Configurar o SnapCenter Server

SnapCenter software

NetApp
November 06, 2025

Índice

Configurar o SnapCenter Server

Adicionar e provisionar o sistema de armazenamento

Adicionar sistemas de armazenamento

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

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

Antes de começar

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

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

- Os nomes dos sistemas de armazenamento devem ser exclusivos.

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

Sobre esta tarefa

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

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

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

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

Passos

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

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

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

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

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

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

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

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

      A porta padrão 443 normalmente funciona.

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

      O valor padrão é 60 segundos.

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

Resultado

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

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

  Se você adicionou FSx SVMs, eles serão listados aqui.

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

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

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

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

Depois que você terminar

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

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

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

Conexões e credenciais de armazenamento

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

Conexões de armazenamento

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

Credenciais

- Administrador de domínio ou qualquer membro do grupo de administradores

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

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

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

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

- Credenciais para grupos de recursos individuais

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

Provisionar armazenamento em hosts Windows

Criar e gerenciar igroups

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

Criar um igroup

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

Passos

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

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

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

   O SnapCenter cria o igroup no sistema de armazenamento.

Renomear um igroup

Você pode usar o SnapCenter para renomear um igroup existente.

Passos

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

Modificar um igroup

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

Passos

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

Excluir um igroup

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

Passos

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

   O SnapCenter exclui o igroup.

Criar e gerenciar discos

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

- O SnapCenter suporta apenas discos básicos. Os discos dinâmicos não são suportados.

- Para GPT, apenas uma partição de dados é permitida e para MBR, uma partição primária com um volume formatado com NTFS ou CSVFS e um caminho de montagem.
- Estilos de partição suportados: GPT, MBR; em uma VM VMware UEFI, apenas discos iSCSI são suportados

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

Visualizar os discos em um host

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

Passos

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

   Os discos estão listados.

Exibir discos agrupados

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

Passos

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

   Os discos estão listados.

Estabelecer uma sessão iSCSI

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

Antes de começar

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

Sobre esta tarefa

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

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

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

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

Passos

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

   O assistente Estabelecer Sessão é exibido.

6. No assistente Estabelecer Sessão, identifique o destino:

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

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

   O SnapCenter estabelece a sessão iSCSI.

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

Crie LUNs ou discos conectados por FC ou iSCSI

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

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

Antes de começar

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

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

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

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

Sobre esta tarefa

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

Passos

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

   O assistente Criar disco é aberto.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Redimensionar um disco

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

Sobre esta tarefa

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

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

Passos

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

   Os discos estão listados.

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

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

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

   O SnapCenter redimensiona o disco.

Conecte um disco

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

Antes de começar

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

Passos

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

   O assistente Conectar disco é aberto.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Desconectar um disco

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

Antes de começar

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

Sobre esta tarefa

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

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

Passos

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

   Os discos estão listados.

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

   O SnapCenter desconecta o disco.

Excluir um disco

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

Passos

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

   Os discos estão listados.

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

   O SnapCenter exclui o disco.

Crie e gerencie compartilhamentos SMB

Para configurar um compartilhamento SMB3 em uma máquina virtual de armazenamento

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

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

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

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

Criar um compartilhamento SMB

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

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

Passos

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

   A caixa de diálogo Novo compartilhamento é aberta.

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

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

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

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

   O SnapCenter cria o compartilhamento SMB no SVM.

Excluir um compartilhamento SMB

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

Passos

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

   O SnapCenter exclui o compartilhamento SMB do SVM.

Recupere espaço no sistema de armazenamento

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

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

Antes de começar

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

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

Sobre esta tarefa

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

  Fazer isso pode atrasar o processo de recuperação.

Etapa

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

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

drive_path é o caminho da unidade mapeado para o LUN.

Provisionar armazenamento usando cmdlets do PowerShell

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

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

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

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

Provisionar armazenamento em ambientes VMware

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

Plataformas de sistema operacional convidado VMware suportadas

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

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

- LUNs RDM

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

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

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

Limitações relacionadas ao servidor VMware ESXi

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

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

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

Privilégios mínimos do vCenter necessários para operações do SnapCenter RDM

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

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

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

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

Gerenciar LUNs FC RDM em um cluster Microsoft

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

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

Requisitos

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

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

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

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

  Você não pode usar discos virtuais para armazenamento compartilhado.

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

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

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

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

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

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

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

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

Limitações

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

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

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

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

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

Criar um FC RDM LUN compartilhado

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

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

Adicionar licenças baseadas no controlador SnapCenter Standard

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

A licença baseada em controlador tem as seguintes características:

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

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

- Bloqueado no número de série do controlador

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

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

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

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

Passos

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

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

   A coluna Licença do Controlador exibe o seguinte status:

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

Etapa 2: Identificar as licenças instaladas no controlador

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

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

Passos

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

Exemplo de saída

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

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

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

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

Etapa 3: recuperar o número de série do controlador

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

Passos

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

Exemplo de saída

```
cluster1::> system show -instance

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

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

3. Registre os números de série.

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

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

Antes de começar

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

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

- Você deve ter o número de série do controlador.

Passos

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

Uma lista de licenças para o controlador especificado é exibida.

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

Etapa 5: adicionar licença baseada em controlador

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

Antes de começar

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

Sobre esta tarefa

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

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

Passos

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

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

   Este comando está disponível no nível de privilégio de administrador.

3. Verifique se a licença do SnapManagerSuite está instalada:

```
license show
```

Etapa 6: Remova a licença de teste

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

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

Passos

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

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

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

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

Configurar alta disponibilidade

Configurar servidores SnapCenter para alta disponibilidade

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

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

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

Configurar alta disponibilidade usando F5

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

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

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

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

Informações adicionais

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

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

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

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

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

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

Passos

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

o Amazon EventBridge Scheduler para iniciar um Step Functions" .

Configurar alta disponibilidade usando o balanceador de carga do Azure

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

Passos

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

== Mude de NLB para F5 para alta disponibilidade

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

Passos

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

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

Alta disponibilidade para o repositório SnapCenter MySQL

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

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

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

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

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

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

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

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

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

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

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

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

Configurar o controle de acesso baseado em função (RBAC)

Criar uma função

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

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

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Funções**.
3. Clique + .
4. Especifique um nome e uma descrição para a nova função.

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

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

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

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

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

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

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

Antes de começar

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

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

  Você deve sempre atribuir os privilégios de acesso total primeiro.

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

Sobre esta tarefa

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

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

duplicados e os ignorará.

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

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

Passos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Crie funções SVM com privilégios mínimos

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

Passos

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

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

   Você deve repetir este comando para cada permissão.

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

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

3. Desbloqueie o usuário.

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

Comandos ONTAP CLI para criar funções SVM e atribuir permissões

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

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

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

"snapmirror policy remove-rule" -access all

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

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

"vserver export-policy rule create" -access all

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

Criar funções SVM para sistemas ASA r2

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

Passos

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

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

   Você deve repetir este comando para cada permissão.

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

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

3. Desbloqueie o usuário.

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

Comandos ONTAP CLI para criar funções SVM e atribuir permissões

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

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

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

"snapmirror policy show" -access all

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

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

"vserver export-policy rule show" -access all

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

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all`
- `security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name`
- `security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name`

Crie funções de cluster ONTAP com privilégios mínimos

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

Passos

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

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

   Você deve repetir este comando para cada permissão.

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

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

3. Desbloqueie o usuário.

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

Comandos ONTAP CLI para criar funções de cluster e atribuir permissões

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

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

"cluster peer show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all

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

"nvme namespace modify" -access all

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

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

"volume qtree show" -access all

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

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

Criar funções de cluster ONTAP para sistemas ASA r2

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

Passos

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

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

   Você deve repetir este comando para cada permissão.

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

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

3. Desbloqueie o usuário.

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

Comandos ONTAP CLI para criar funções de cluster e atribuir permissões

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

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

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

"nvme subsystem map" -access all

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

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

"volume file clone create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all

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

```
"vserver modify" -access all
```

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

Adicionar um usuário ou grupo e atribuir função e ativos

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

Antes de começar

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

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

- O SnapCenter inclui várias funções predefinidas.

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

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

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

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

Operação	Atribuição de ativos
Proteja os recursos	anfitrião, política
Backup	host, grupo de recursos, política
Restaurar	host, grupo de recursos
Clone	host, grupo de recursos, política
Ciclo de vida do clone	hospedar
Criar um Grupo de Recursos	hospedar

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

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

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

  Você deve adicionar ativos antes de atribuir acesso aos usuários.

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

Passos

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

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

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

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

c. Repita esse procedimento para todos os ativos necessários.

d. Clique em **Salvar**.

5. Clique em **Enviar**.

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

Configurar definições de log de auditoria

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

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

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

Sobre esta tarefa

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

  Unidades compartilhadas ou montadas em rede não são suportadas.

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

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

Passos

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

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

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

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

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

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

Configurar conexões MySQL seguras com o SnapCenter Server

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

Configurar conexões MySQL seguras para configurações autônomas do SnapCenter Server

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

Os seguintes certificados são gerados:

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

Passos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Inicie o aplicativo web SnapCenter Server no IIS.

Configurar conexões MySQL seguras para configurações de HA

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

Os seguintes certificados são gerados:

- Certificado CA

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

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

Passos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

+

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

+

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

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

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

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

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

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

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

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

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

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

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

Informações sobre direitos autorais

Informações sobre marcas comerciais