Item	Requisitos
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 .
Contagem mínima de CPU	4 núcleos
RAM mínima	8 GB O pool de buffers do MySQL Server usa 20% do total de RAM.
Espaço mínimo no disco rígido para o software e logs do servidor SnapCenter	4 GB Se você tiver o repositório SnapCenter na mesma unidade em que o servidor SnapCenter está instalado, então é recomendável ter 10 GB.

Item	Requisitos
Espaço mínimo no disco rígido para o repositório SnapCenter	6 GB OBSERVAÇÃO: Se você tiver o servidor SnapCenter na mesma unidade em que o repositório SnapCenter está instalado, então é recomendável ter 10 GB.
Pacotes de software necessários	• Microsoft .NET Framework 4.7.2 ou posterior • Windows Management Framework (WMF) 4,0 ou posterior • PowerShell 4,0 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 . Para obter as informações mais recentes sobre versões suportadas, "Ferramenta de Matriz de interoperabilidade do NetApp" consulte .

Requisitos de host SAN

Se o seu host SnapCenter fizer parte de um ambiente FC/iSCSI, talvez seja necessário instalar software adicional no sistema para permitir o acesso ao storage ONTAP.

O SnapCenter não inclui Utilitários do anfitrião ou um DSM. Se o seu host SnapCenter fizer parte de um ambiente SAN, talvez seja necessário instalar e configurar o seguinte software:

- Utilitários do host

  Os Utilitários de host são compatíveis com FC e iSCSI e permitem que você use o MPIO em seus servidores Windows. Para obter informações, "Documentação dos utilitários do host"consulte .

- Microsoft DSM para Windows MPIO

  Este software funciona com drivers MPIO do 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 .

Sistemas e aplicações de storage compatíveis

Você deve conhecer o sistema de storage compatível, as aplicações e os bancos de

dados.

- O SnapCenter oferece suporte ao ONTAP 8.3.0 e posterior para proteger seus dados.
- O SnapCenter oferece suporte ao Amazon FSX for NetApp ONTAP para proteger seus dados da versão de patch do software SnapCenter 4,5 P1.

  Se você estiver usando o Amazon FSX for NetApp ONTAP, verifique se os plug-ins de host do servidor SnapCenter são atualizados para 4,5 P1 ou posterior para executar operações de proteção de dados.

  Para obter informações sobre o Amazon FSX for NetApp ONTAP, "Documentação do Amazon FSX para NetApp ONTAP" consulte .

- O SnapCenter oferece suporte à proteção de diferentes aplicativos e bancos de dados.

  Para obter informações detalhadas sobre os aplicativos e bancos de dados suportados, "Ferramenta de Matriz de interoperabilidade do NetApp" consulte .

Navegadores suportados

O software SnapCenter pode ser usado em vários navegadores.

- Chrome

  Se você estiver usando o V66, talvez não inicie a GUI do SnapCenter.

- Internet Explorer

  SnapCenter UI não carrega corretamente se você estiver usando IE 10 ou versões anteriores. Você deve atualizar para o IE 11.

  - Somente a segurança de nível padrão é suportada.

    Fazer alterações nas configurações de segurança do Internet Explorer resulta em problemas significativos de exibição do navegador.

  - A exibição de compatibilidade do Internet Explorer deve ser desativada.
- Microsoft Edge

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

Requisitos de conexão e porta

Você deve garantir que os requisitos de conexões e portas sejam atendidos antes de instalar os plug-ins do servidor SnapCenter e do aplicativo ou do banco de dados.

- Os aplicativos não podem compartilhar uma porta.

  Cada porta deve ser dedicada ao aplicativo apropriado.

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

Você pode alterar uma porta de plug-in após a instalação usando o assistente Modificar host.

- 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.

Tipo de porta	Porta predefinida
Porta SnapCenter	8146 (HTTPS), bidirecional, personalizável, como no URL *https://server:8146* Usado para comunicação entre o cliente SnapCenter (o usuário SnapCenter) e o servidor SnapCenter. Também usado para comunicação dos hosts de plug-in para o servidor SnapCenter. Para personalizar a porta, consulte "Instale o servidor SnapCenter usando o assistente de instalação."
Porta de comunicação SnapCenter SMCore	8145 (HTTPS), bidirecional, personalizável A porta é usada para comunicação entre o servidor SnapCenter e os hosts onde os plug-ins do SnapCenter estão instalados. Para personalizar a porta, consulte "Instale o servidor SnapCenter usando o assistente de instalação."
Porta MySQL	3306 (HTTPS), bidirecional A porta é usada para comunicação entre o SnapCenter e o banco de dados do repositório MySQL. Você pode criar conexões seguras do servidor SnapCenter para o servidor MySQL. "Saiba mais"

Tipo de porta	Porta predefinida
Hosts de plug-in do Windows	135, 445 (TCP) Além das portas 135 e 445, o intervalo de portas dinâmico especificado pela Microsoft também deve estar aberto. As operações de instalação remota usam o serviço Windows Management Instrumentation (WMI), que procura dinamicamente esse intervalo de portas. Para obter informações sobre o intervalo de portas dinâmico suportado, consulte "Visão geral do serviço e requisitos de porta de rede para Windows" As portas são usadas para comunicação entre o servidor SnapCenter e o host no qual o plug-in está sendo instalado. Para enviar binários de pacotes de plug-in para hosts de plug-in do Windows, as portas devem estar abertas apenas no host de plug-in e podem ser fechadas após a instalação.
Hosts plug-in Linux ou AIX	22 (SSH) As portas são usadas para comunicação entre o servidor SnapCenter e o host onde o plug-in está sendo instalado. As portas são usadas pelo SnapCenter para copiar binários de pacotes de plug-in para hosts de plug-in Linux ou AIX e devem ser abertas ou excluídas do firewall ou iptables.
Pacote de plug-ins do SnapCenter para Windows, pacote de plug-ins do SnapCenter para Linux ou pacote de plug-ins do SnapCenter para AIX	8145 (HTTPS), bidirecional, personalizável A porta é usada para comunicação entre SMCore e hosts onde o pacote plug-ins está instalado. O caminho de comunicação também precisa ser aberto entre o LIF de gerenciamento da SVM e o servidor SnapCenter. Para personalizar a porta, consulte "Adicione hosts e instale o plug-in do SnapCenter para Microsoft Windows" ou "Adicione hosts e instale o pacote de plug-ins do SnapCenter para Linux ou AIX."
Plug-in SnapCenter para banco de dados Oracle	27216, personalizável A porta JDBC padrão é usada pelo plug-in para Oracle para conexão com o banco de dados Oracle. Para personalizar a porta, consulte "Adicione hosts e instale o pacote de plug-ins do SnapCenter para Linux ou AIX."

Tipo de porta	Porta predefinida
Plug-ins personalizados para SnapCenter	9090 (HTTPS), fixo Esta é uma porta interna que é usada somente no host de plug-in personalizado; nenhuma exceção de firewall é necessária. A comunicação entre o servidor SnapCenter e plug-ins personalizados é roteada através da porta 8145.
Porta de comunicação do cluster ONTAP ou SVM	443 (HTTPS), bidirectional80 (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 o banco de dados SAP HANA vCode Spell Checkerports	3instance_number13 ou 3instance_number15, HTTP ou HTTPS, bidirecional e personalizável 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. Por exemplo, 32013 é o número da porta, por exemplo, 20 e 31015 é o número da porta, por exemplo, 10. Para personalizar a porta, consulte "Adicione hosts e instale pacotes plug-in em hosts remotos."
Porta de comunicação do controlador de domínio	Consulte a documentação da Microsoft para identificar as portas que devem ser abertas no firewall em um controlador de domínio para que a autenticação funcione corretamente. É necessário abrir as portas necessárias da Microsoft no controlador de domínio para que o servidor SnapCenter, os hosts Plug-in ou outro cliente Windows possam autenticar os usuários.

Para modificar os detalhes da porta, "Modificar hosts de plug-in"consulte .

Licenças SnapCenter

O SnapCenter requer várias licenças para habilitar a proteção de dados de aplicativos, bancos de dados, sistemas de arquivos e máquinas virtuais. O tipo de licenças do SnapCenter que você instala depende do ambiente de storage e dos recursos que

deseja usar.

Licença	Quando necessário
Baseado em controladora padrão da SnapCenter	Necessário para FAS e AFF A licença padrão da SnapCenter é uma licença baseada em controlador e está incluída como parte do pacote premium. Se você tiver a licença do SnapManager Suite, você também obtém o direito de licença padrão do SnapCenter. Se você quiser instalar o SnapCenter em uma base de avaliação com o storage FAS ou AFF, poderá obter uma licença de avaliação do pacote Premium entrando em Contato com o representante de vendas. O SnapCenter também é oferecido como parte do pacote de proteção de dados. Se você comprou o A400 ou posterior, você deve comprar o pacote de proteção de dados.
Baseado em capacidade padrão da SnapCenter	Necessário com ONTAP Select e Cloud Volumes ONTAP Se você é um cliente do Cloud Volumes ONTAP ou do ONTAP Select, precisa adquirir uma licença baseada em capacidade por TB com base nos dados gerenciados pelo SnapCenter. Por padrão, o SnapCenter envia uma licença de teste baseada em capacidade padrão SnapCenter de 90 dias e 100 TB incorporada. Para outros detalhes, entre em Contato com o representante de vendas.
SnapMirror ou SnapVault	ONTAP A licença SnapMirror ou SnapVault é necessária se a replicação estiver ativada no SnapCenter.
SnapRestore	Necessário para restaurar e verificar backups. Em sistemas de storage primário • Necessário nos sistemas de destino do SnapVault para executar a verificação remota e restaurar a partir de um backup. • Necessário nos sistemas de destino SnapMirror para efetuar a verificação remota.

Licença	Quando necessário
FlexClone	Necessário clonar bancos de dados e operações de verificação. Em sistemas de storage primário e secundário • Necessário nos sistemas de destino do SnapVault para criar clones a partir do backup do Vault secundário. • Necessário nos sistemas de destino do SnapMirror para criar clones do backup secundário do SnapMirror.
Protocolos	• Licença iSCSI ou FC para LUNs • Licença CIFS para compartilhamentos SMB • Licença NFS para VMDKs do tipo NFS • Licença iSCSI ou FC para VMDKs do tipo VMFS Necessário nos sistemas de destino do SnapMirror para fornecer dados se um volume de origem não estiver disponível.
Licenças padrão da SnapCenter (opcional)	Destinos secundários É recomendado, mas não obrigatório, que você adicione licenças padrão do SnapCenter a destinos secundários. Se as licenças padrão do SnapCenter não estiverem habilitadas em destinos secundários, você não poderá usar o SnapCenter para fazer backup de recursos no destino secundário após executar uma operação de failover. No entanto, é necessária uma licença FlexClone em destinos secundários para executar operações de clonagem e verificação.

As licenças do SnapCenter Advanced e do SnapCenter nas File Services estão obsoletas e não estão mais disponíveis.

Você deve instalar uma ou mais licenças do SnapCenter. Para obter informações sobre como adicionar licenças, "Adicione licenças padrão baseadas em controladora SnapCenter"consulte ou "Adicione licenças padrão baseadas em capacidade do SnapCenter".

Licenças SMBR (Single Mailbox Recovery)

Se você estiver usando o plug-in do SnapCenter para gerenciar bancos de dados do Microsoft Exchange Server e a recuperação de caixa de correio única (SMBR), você precisará de licença adicional para SMBR,

que precisa ser adquirida separadamente com base na caixa de correio do usuário.

A recuperação de caixa de correio única NetApp chegou ao fim da disponibilidade (EOA) em 12 de maio de 2023. Para obter mais informações, "CPC-00507"consulte . A NetApp continuará a oferecer suporte a clientes que adquiriram capacidade, manutenção e suporte da caixa de correio por meio de números de peça de marketing introduzidos em 24 de junho de 2020, durante o período do direito ao suporte.

O NetApp Single Mailbox Recovery é um produto parceiro fornecido pela Ontrack. O Ontrack PowerControls oferece recursos semelhantes aos da recuperação de caixa de correio única do NetApp. Os clientes podem adquirir novas licenças de software Ontrack PowerControls e renovações de manutenção e suporte Ontrack PowerControls do Ontrack (até licensingteam@ontrack.com) para recuperação granular da caixa de correio após a data EOA de 12 de maio de 2023.

Métodos de autenticação para suas credenciais

As credenciais usam diferentes métodos de autenticação, dependendo do aplicativo ou do ambiente. As credenciais autenticam os usuários para que eles possam executar operações do SnapCenter. Você deve criar um conjunto de credenciais para a instalação de plug-ins e outro conjunto para operações de proteção de dados.

Autenticação do Windows

O método de autenticação do Windows é autenticado no ative Directory. Para autenticação do Windows, o ative Directory é configurado fora do SnapCenter. O SnapCenter se autentica sem configuração adicional. Você precisa de uma credencial do Windows para executar tarefas como adicionar hosts, instalar pacotes de plug-in e agendar tarefas.

Autenticação de domínio não confiável

O SnapCenter permite a criação de credenciais do Windows usando usuários e grupos pertencentes aos domínios não confiáveis. Para que a autenticação seja bem-sucedida, você deve Registrar os domínios não confiáveis com o SnapCenter.

Autenticação local do grupo de trabalho

O SnapCenter permite a criação de credenciais do Windows com usuários e grupos de trabalho locais. A autenticação do Windows para usuários e grupos de grupos de trabalho locais não acontece no momento da criação de credenciais do Windows, mas é adiada até que o Registro do host e outras operações de host sejam executadas.

Autenticação do SQL Server

O método de autenticação SQL é autenticado em uma instância do SQL Server. Isso significa que uma instância do SQL Server deve ser descoberta no SnapCenter. Portanto, antes de adicionar uma credencial SQL, você deve adicionar um host, instalar pacotes de plug-in e atualizar recursos. Você precisa de autenticação do SQL Server para executar operações como agendamento no SQL Server ou descoberta de recursos.

Autenticação Linux

O método de autenticação Linux é autenticado em um host Linux. Você precisa de autenticação Linux durante a etapa inicial de adicionar o host Linux e instalar o pacote de plug-ins do SnapCenter remotamente a partir da GUI do SnapCenter.

Autenticação AIX

O método de autenticação AIX é autenticado em um host AIX. Você precisa de autenticação AIX durante a etapa inicial de adicionar o host AIX e instalar o pacote de plug-ins do SnapCenter para AIX remotamente a partir da GUI do SnapCenter.

Autenticação de banco de dados Oracle

O método de autenticação de banco de dados Oracle é autenticado em um banco de dados Oracle. Você precisa de uma autenticação de banco de dados Oracle para executar operações no banco de dados Oracle se a autenticação do sistema operacional (os) estiver desativada no host do banco de dados. Portanto, antes de adicionar uma credencial de banco de dados Oracle, você deve criar um usuário Oracle no banco de dados Oracle com sysdba Privileges.

Autenticação Oracle ASM

O método de autenticação Oracle ASM é autenticado em uma instância do Oracle Automatic Storage Management (ASM). Se for necessário acessar a instância do Oracle ASM e se a autenticação do sistema operacional (os) estiver desativada no host do banco de dados, você precisará de uma autenticação Oracle ASM. Portanto, antes de adicionar uma credencial Oracle ASM, você deve criar um usuário Oracle com sysasm Privileges na instância ASM.

Autenticação de catálogo RMAN

O método de autenticação de catálogo RMAN é autenticado no banco de dados de catálogo do Oracle Recovery Manager (RMAN). Se você configurou um mecanismo de catálogo externo e registrou seu banco de dados no banco de dados de catálogo, você precisa adicionar autenticação de catálogo RMAN.

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.

Gerenciamento da autenticação multifator (MFA)

Este tópico descreve como 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)

Este tópico descreve como ativar a funcionalidade MFA no servidor do Serviço de Federação do ative Directory (AD FS) e no servidor SnapCenter.

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 .

O que você vai precisar

- 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 -Enable -Path` o cmdlet.

   O parâmetro PATH especifica a localização do arquivo xml de metadados MFA do AD FS, que foi copiado para o servidor SnapCenter na etapa 3.

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. Clique em **confiança de parte**.
   b. Clique com o botão direito do Mouse na confiança de quem confia que foi criada para o SnapCenter e clique em **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 -Disable` 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.

Instale o servidor SnapCenter

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.

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

O que você vai precisar

- 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:\"`

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.

O que você vai precisar

- 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.

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

Para especificar o seguinte…	Use um destes formatos…
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.

Resultados

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"

Faça login no SnapCenter usando autenticação multifator (MFA)

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

O que você vai precisar

- 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 certificado CA

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.

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**.

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.

O que você vai precisar

- 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 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.

O que você vai precisar

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.

Para este campo…	Faça isso…
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 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.

Configurar alta disponibilidade

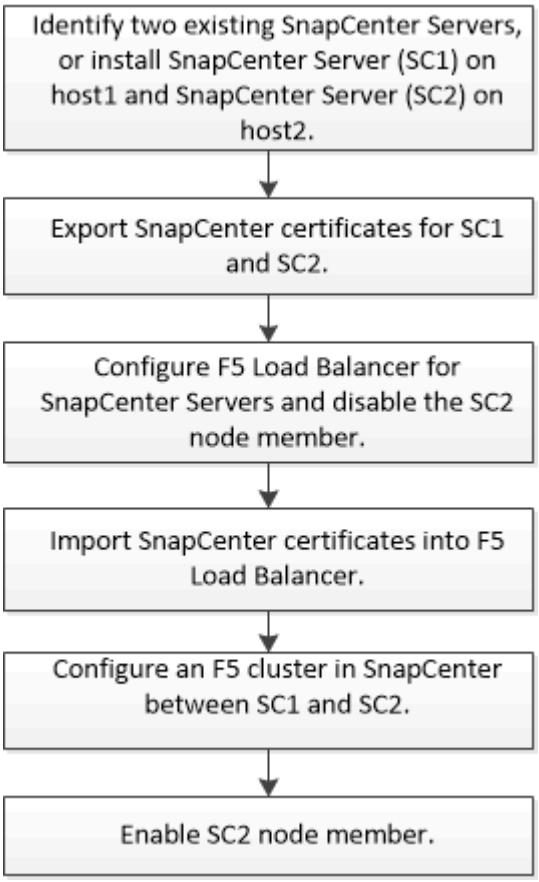
Configurar servidores SnapCenter para alta disponibilidade usando o F5

Para oferecer suporte à alta disponibilidade (HA) no SnapCenter, é possível 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.

Se você atualizou a partir do SnapCenter 4,2.x e estava usando anteriormente o balanceamento de carga de rede (NLB), você pode continuar usando essa configuração ou switch para F5.

A imagem do fluxo de trabalho lista as etapas para configurar os servidores SnapCenter para alta disponibilidade usando o balanceador de carga F5. Para obter instruções detalhadas, "Como configurar servidores SnapCenter para alta disponibilidade usando o balanceador de carga F5" consulte .



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 de configuração do F5

- 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 nó parcialmente resolvido pelo nó NLB ou F5 e se o nó SnapCenter não conseguir alcançar esse nó, a página do host do SnapCenter alternará entre hosts inativos e o estado em execução com frequência. Para resolver esse problema, você deve garantir que ambos os nós do SnapCenter sejam capazes de resolver o host no nó NLB ou F5.
- Os comandos SnapCenter para configurações de MFA devem ser executados em todos os nós. 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 nó será bloqueado após a ativação do MFA.
- Durante o failover, as configurações do log de auditoria não serão refletidas no segundo nó. Portanto, você deve repetir manualmente as configurações de log de auditoria no nó passivo F5 quando ele se tornar ativo.

Configure o Microsoft Network Load Balancer manualmente

Você pode configurar o balanceamento de carga de rede (NLB) da Microsoft para configurar o SnapCenter High Availability. A partir do SnapCenter 4,2, 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 .

SnapCenter 4.1.1 ou configuração anterior suportada de balanceamento de carga de rede (NLB) durante a instalação do SnapCenter.

Mude de NLB para F5 para obter 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 .

Exportar certificados SnapCenter

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.

Resultados

Os certificados são exportados no formato .pfx.

Configurar controles de acesso baseados em função (RBAC)

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.

O que você vai precisar

- 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.

  No SnapCenter 4,5, você pode incluir apenas os seguintes carateres especiais em nomes de usuário e nomes de grupo: Espaço ( ), hífen (-), sublinhado (_) e dois pontos (:). Se você quiser usar uma função que você criou em uma versão anterior do SnapCenter com esses carateres especiais, você pode desativar a validação do nome da função alterando o valor do parâmetro 'DisableSQLInjectionValidation' para true no arquivo web.config localizado onde o SnapCenter está instalado. Depois de modificar o valor, não é necessário reiniciar o serviço.

- 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 cópias Snapshot, atribua a conexão de storage para o volume de origem e destino ao usuário que está realizando 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.

Crie uma função

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

Você deve ter feito 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. Na página Adicionar função, especifique um nome e uma descrição para a nova função.

   No SnapCenter 4,5, você pode incluir apenas os seguintes carateres especiais em nomes de usuário e nomes de grupo: Espaço ( ), hífen (-), sublinhado (_) e dois pontos (:). Se você quiser usar uma função que você criou em uma versão anterior do SnapCenter com esses carateres especiais, você pode desativar a validação do nome da função alterando o valor do parâmetro 'DisableSQLInjectionValidation' para true no arquivo web.config localizado onde o SnapCenter está instalado. Depois de modificar o valor, não é necessário reiniciar o serviço.

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 ONTAP RBAC usando comandos de login de segurança

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

O que você vai precisar

- Antes de criar uma função RBAC do ONTAP para sistemas de storage que executam o Clustered ONTAP, é necessário identificar o seguinte:
  - A tarefa (ou tarefas) que você deseja executar
  - O Privileges necessário para executar essas tarefas
- A configuração de uma função RBAC exige que você execute as seguintes ações:
  - 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.
  - Varie a configuração dependendo se os plug-ins do SnapCenter estão conetados ao IP do administrador de cluster para todo o cluster ou diretamente conetados a um SVM no cluster.

Sobre esta tarefa

Para simplificar a configuração dessas funções em sistemas de storage, você pode usar a ferramenta Criador de usuários do RBAC para Data ONTAP, publicada no Fórum de Comunidades do NetApp.

Esta ferramenta lida automaticamente com a configuração correta do ONTAP Privileges. Por exemplo, a ferramenta Criador de Usuário RBAC para Data 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 Data 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".

> Para consistência, a documentação do SnapCenter refere-se às funções como usando o Privileges. A GUI do OnCommand System Manager usa o termo *attribute* em vez de *Privilege*. Ao configurar funções RBAC do ONTAP, esses dois termos significam a mesma coisa.

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 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 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 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
```

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 -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 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 "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 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 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`

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.

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**.

Adicione sistemas de storage

Você deve configurar o sistema de armazenamento que dá acesso à SnapCenter ao armazenamento ONTAP ou ao Amazon FSX for NetApp ONTAP para executar operações de proteção de dados e provisionamento.

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.

O que você vai precisar

- 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 estiver planejando replicar cópias Snapshot 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 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 do sistema de armazenamento, que não incluem o nome do 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.
Nome de utilizador/Palavra-passe	Insira as credenciais do usuário de storage que tem o Privileges necessário para acessar o sistema de storage.

Para este campo…	Faça isso…
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.

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

      A porta padrão 443 normalmente funciona.

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

      O valor padrão é de 60 segundos.

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

Resultados

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
enable -noteto enable
```

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

Adicione licenças padrão baseadas em controladora SnapCenter

Uma licença baseada em controlador padrão da SnapCenter é necessária se você estiver usando controladores de storage FAS ou AFF.

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
- Habilitado adicionando-o diretamente ao controlador de storage FAS ou AFF usando a linha de comando Gerenciador de sistema do ONTAP ou cluster de storage

  Você não insere nenhuma informação de licença na GUI do SnapCenter para as licenças baseadas no controlador do 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 GUI do SnapCenter para ver se uma licença do SnapManager Suite está instalada em sistemas de storage primário FAS ou AFF e identificar quais sistemas de storage podem exigir licenças do SnapManager Suite. As licenças do SnapManager Suite se aplicam somente a SVMs ou clusters do FAS e AFF em sistemas de storage primário.

Se você já tiver uma licença do SnapManager Suite no controlador, o direito de licença baseado em controlador padrão da SnapCenter é fornecido automaticamente. Os nomes da licença SnapManagerSuite e da licença baseada no controlador padrão SnapCenter são usados de forma intercambiável, mas referem-se 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 ou AFF.
   -  Indica que uma licença do SnapManager Suite não está instalada em um sistema de storage primário FAS ou AFF.
   - Não aplicável indica que uma licença do SnapManager Suite não é aplicável porque o controlador de storage está em plataformas de storage Cloud Volumes ONTAP, ONTAP Select ou secundárias.

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 ou AFF.

A licença baseada em controladora padrão do SnapCenter é exibida como licença SnapManagerSuite no controlador.

Passos

1. Faça login no controlador NetApp usando a linha de comando ONTAP.
2. Digite o comando license show e, em seguida, exiba a saída para determinar se a licença 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

Você precisa ter o número de série do controlador para recuperar o número de série da sua licença baseada no controlador. Você pode recuperar o número de série do controlador usando a linha de comando ONTAP. Você deve ser um administrador de cluster no sistema FAS ou AFF.

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 você estiver usando o armazenamento FAS ou AFF, poderá recuperar a licença baseada no controlador SnapCenter do site de suporte da NetApp antes de instalá-la 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, nenhuma informação será retornada 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 ou AFF e tiver uma licença padrão ou SnapManagerSuite SnapCenter.

Antes de começar

- Você deve ser um administrador de cluster no sistema FAS ou AFF.
- 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 ou AFF, obtenha uma licença de avaliação do pacote Premium para instalar na controladora.

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 padrão SnapCenter baseada em controlador e precisar remover a licença de avaliação baseada em capacidade (número de série que termina com "'50""), você deve usar os comandos MySQL para remover a licença de teste manualmente. A licença de teste não pode ser excluída usando a GUI 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. Se você adquiriu uma licença baseada em capacidade padrão do SnapCenter e a adiciona à GUI do SnapCenter, a licença de teste será substituída automaticamente.

Passos

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

      Para obter informações sobre os cmdlets, "Guia de referência de cmdlet do software SnapCenter" consulte .
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';
   ```

Adicione licenças padrão baseadas em capacidade do SnapCenter

Você usa uma licença de capacidade padrão da SnapCenter para proteger dados nas plataformas ONTAP Select e Cloud Volumes ONTAP.

Uma licença de capacidade tem as seguintes caraterísticas:

- Composto por um número de série de nove dígitos com o formato 51xxxxxxx

  Você usa o número de série da licença e as credenciais de login válidas do site de suporte da NetApp para habilitar a licença usando a GUI do SnapCenter.
- Disponível como uma licença perpétua separada, com o custo baseado na capacidade de storage usada ou no tamanho dos dados que você deseja proteger, o que for menor, e os dados são gerenciados pela SnapCenter
- Disponível por terabyte

  Por exemplo, você pode obter uma licença baseada em capacidade para 1 TB, 2 TBs, 4 TBs e assim por diante.
- Disponível como uma licença de teste de 90 dias com direito a capacidade de 100 TB

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

O SnapCenter calcula automaticamente o uso da capacidade uma vez por dia à meia-noite no storage ONTAP Select e Cloud Volumes ONTAP gerenciado. Quando você usa uma licença de capacidade padrão, o SnapCenter calcula a capacidade não utilizada deduzindo a capacidade usada em todos os volumes da capacidade total licenciada. Se a capacidade utilizada exceder a capacidade licenciada, é apresentado um aviso de utilização excessiva no painel do SnapCenter. Se você configurou limites de capacidade e notificações no SnapCenter, um e-mail será enviado quando a capacidade usada atingir o limite especificado.

Etapa 1: Calcule os requisitos de capacidade

Antes de obter uma licença baseada em capacidade do SnapCenter, calcule a quantidade de capacidade em um host que deve ser gerenciado pelo SnapCenter.

Você deve ser um administrador de cluster no sistema Cloud Volumes ONTAP ou ONTAP Select.

Sobre esta tarefa

O SnapCenter calcula a capacidade real utilizada. Se o tamanho do sistema de arquivos ou banco de dados for de 1 TB, mas apenas 500 GB de espaço for usado, o SnapCenter calcula 500 GB de capacidade usada. A capacidade de volume é calculada após a deduplicação e a compactação, e é baseada na capacidade usada de todo o volume.

Passos

1. Faça login no controlador NetApp usando a linha de comando ONTAP.
2. Para ver a capacidade de volume utilizada, introduza o comando.

```
select::> vol show -fields used -volume Engineering,Marketing
vserver volume       used
------- ------       ------
VS1     Engineering  2.13TB
VS1     Marketing    2.62TB

2   entries were displayed.
```

A capacidade combinada usada para os dois volumes é inferior a 5 TB; portanto, se você quiser proteger todos os 5 TB de dados, o requisito mínimo de licença baseada em capacidade da SnapCenter é de 5 TB.

No entanto, se você quiser proteger apenas 2 TB dos 5 TB da capacidade total utilizada, você pode adquirir uma licença baseada em capacidade de 2 TB.

Passo 2: Recupere o número de série da licença baseada em capacidade

O número de série da licença baseada em capacidade do SnapCenter está disponível na confirmação do pedido ou no pacote de documentação; no entanto, se você não tiver esse número de série, poderá recuperá-lo no site de suporte da NetApp.

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

Passos

1. Inicie sessão no "Site de suporte da NetApp".

2. Navegue até **sistemas** > **licenças de software**.
3. Na área critérios de seleção, escolha **SC_STANDARD** no menu suspenso Mostrar tudo: Números de série e licenças.

4. Digite o nome da sua empresa e selecione **Go!**.

   É apresentado o número de série da licença SnapCenter de nove dígitos, com o formato 51xxxxxxx.

5. Registe o número de série.

Passo 3: Gerar um arquivo de licença do NetApp

Se você não quiser inserir as credenciais do site de suporte da NetApp e o número de série da licença SnapCenter na interface gráfica do usuário do SnapCenter ou se não tiver acesso à Internet ao site de suporte da NetApp da SnapCenter, você poderá gerar um arquivo de licença do NetApp (NLF). Em seguida, você pode baixar e armazenar o arquivo em um local acessível a partir do host do SnapCenter.

Antes de começar

- Você deve usar o SnapCenter com ONTAP Select ou Cloud Volumes ONTAP.
- Você deve ter credenciais de login válidas no site de suporte da NetApp.
- Você deve ter seu número de série de nove dígitos da licença no formato 51xxxxxxx.

Passos

1. Navegue até "Gerador de arquivos de licença NetApp" .
2. Introduza as informações necessárias.
3. No campo linha de produtos, selecione **padrão SnapCenter (baseado em capacidade)** no menu suspenso.
4. No campo número de série do produto, insira o número de série da licença SnapCenter
5. Leia e aceite a Política de Privacidade de dados da NetApp e selecione **Enviar**.
6. Guarde o ficheiro de licença e, em seguida, registe a localização do ficheiro.

Passo 4: Adicione licença baseada em capacidade

Se você estiver usando o SnapCenter com plataformas ONTAP Select ou Cloud Volumes ONTAP, instale uma ou mais licenças baseadas em capacidade do SnapCenter.

Antes de começar

- Você deve fazer login como usuário Administrador do SnapCenter.

- Você deve ter credenciais de login válidas no site de suporte da NetApp.
- Você deve ter seu número de série de nove dígitos da licença no formato 51xxxxxxx.

  Se você estiver usando um arquivo de licença NetApp (NLF) para adicionar sua licença, você deve saber a localização do arquivo de licença.

Sobre esta tarefa

Você pode executar as seguintes tarefas na página Configurações:

- Adicione uma licença.
- Veja os detalhes da licença para localizar rapidamente informações sobre cada licença.
- Modifique uma licença quando quiser substituir a licença existente, por exemplo, para atualizar a capacidade da licença ou para alterar as configurações de notificação de limite.
- Exclua uma licença quando você quiser substituir uma licença existente ou quando a licença não for mais necessária.

> A licença de teste (número de série que termina com 50) não pode ser excluída usando a GUI do SnapCenter. A licença de teste é automaticamente substituída quando você adiciona uma licença baseada em capacidade padrão da SnapCenter adquirida.

Passos

1. No painel de navegação esquerdo, selecione **Configurações**.
2. Na página Configurações, selecione **Software**.
3. Na seção Licença da página Software, selecione **Add** (+).
4. No assistente Adicionar licença SnapCenter, selecione um dos seguintes métodos para obter a licença que deseja adicionar:

Para este campo…	Faça isso…
Insira suas credenciais de login do site de suporte da NetApp (NSS) para importar licenças	a. Introduza o seu nome de utilizador NSS. b. Introduza a sua palavra-passe NSS. c. Introduza o número de série da licença baseada no controlador.
Ficheiro de licença do NetApp	a. Navegue até o local do arquivo de licença e selecione-o. b. Selecione **Open**.

5. Na página notificações, insira o limite de capacidade no qual o SnapCenter envia notificações por e-mail, EMS e AutoSupport.

   O limite padrão é de 90%.

6. Para configurar o servidor SMTP para notificações por e-mail, selecione **Configurações** > **Configurações globais** > **Configurações do servidor de notificação** e insira os seguintes detalhes:

Para este campo…	Faça isso…
Preferência por e-mail	Escolha **sempre** ou **nunca**.
Forneça configurações de e-mail	Se selecionar **Always**, especifique o seguinte: • Endereço de e-mail do remetente • Endereço de e-mail do destinatário • Opcional: Edite a linha de assunto padrão O assunto padrão diz o seguinte: "Notificação de capacidade de licença da SnapCenter".

7. Se pretender que as mensagens do sistema de Gestão de Eventos (EMS) sejam enviadas para o syslog do sistema de armazenamento ou que as mensagens AutoSupport sejam enviadas para o sistema de armazenamento para operações com falha, selecione as caixas de verificação adequadas. A ativação do AutoSupport é recomendada para ajudar a solucionar problemas que possam ocorrer.
8. Selecione **seguinte**.
9. Revise o resumo e selecione **Finish**.

Provisione seu sistema de storage

Provisione storage em hosts do Windows

Configurar armazenamento LUN

Pode utilizar o SnapCenter para configurar um LUN ligado a FC ou ligado a iSCSI. Você também pode usar o SnapCenter para conetar um LUN existente a um host do Windows.

LUNs são a unidade básica de armazenamento em uma configuração SAN. O host do Windows vê LUNs no seu sistema como discos virtuais. Para obter mais informações, "Guia de configuração de SAN ONTAP 9"consulte .

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.

Desligar uma sessão iSCSI

Ocasionalmente, pode ser necessário desconetar uma sessão iSCSI de um destino com o qual você tem várias sessões.

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. Na lista de sessões iSCSI, selecione a sessão que deseja desconetar e clique em **desconetar sessão**.
6. Na caixa de diálogo desconetar sessão, clique em **OK**.

   O SnapCenter desliga a sessão iSCSI.

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.

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.

O que você vai precisar

- 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**.

Selecione…	Se…
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.
Tamanho da LUN	Especifique o tamanho do LUN; mínimo de 150 MB. Selecione MB, GB ou TB na lista suspensa adjacente.

Propriedade	Descrição
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 uma cópia Snapshot antes de redimensionar um LUN.
- Se você precisar restaurar um LUN de uma cópia Snapshot feita antes que o LUN fosse redimensionado, o SnapCenter redimensionará automaticamente o LUN para o tamanho da cópia Snapshot.

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

O que você vai precisar

- 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.
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.

Neste campo…	Faça isso…
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.
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.

O que você vai precisar

- 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.

Crie e gerencie compartilhamentos SMB

Para configurar um compartilhamento SMB3 em uma máquina virtual de armazenamento (SVM), você pode usar a interface de usuário do SnapCenter ou cmdlets do PowerShell.

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.
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.

O que você vai precisar

- 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 você 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 fornecidos pelo plug-in do SnapCenter para Microsoft Windows. 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 cópias Snapshot.

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 .

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 web.config.

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

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

7. Atualize o arquivo web.config com os caminhos que foram 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 web.config para ambos os nós de HA.

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

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

8. Atualize o arquivo web.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.

Recursos ativados em seu host Windows durante a instalação

O instalador do servidor SnapCenter permite os recursos e funções do Windows em seu host Windows durante a instalação. Isso pode ser de interesse para fins de 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 ◦ ASP.NET 4.7.2 ◦ 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 4.7.2 é um dos nossos selecionados Jogos de Plataforma	• .NET Framework 4.7.2 • ASP.NET 4.7.2 • Windows Communication Foundation (WCF) HTTP Activation45 ◦ Ativação TCP ◦ Ativação HTTP ◦ Ativação do Message Queuing (MSMQ) 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. • MSMQ Server
Serviço de ativação do processo do Windows	• Modelo do processo
APIs de configuração	Tudo

Informações sobre direitos autorais

Informações sobre marcas comerciais