



Proteja bancos de dados Microsoft SQL Server

SnapCenter Software 4.7

NetApp
April 02, 2025

Índice

Proteja bancos de dados Microsoft SQL Server	1
Plug-in do SnapCenter para Microsoft SQL Server	1
Visão geral do plug-in do SnapCenter para Microsoft SQL Server	1
O que você pode fazer com o plug-in SnapCenter para Microsoft SQL Server	1
Plug-in do SnapCenter para recursos do Microsoft SQL Server	2
Suporte para mapeamento LUN assimétrico em clusters Windows	3
Tipos de storage compatíveis com plug-ins do SnapCenter para Microsoft Windows e Microsoft SQL Server	4
Recomendações de layout de storage para o plug-in SnapCenter para Microsoft SQL Server	6
ONTAP Privileges mínimo necessário para plug-in SQL	8
Preparar sistemas de storage para replicação SnapMirror e SnapVault para plug-in para SQL Server ..	12
Estratégia de backup para recursos do SQL Server	13
Estratégia de restauração para SQL Server	17
Defina uma estratégia de clonagem para o SQL Server	21
Início rápido para instalar o plug-in do SnapCenter para SQL Server	22
Prepare-se para a instalação	22
Instale o servidor SnapCenter	25
Instale o plug-in para Microsoft SQL Server	26
Prepare-se para instalar o plug-in do SnapCenter para Microsoft SQL Server	27
Fluxo de trabalho de instalação para o plug-in SnapCenter para Microsoft SQL Server	27
Pré-requisitos para adicionar hosts e instalar o plug-in do SnapCenter para Microsoft SQL Server ..	28
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Windows	29
Configure credenciais para o pacote de plug-ins do SnapCenter para Windows	29
Configure credenciais para um recurso do SQL Server individual	31
Configure o gMSA no Windows Server 2012 ou posterior	34
Instale o plug-in do SnapCenter para Microsoft SQL Server	35
Configure certificado CA	41
Configure a recuperação de desastres	44
Instale o plug-in do SnapCenter para VMware vSphere	47
Implantar certificado CA	47
Configure o arquivo CRL	47
Prepare-se para a proteção de dados	47
Pré-requisitos para usar o plug-in do SnapCenter para Microsoft SQL Server	47
Como recursos, grupos de recursos e políticas são usados para proteger o SQL Server	48
Faça backup do banco de dados do SQL Server, instância ou grupo de disponibilidade	49
Fluxo de trabalho de backup	49
Determine se os recursos estão disponíveis para backup	50
Migrar recursos para o sistema de storage NetApp	52
Criar políticas de backup para bancos de dados do SQL Server	54
Crie grupos de recursos e anexe políticas para o SQL Server	61
Requisitos para fazer backup de recursos SQL	64
Faça backup de recursos SQL	65
Fazer backup de grupos de recursos do SQL Server	67

Monitorar operações de backup	68
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell ..	70
Faça backup de recursos usando cmdlets do PowerShell	71
Cancele o plug-in do SnapCenter para operações de backup do Microsoft SQL Server	73
Veja os backups e clones do SQL Server na página topologia	74
Remova backups usando cmdlets do PowerShell	75
Limpe a contagem de backup secundária usando cmdlets do PowerShell	75
Restaurar recursos do SQL Server	76
Restoure o fluxo de trabalho	76
Requisitos para restaurar um banco de dados	77
Restoure backups de banco de dados do SQL Server	78
Restoure um banco de dados SQL Server a partir do armazenamento secundário	82
Reseed Availability Group Databases	83
Restoure recursos usando cmdlets do PowerShell	84
Monitorar operações de restauração de recursos SQL	86
Cancelar operações de restauração de recursos SQL	87
Clonar recursos de banco de dados do SQL Server	88
Fluxo de trabalho clone	88
Clone de um backup de banco de dados do SQL Server	89
Clonar backups usando cmdlets do PowerShell	92
Execute o ciclo de vida do clone	96
Monitorar operações de clone de banco de dados SQL	98
Cancelar operações de clone de recursos SQL	99
Divida um clone	100

Proteja bancos de dados Microsoft SQL Server

Plug-in do SnapCenter para Microsoft SQL Server

Visão geral do plug-in do SnapCenter para Microsoft SQL Server

O plug-in do SnapCenter para Microsoft SQL Server é um componente do lado do host do software NetApp SnapCenter que permite o gerenciamento de proteção de dados com reconhecimento de aplicativos de bancos de dados do Microsoft SQL Server. O plug-in para SQL Server automatiza as operações de backup, verificação, restauração e clone de banco de dados do SQL Server em seu ambiente SnapCenter.

Quando o plug-in para SQL Server é instalado, você pode usar o SnapCenter com a tecnologia NetApp SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia NetApp SnapVault para executar replicação de backup de disco para disco para fins de conformidade ou arquivamento de padrões.

O que você pode fazer com o plug-in SnapCenter para Microsoft SQL Server

Quando o plug-in do SnapCenter for instalado no seu ambiente, você pode usar o SnapCenter para fazer backup, restaurar e clonar bancos de dados do SQL Server.

Você pode executar as seguintes tarefas que dão suporte a operações de backup, operações de restauração e operações de clone de bancos de dados e recursos de banco de dados do SQL Server:

- Faça backup de bancos de dados do SQL Server e logs de transações associados

Não é possível criar um backup de log para bancos de dados de sistema mestre e msdb. No entanto, você pode criar backups de log para o banco de dados do sistema modelo.

- Restaure os recursos do banco de dados
 - Você pode restaurar bancos de dados do sistema mestre, bancos de dados do sistema msdb e bancos de dados do sistema modelo.
 - Não é possível restaurar vários bancos de dados, instâncias e grupos de disponibilidade.
 - Não é possível restaurar o banco de dados do sistema para um caminho alternativo.
- Criar clones pontuais de bancos de dados de produção

Não é possível executar operações de backup, restauração, clone e clone do ciclo de vida em bancos de dados do sistema tempdb.

- Verifique as operações de backup imediatamente ou adie a verificação até mais tarde

A verificação do banco de dados do sistema do SQL Server não é suportada. O SnapCenter clones os bancos de dados para executar a operação de verificação. O SnapCenter não pode clonar bancos de dados do sistema do SQL Server e, portanto, a verificação desses bancos de dados não é suportada.

- Programe operações de backup e operações de clone
- Monitore operações de backup, operações de restauração e operações de clone



O Plug-in para SQL Server não suporta backup e recuperação de bancos de dados SQL Server em compartilhamentos SMB.

Plug-in do SnapCenter para recursos do Microsoft SQL Server

O plug-in para SQL Server é integrado ao Microsoft SQL Server no host do Windows e com a tecnologia de cópia Snapshot do NetApp no sistema de storage. Para trabalhar com o plug-in para SQL Server, use a interface do SnapCenter.

O Plug-in para SQL Server inclui estes principais recursos:

- * Interface gráfica unificada do usuário com SnapCenter*

A interface do SnapCenter fornece padronização e consistência entre plug-ins e ambientes. A interface do SnapCenter permite concluir processos consistentes de backup e restauração em plug-ins, usar relatórios centralizados, usar visualizações de dashboard rápidas, configurar controle de acesso baseado em funções (RBAC) e monitorar tarefas em todos os plug-ins. O SnapCenter também oferece gerenciamento centralizado de políticas e agendamento para dar suporte a operações de backup e clone.

- * Administração central automatizada*

Você pode agendar backups de rotina do SQL Server, configurar a retenção de backup baseada em políticas e configurar operações de restauração pontuais e atualizadas. Você também pode monitorar proativamente seu ambiente SQL Server configurando o SnapCenter para enviar alertas de e-mail.

- **Tecnologia de cópia Snapshot NetApp sem interrupções**

O plug-in para SQL Server usa a tecnologia de cópia Snapshot do NetApp com o plug-in do NetApp SnapCenter para Microsoft Windows. Isso permite que você faça backup de bancos de dados em segundos e restaurá-los rapidamente sem deixar o SQL Server offline. As cópias Snapshot consomem espaço mínimo de storage.

Além desses principais recursos, o Plug-in para SQL Server oferece os seguintes benefícios:

- Suporte ao fluxo de trabalho de backup, restauração, clone e verificação
- Delegação de funções centralizada e segurança compatível com RBAC
- Criação de cópias pontuais e com uso eficiente de espaço de bancos de dados de produção para teste ou extração de dados usando a tecnologia NetApp FlexClone

É necessária uma licença FlexClone no sistema de storage que mantém o clone.

- Verificação de backup sem interrupções e automatizada
- Capacidade de executar vários backups ao mesmo tempo em vários servidores
- Cmdlets do PowerShell para scripts de operações de backup, verificação, restauração e clone
- Suporte para AlwaysOn Availability Groups (AGS) no SQL Server para acelerar as operações de configuração, backup e restauração AG
- Banco de dados in-memory e Buffer Pool Extension (BPE) como parte do SQL Server 2014
- Suporte para backup de LUNs e discos de máquina virtual (VMDKs)
- Suporte para infraestruturas físicas e virtualizadas

- Suporte para iSCSI, Fibre Channel, FCoE, mapeamento de dispositivos brutos (RDM) e VMDK em NFS e VMFS



Os volumes nas devem ter uma política de exportação padrão na máquina virtual de storage (SVM).

- Suporte para FileStream e grupo de arquivos em bancos de dados autônomos do SQL Server.

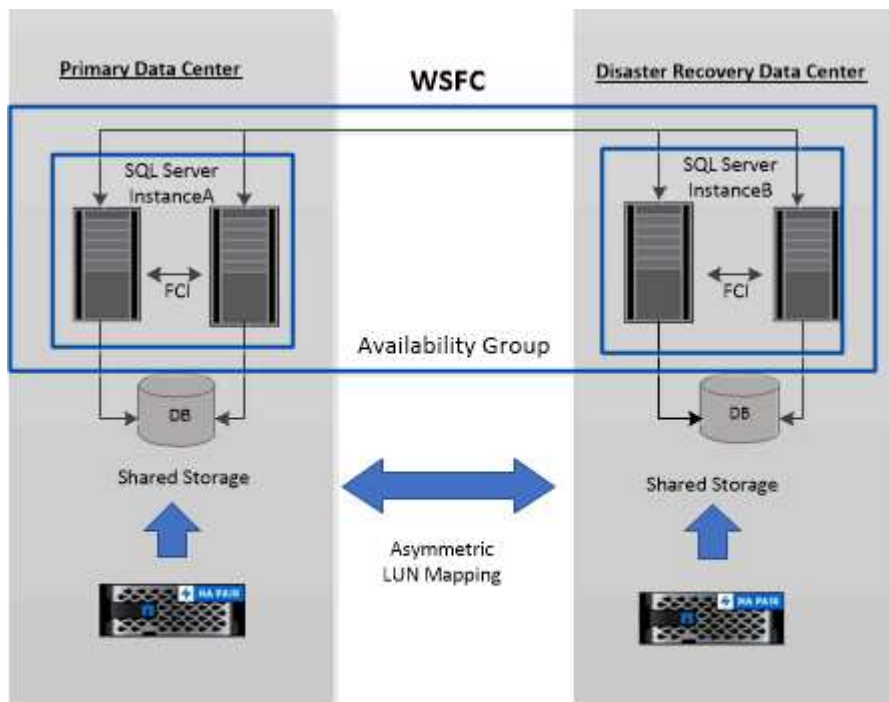
Suporte para mapeamento LUN assimétrico em clusters Windows

O plug-in do SnapCenter para Microsoft SQL Server suporta a descoberta no SQL Server 2012 e posterior, configurações de mapeamento LUN assimétrico (ALM) para alta disponibilidade e grupos de disponibilidade para recuperação de desastres. Ao descobrir recursos, o SnapCenter descobre bancos de dados em hosts locais e em hosts remotos em configurações ALM.

Uma configuração ALM é um único cluster de failover de servidor Windows que contém um ou mais nós em um data center primário e um ou mais nós em um centro de recuperação de desastres.

Segue-se um exemplo de uma configuração ALM:

- Duas instâncias de cluster de failover (FCI) em um data center de vários locais
- FCI para alta disponibilidade local (HA) e Availability Group (AG) para recuperação de desastres com uma instância autônoma no local de recuperação de desastres



WSFC—Windows Server Failover Cluster

O storage no data center principal é compartilhado entre os nós de FCI presentes no data center principal. O storage no data center de recuperação de desastres é compartilhado entre os nós FCI presentes no data center de recuperação de desastres.

O storage no data center principal não é visível para os nós no data center de recuperação de desastres e vice-versa.



A arquitetura DO ALM combina duas soluções de storage compartilhado usadas pelo FCI, com uma solução de storage não compartilhada ou dedicada usada pelo SQL AG. A solução AG usa letras de unidade idênticas para recursos de disco compartilhados entre data centers. Esse arranjo de storage, em que um disco de cluster é compartilhado entre um subconjunto de nós dentro de um WSFC, é conhecido como ALM.


Tipos de storage compatíveis com plug-ins do SnapCenter para Microsoft Windows e Microsoft SQL Server

O SnapCenter suporta uma ampla variedade de tipos de armazenamento em máquinas físicas e máquinas virtuais. Você deve verificar se há suporte disponível para o seu tipo de armazenamento antes de instalar o pacote para o seu host.

O suporte para provisionamento e proteção de dados do SnapCenter está disponível no Windows Server. Para obter as informações mais recentes sobre versões suportadas, consulte o ["Ferramenta de Matriz de interoperabilidade do NetApp"](#).

Máquina	Tipo de armazenamento	Provisione usando	Notas de suporte
Servidor físico	LUNs conectados a FC	Cmdlets da interface gráfica do usuário (GUI) do SnapCenter ou do PowerShell	
Servidor físico	LUNs ligados ao iSCSI	Cmdlets SnapCenter GUI ou PowerShell	
Servidor físico	Compartilhamentos de SMB3 TB (CIFS) residentes em uma máquina virtual de storage (SVM)	Cmdlets SnapCenter GUI ou PowerShell	Suporte apenas para provisionamento. Não é possível usar o SnapCenter para fazer backup de dados ou compartilhamentos usando o protocolo SMB.
VMware VM	LUNs RDM ligados por um FC ou iSCSI HBA	Cmdlets do PowerShell	
VMware VM	iSCSI LUNs ligados diretamente ao sistema convidado pelo iniciador iSCSI	Cmdlets SnapCenter GUI ou PowerShell	
VMware VM	Armazenamentos de dados NFS ou VMFS (Virtual Machine File Systems)	VMware vSphere	

Máquina	Tipo de armazenamento	Provisione usando	Notas de suporte
VMware VM	Um sistema convidado conectado a SMB3 compartilhamentos residentes em um SVM	Cmdlets SnapCenter GUI ou PowerShell	<p>Suporte apenas para provisionamento.</p> <p>Não é possível usar o SnapCenter para fazer backup de dados ou compartilhamentos usando o protocolo SMB.</p>
VM Hyper-V	LUNs de FC virtual (VFC) conectados por um switch Fibre Channel virtual	Cmdlets SnapCenter GUI ou PowerShell	<p>Você deve usar o Hyper-V Manager para provisionar LUNs Virtual FC (VFC) conectados por um switch Fibre Channel virtual.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>O Hyper-V passa por discos e faz backup de bancos de dados em VHD(x) que são provisionados no armazenamento NetApp não são suportados.</p> </div>
VM Hyper-V	iSCSI LUNs ligados diretamente ao sistema convidado pelo iniciador iSCSI	Cmdlets SnapCenter GUI ou PowerShell	<div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>O Hyper-V passa por discos e faz backup de bancos de dados em VHD(x) que são provisionados no armazenamento NetApp não são suportados.</p> </div>

Máquina	Tipo de armazenamento	Provisione usando	Notas de suporte
VM Hyper-V	Um sistema convidado conectado a SMB3 compartilhamentos residentes em um SVM	Cmdlets SnapCenter GUI ou PowerShell	<p>Suporte apenas para provisionamento.</p> <p>Não é possível usar o SnapCenter para fazer backup de dados ou compartilhamentos usando o protocolo SMB.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;">  <p>O Hyper-V passa por discos e faz backup de bancos de dados em VHD(x) que são provisionados no armazenamento NetApp não são suportados.</p> </div>

Recomendações de layout de storage para o plug-in SnapCenter para Microsoft SQL Server

Um layout de armazenamento bem projetado permite que o servidor SnapCenter faça backup de seus bancos de dados para atender aos seus objetivos de recuperação. Você deve considerar vários fatores ao definir seu layout de armazenamento, incluindo o tamanho do banco de dados, a taxa de alteração do banco de dados e a frequência com que você realiza backups.

As seções a seguir definem as recomendações e restrições de layout de storage para LUNs e discos de máquina virtual (VMDKs) com o plug-in SnapCenter para Microsoft SQL Server instalado no seu ambiente.

Nesse caso, os LUNs podem incluir discos VMware RDM e LUNs iSCSI de conexão direta mapeados para o convidado.

Requisitos de LUN e VMDK

Opcionalmente, você pode usar LUNs ou VMDKs dedicados para obter performance e gerenciamento ideais para os seguintes bancos de dados:

- Bancos de dados de sistemas mestres e de modelos
- Tempdb
- Arquivos de banco de dados do usuário (.mdf e .ndf)

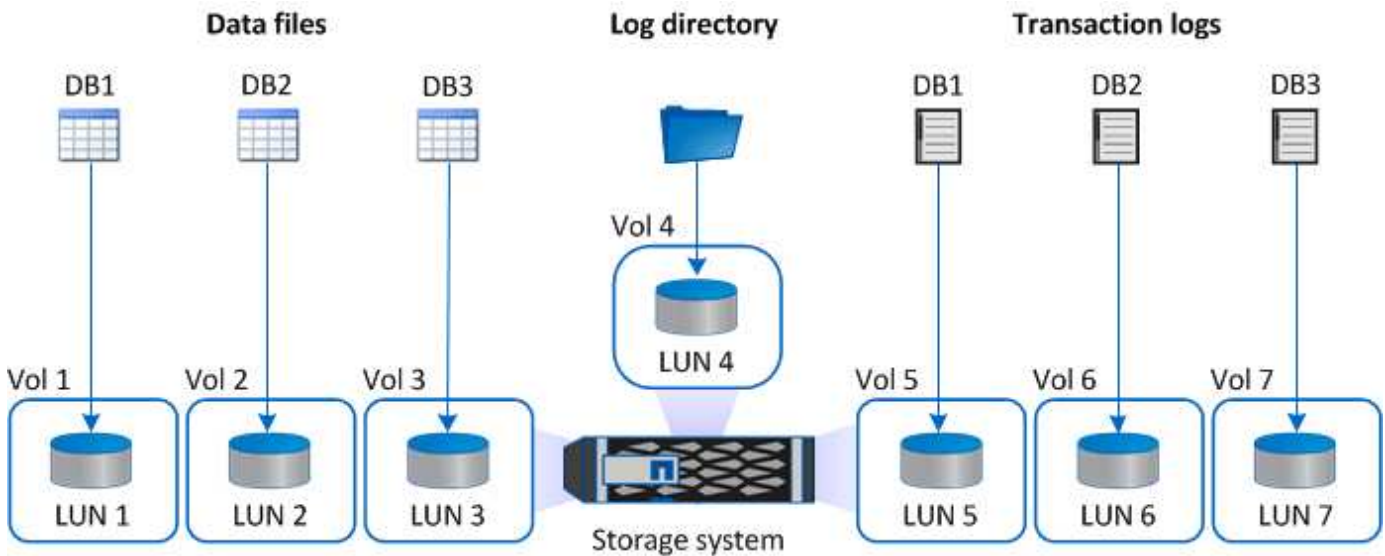
- Arquivos de log de transações de banco de dados do usuário (.ldf)
- Diretório de log

Para restaurar bancos de dados grandes, a prática recomendada é usar LUNs ou VMDKs dedicados. O tempo necessário para restaurar um LUN ou VMDK completo é menor do que o tempo necessário para restaurar os arquivos individuais que são armazenados no LUN ou VMDK.

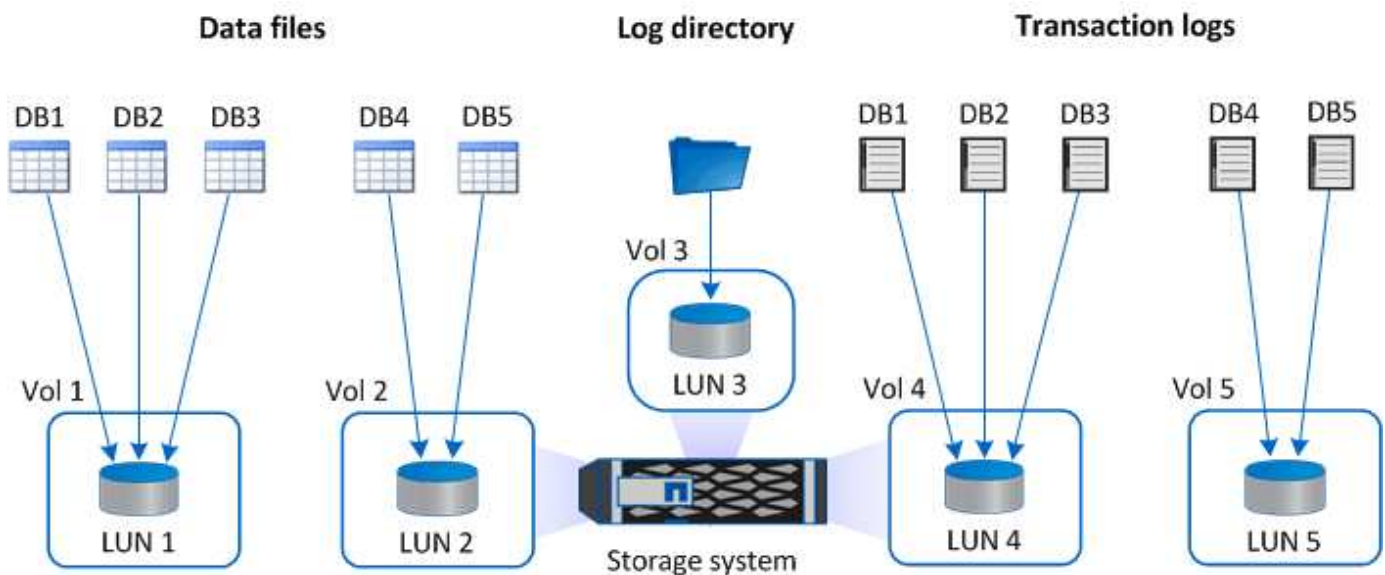
Para o diretório de log, você deve criar um LUN ou VMDK separado para que haja espaço livre suficiente nos discos de arquivo de dados ou log.

Layouts de amostra de LUN e VMDK

O gráfico a seguir mostra como você pode configurar o layout de armazenamento para bancos de dados grandes em LUNs:

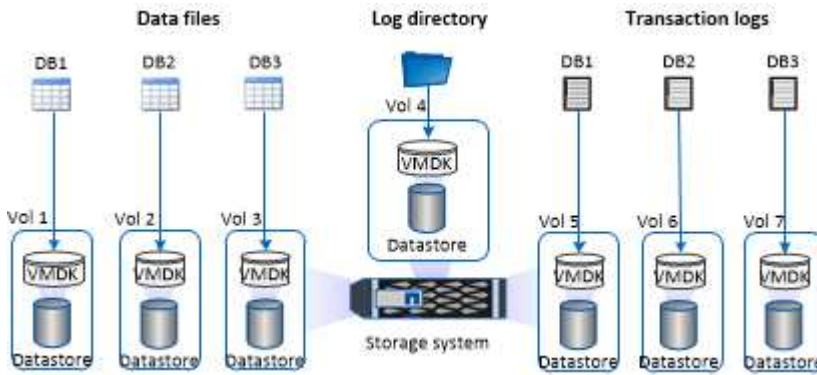


O gráfico a seguir mostra como você pode configurar o layout de armazenamento para bancos de dados médios ou pequenos em LUNs:

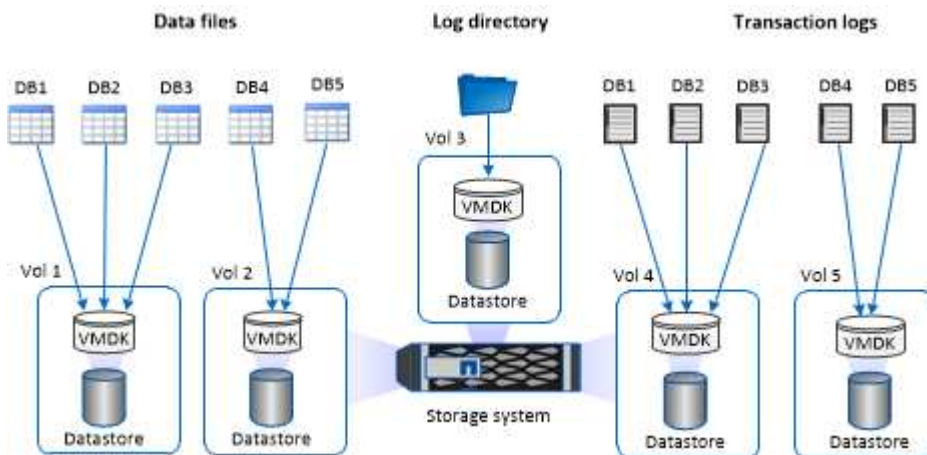


O gráfico a seguir mostra como você pode configurar o layout de armazenamento para bancos de dados

grandes em VMDKs:



O gráfico a seguir mostra como você pode configurar o layout de armazenamento para bancos de dados médios ou pequenos em VMDKs:



ONTAP Privileges mínimo necessário para plug-in SQL

Os ONTAP Privileges mínimos necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
event generate-AutoSupport-log
mostra o histórico de trabalhos
paragem do trabalho

Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior

lun

lun criar

eliminação lun

lun igrop add

lun igrop criar

eliminação do agrupamento lun

mudar o nome do grupo lun

show de grupos de lun

nós complementares de mapeamento de lun

mapeamento lun criar

eliminação do mapeamento lun

mapeamento lun remove-reporting-nonos

mostra de mapeamento lun

modificação de lun

movimentação de lun no volume

lun offline

lun online

redimensionar lun

série lun

mostra lun

Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior

regra adicional de política do SnapMirror

regra de modificação de política do SnapMirror

regra de remoção da política do SnapMirror

SnapMirror policy show

restauração de SnapMirror

SnapMirror show

SnapMirror show-history

atualização do SnapMirror

SnapMirror update-ls-set

SnapMirror lista-destinos

versão

Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior

clone de volume criar

show de clone de volume

início da divisão do clone de volume

paragem dividida clone volume

criar volume

destruição de volume

clone de arquivo de volume criar

show-disk-use do arquivo de volume

volume off-line

volume online

modificação do volume

criar qtree de volume

eliminação de qtree de volume

modificação de qtree de volume

apresentação de qtree de volume

restrição de volume

apresentação do volume

criar instantâneo de volume

eliminar instantâneo do volume

modificação do instantâneo do volume

mudar o nome do instantâneo do volume

restauração de snapshot de volume

restauração de arquivo de snapshot de volume

apresentação de instantâneo do volume

desmontar o volume

Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior

svm cifs

compartilhamento cifs de svm criar

exclusão de compartilhamento cifs de svm

apresentação do shadowcopy cifs de svm

exibição de compartilhamento cifs de svm

mostra cifs de svm

política de exportação de svm

criação de política de exportação de svm

exclusão da política de exportação do svm

regra de política de exportação de svm criar

a regra de política de exportação do svm é exibida

exibição da política de exportação do svm

svm iscsi

apresentação da ligação iscsi de svm

mostra o svm

interface de rede

mostra da interface de rede

svm

MetroCluster show

Preparar sistemas de storage para replicação SnapMirror e SnapVault para plug-in para SQL Server

Você pode usar um plug-in do SnapCenter com a tecnologia ONTAP SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia ONTAP SnapVault para executar replicação de backup disco a disco para conformidade com os padrões e outros fins relacionados à governança. Antes de executar essas tarefas, você deve configurar uma relação de proteção de dados entre os volumes de origem e destino e inicializar a relação.

O SnapCenter executa as atualizações para o SnapMirror e o SnapVault após concluir a operação de cópia Snapshot. As atualizações SnapMirror e SnapVault são executadas como parte da tarefa SnapCenter; não crie uma agenda ONTAP separada.



Se você estiver vindo para o SnapCenter de um produto NetApp SnapManager e estiver satisfeito com as relações de proteção de dados que configurou, ignore esta seção.

Uma relação de proteção de dados replica dados no storage primário (o volume de origem) para o storage secundário (o volume de destino). Ao inicializar a relação, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.



O SnapCenter não suporta relações em cascata entre volumes SnapMirror e SnapVault (**Primary > Mirror > Vault**). Você deve usar relacionamentos de fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis de versão e como configurá-los, consulte "[Documentação do ONTAP](#)".



O SnapCenter não suporta replicação **Sync_mirror**.

Estratégia de backup para recursos do SQL Server

Defina uma estratégia de backup para recursos do SQL Server

Definir uma estratégia de backup antes de criar seus trabalhos de backup ajuda a garantir que você tenha os backups necessários para restaurar ou clonar seus bancos de dados com êxito. Seu Contrato de nível de serviço (SLA), objetivo de tempo de recuperação (rto) e objetivo do ponto de restauração (RPO) determinam em grande parte a sua estratégia de backup.

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. O rto é o momento em que um processo de negócios deve ser restaurado após uma interrupção no serviço. Um RPO define a estratégia para a era dos arquivos que precisam ser recuperados do storage de backup para que as operações regulares sejam retomadas após uma falha. O SLA, rto e RPO contribuem para a estratégia de backup.

Tipos de backups suportados

O backup de bancos de dados do sistema e do usuário do SQL Server usando o SnapCenter exige que você escolha o tipo de recurso, como bancos de dados, instâncias do SQL Server e grupos de disponibilidade (AG). A tecnologia de cópia Snapshot é utilizada para criar cópias on-line e somente leitura dos volumes nos quais os recursos residem.

Você pode selecionar a opção somente cópia para especificar que o SQL Server não trunca os logs de transação. Você deve usar essa opção quando também estiver gerenciando o SQL Server com outros aplicativos de backup. Manter os logs de transação intactos permite que qualquer aplicativo de backup restaure os bancos de dados do sistema. Os backups somente de cópia são independentes da sequência de backups programados e não afetam os procedimentos de backup e restauração do banco de dados.

Tipo de cópia de segurança	Descrição	Opção somente cópia com tipo de backup
Backup completo e backup de log	<p>Faz backup do banco de dados do sistema e trunca os logs de transação.</p> <p>O SQL Server trunca os logs de transação removendo as entradas que já estão comprometidas com o banco de dados.</p> <p>Após a conclusão do backup completo, essa opção cria um log de transações que captura informações de transação. Normalmente, você deve escolher essa opção. No entanto, se o tempo de backup for curto, você pode optar por não executar um backup de log de transações com backup completo.</p> <p>Não é possível criar um backup de log para bancos de dados de sistema mestre e msdb. No entanto, você pode criar backups de log para o banco de dados do sistema modelo.</p>	<p>Faz backup dos arquivos do banco de dados do sistema e dos logs de transação sem truncar os logs.</p> <p>Um backup só de cópia não pode servir como uma base diferencial ou backup diferencial e não afeta a base diferencial. Restaurar um backup completo somente de cópia é o mesmo que restaurar qualquer outro backup completo.</p>
Backup completo do banco de dados	<p>Faz cópias de segurança dos arquivos da base de dados do sistema.</p> <p>Você pode criar backup completo do banco de dados para bancos de dados de sistema master, model e msdb.</p>	<p>Faz cópias de segurança dos arquivos da base de dados do sistema.</p>
Backup do log de transações	<p>Faz o backup dos logs de transação truncados, copiando apenas as transações que foram confirmadas desde o backup do log de transação mais recente.</p> <p>Se você agendar backups frequentes de log de transações juntamente com backups completos de bancos de dados, poderá escolher pontos de recuperação granular.</p>	<p>Faz backup dos logs de transação sem truncar-los.</p> <p>Este tipo de cópia de segurança não afeta a sequência de cópias de segurança de registros regulares. Backups de log somente de cópia são úteis para executar operações de restauração on-line.</p>

Agendamentos de backup para Plug-in para servidor SQL

A frequência de backup (tipo de agendamento) é especificada em políticas; uma programação de backup é especificada na configuração do grupo de recursos. O fator mais crítico na determinação de uma frequência ou programação de backup é a taxa de alteração do recurso e a importância dos dados. Você pode fazer backup de um recurso muito usado a cada hora, enquanto você pode fazer backup de um recurso raramente usado uma vez por dia. Outros fatores incluem a importância do recurso para a sua organização, seu Contrato de nível de Serviço (SLA) e seu objetivo de ponto de recuperação (RPO).

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. Um RPO define a estratégia para a era dos arquivos que precisam ser recuperados do storage de backup para que as operações regulares sejam retomadas após uma falha. O SLA e o RPO contribuem para a estratégia de proteção de dados.

Mesmo para um recurso muito usado, não é necessário executar um backup completo mais de uma ou duas vezes por dia. Por exemplo, backups regulares de log de transações podem ser suficientes para garantir que você tenha os backups necessários. Quanto mais você fizer backup de seus bancos de dados, menos Registros de transações que o SnapCenter precisa usar no momento da restauração, o que pode resultar em operações de restauração mais rápidas.

Os programas de backup têm duas partes, como segue:

- Frequência de backup

A frequência de backup (com que frequência os backups devem ser executados), chamada *schedule type* para alguns plug-ins, faz parte de uma configuração de política. Você pode selecionar a frequência de backup da política por hora, dia, semanal ou mensal. Se você não selecionar nenhuma dessas frequências, a política criada será uma política somente sob demanda. Você pode acessar políticas clicando em **Configurações > políticas**.

- Fazer backup de programações

As agendas de backup (exatamente quando os backups devem ser executados) fazem parte de uma configuração de grupo de recursos. Por exemplo, se você tiver um grupo de recursos que tenha uma política configurada para backups semanais, poderá configurar a programação para fazer backup todas as quintas-feiras às 10:00 horas. Você pode acessar programações de grupos de recursos clicando em **recursos > grupos de recursos**.

Número de trabalhos de backup necessários para bancos de dados

Os fatores que determinam o número de tarefas de backup de que você precisa incluem o tamanho do banco de dados, o número de volumes usados, a taxa de alteração do banco de dados e seu Contrato de nível de Serviço (SLA).

Para backups de bancos de dados, o número de tarefas de backup que você escolhe geralmente depende do número de volumes nos quais você colocou seus bancos de dados. Por exemplo, se você colocou um grupo de bancos de dados pequenos em um volume e um banco de dados grande em outro volume, você pode criar um trabalho de backup para os bancos de dados pequenos e um trabalho de backup para o banco de dados grande.

Convenções de nomenclatura de backup para Plug-in para SQL Server

Você pode usar a convenção de nomenclatura de cópia Snapshot padrão ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um carimbo de data/hora aos nomes de cópia Snapshot que o ajuda a identificar quando as cópias foram criadas.

A cópia Snapshot usa a seguinte convenção de nomenclatura padrão:

```
resourcegroupname_hostname_timestamp
```

Você deve nomear seus grupos de recursos de backup logicamente, como no exemplo a seguir:

```
dts1_mach1x88_03-12-2015_23.17.26
```

Neste exemplo, os elementos de sintaxe têm os seguintes significados:

- *dts1* é o nome do grupo de recursos.
- *mach1x88* é o nome do host.
- *03-12-2015_23.17.26* é a data e o carimbo de data/hora.

Como alternativa, você pode especificar o formato do nome da cópia Snapshot enquanto protege recursos ou grupos de recursos selecionando **usar formato de nome personalizado para cópia Snapshot**. Por exemplo, `customtext_resourcegroup_policy_hostname` ou `resourcegroup_hostname`. Por padrão, o sufixo do carimbo de hora é adicionado ao nome da cópia Instantânea.

Opções de retenção de backup para Plug-in para SQL Server

Você pode escolher o número de dias para os quais reter cópias de backup ou especificar o número de cópias de backup que deseja reter, até um máximo de ONTAP de 255 cópias. Por exemplo, sua organização pode exigir que você retenha 10 dias de cópias de backup ou 130 cópias de backup.

Ao criar uma política, você pode especificar as opções de retenção para o tipo de backup e o tipo de agendamento.

Se você configurar a replicação do SnapMirror, a política de retenção será espelhada no volume de destino.

O SnapCenter exclui os backups retidos que têm rótulos de retenção que correspondem ao tipo de agendamento. Se o tipo de agendamento tiver sido alterado para o grupo de recursos ou recursos, os backups com o rótulo de tipo de agendamento antigo ainda poderão permanecer no sistema.



Para retenção de longo prazo de cópias de backup, você deve usar o backup SnapVault.

Quanto tempo para reter backups de log de transações no sistema de armazenamento de origem

O plug-in do SnapCenter para Microsoft SQL Server precisa de backups de log de transações para executar operações de restauração atualizadas, que restauram seu banco de dados para um tempo entre dois backups completos.

Por exemplo, se o Plug-in para SQL Server fez um backup completo às 8:00 da manhã e outro backup completo às 5:00 da tarde, ele poderia usar o backup de log de transações mais recente para restaurar o banco de dados a qualquer momento entre as 8:00 da manhã e as 5:00 da tarde se os logs de transação não estiverem disponíveis, o Plug-in para SQL Server pode executar operações de restauração pontual apenas, que restauram um banco de dados para o momento em que o backup completo.

Normalmente, você precisa de operações de restauração mais atualizadas por apenas um dia ou dois. Por padrão, o SnapCenter mantém um mínimo de dois dias.

Vários bancos de dados no mesmo volume

Você pode colocar todos os bancos de dados no mesmo volume, porque a política de backup tem uma opção para definir o máximo de bancos de dados por backup (o valor padrão é 100).

Por exemplo, se você tiver 200 bancos de dados no mesmo volume, duas cópias Snapshot serão criadas com 100 bancos de dados em cada uma das duas cópias Snapshot.

Verificação de cópia de backup usando o volume de storage primário ou secundário para Plug-in para SQL Server

É possível verificar cópias de backup no volume de storage primário ou no volume de storage secundário SnapMirror ou SnapVault. A verificação usando um volume de storage secundário reduz a carga no volume de storage primário.

Quando você verifica um backup no volume de storage primário ou secundário, todas as cópias Snapshot primário e secundário são marcadas como verificadas.

A licença SnapRestore é necessária para verificar cópias de backup no volume de storage secundário SnapMirror e SnapVault.

Quando agendar trabalhos de verificação

Embora o SnapCenter possa verificar os backups imediatamente após a criação, isso pode aumentar significativamente o tempo necessário para concluir a tarefa de backup e usar muitos recursos. Portanto, é quase sempre melhor agendar a verificação em um trabalho separado para um momento posterior. Por exemplo, se você fizer backup de um banco de dados às 5:00 horas por dia, poderá agendar a verificação para ocorrer uma hora depois às 6:00 horas

Pelo mesmo motivo, geralmente não é necessário executar a verificação de backup toda vez que você executar um backup. Realizar a verificação em intervalos regulares, mas menos frequentes, geralmente é suficiente para garantir a integridade do backup. Um único trabalho de verificação pode verificar vários backups ao mesmo tempo.

Estratégia de restauração para SQL Server

Defina uma estratégia de restauração para o SQL Server

Definir uma estratégia de restauração para o SQL Server permite que você restaure seu banco de dados com sucesso.

Fontes e destinos para uma operação de restauração

É possível restaurar um banco de dados SQL Server a partir de uma cópia de backup em um storage primário ou secundário. Você também pode restaurar o banco de dados para diferentes destinos, além de sua localização original, permitindo que você escolha o destino que atende aos seus requisitos.

Fontes para uma operação de restauração

É possível restaurar bancos de dados do storage primário ou secundário.

Destinos para uma operação de restauração

Você pode restaurar bancos de dados para vários destinos:

Destino	Descrição
A localização original	Por padrão, o SnapCenter restaura o banco de dados para o mesmo local na mesma instância do SQL Server.
Um local diferente	Você pode restaurar o banco de dados para um local diferente em qualquer instância do SQL Server dentro do mesmo host.
Local original ou diferente usando nomes de banco de dados diferentes	Você pode restaurar o banco de dados com um nome diferente para qualquer instância do SQL Server no mesmo host onde o backup foi criado.



A restauração para host alternativo em servidores ESX para bancos de dados SQL em VMDKs (datastores NFS e VMFS) não é suportada.

Modelos de recuperação do SQL Server suportados pelo SnapCenter

Modelos de recuperação específicos são atribuídos a cada tipo de banco de dados por padrão. O administrador do banco de dados do SQL Server pode reatribuir cada banco de dados a um modelo de recuperação diferente.

O SnapCenter suporta três tipos de modelos de recuperação de SQL Server:

- Modelo de recuperação simples

Quando você usa o modelo de recuperação simples, não é possível fazer backup dos logs de transação.

- Modelo de recuperação completo

Quando você usa o modelo de recuperação completo, você pode restaurar um banco de dados para seu estado anterior a partir do ponto de falha.

- Modelo de recuperação registrado em massa

Quando você usa o modelo de recuperação registrado em massa, você deve executar manualmente a operação registrada em massa. Você deve executar a operação em massa registrada se o log de transações que contém o Registro de confirmação da operação não tiver sido feito backup antes da restauração. Se a operação registrada em massa inserir 10 milhões de linhas em um banco de dados e o banco de dados falhar antes do backup do log de transação, o banco de dados restaurado não conterá as linhas que foram inseridas pela operação registrada em massa.

Tipos de operações de restauração

Você pode usar o SnapCenter para executar diferentes tipos de operações de restauração em recursos do SQL Server.

- Restaurar mais atualizado
- Restaurar para um ponto anterior no tempo

Você pode restaurar até o minuto ou restaurar para um ponto anterior no tempo nas seguintes situações:

- Restauração a partir do storage secundário SnapMirror ou SnapVault
- Restaurar para caminho alternativo (local)



O SnapCenter não é compatível com SnapRestore baseado em volume.

Restoure até o minuto

Em uma operação de restauração atualizada (selecionada por padrão), os bancos de dados são recuperados até o ponto de falha. O SnapCenter realiza isso executando a seguinte sequência:

1. Faz o backup do último log de transações ativo antes de restaurar o banco de dados.
2. Restaura os bancos de dados do backup completo do banco de dados selecionado.
3. Aplica todos os logs de transação que não foram comprometidos com os bancos de dados (incluindo Registros de transações dos backups desde o momento em que o backup foi criado até o momento mais atual).

Os logs de transações são movidos para frente e aplicados a quaisquer bancos de dados selecionados.

Uma operação de restauração atualizada requer um conjunto contíguo de logs de transações.

Como o SnapCenter não pode restaurar logs de transação de banco de dados SQL Server a partir de arquivos de backup de envio de log (o envio de log permite enviar automaticamente backups de log de transações de um banco de dados primário em uma instância de servidor primário para um ou mais bancos de dados secundários em instâncias de servidor secundário separadas), você não é capaz de executar uma operação de restauração atualizada dos backups de log de transações. Por esse motivo, você deve usar o SnapCenter para fazer backup de seus arquivos de log de transação de banco de dados SQL Server.

Se você não precisar manter a capacidade de restauração atualizada para todos os backups, poderá configurar a retenção de backup de log de transações do sistema por meio das políticas de backup.

Exemplo de uma operação de restauração atualizada

Suponha que você execute o backup do SQL Server todos os dias ao meio-dia, e na quarta-feira às 4:00 horas você precisa restaurar a partir de um backup. Por algum motivo, o backup do meio-dia de quarta-feira

falhou a verificação, então você decide restaurar a partir do backup do meio-dia de terça-feira. Depois disso, se o backup for restaurado, todos os logs de transação são movidos para a frente e aplicados aos bancos de dados restaurados, começando com aqueles que não foram confirmados quando você criou o backup de terça-feira e continuando através do último log de transação escrito na quarta-feira às 4:00 horas (se os logs de transação foram copiados).

Restaurar para um ponto anterior no tempo

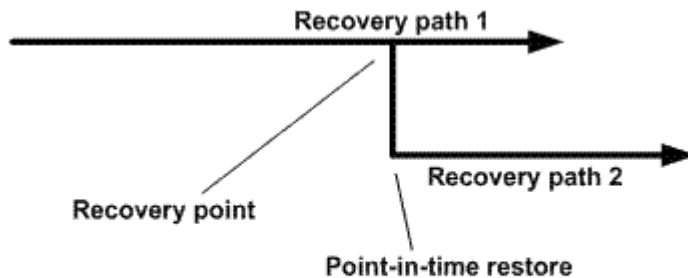
Em uma operação de restauração pontual, os bancos de dados são restaurados apenas para um tempo específico do passado. Uma operação de restauração pontual ocorre nas seguintes situações de restauração:

- O banco de dados é restaurado para um determinado tempo em um log de transação de backup.
- O banco de dados é restaurado e apenas um subconjunto de logs de transações de backup é aplicado a ele.



Restaurar um banco de dados para um ponto no tempo resulta em um novo caminho de recuperação.

A imagem a seguir ilustra os problemas quando uma operação de restauração pontual é executada:



Na imagem, o caminho de recuperação 1 consiste em um backup completo seguido por vários backups de log de transações. Você restaura o banco de dados para um ponto no tempo. Novos backups de log de transações são criados após a operação de restauração pontual, o que resulta no caminho de recuperação 2. Os novos backups de log de transações são criados sem criar um novo backup completo. Devido a corrupção de dados ou outros problemas, você não pode restaurar o banco de dados atual até que um novo backup completo seja criado. Além disso, não é possível aplicar os logs de transação criados no caminho de recuperação 2 ao backup completo pertencente ao caminho de recuperação 1.

Se você aplicar backups de log de transações, você também pode especificar uma data e hora em particular na qual deseja interromper o aplicativo de transações de backup. Para fazer isso, você especifica uma data e hora dentro do intervalo disponível e o SnapCenter remove quaisquer transações que não foram confirmadas antes desse ponto no tempo. Você pode usar esse método para restaurar bancos de dados a um ponto no tempo antes de uma corrupção ocorrer ou para recuperar de um banco de dados acidental ou exclusão de tabela.

Exemplo de uma operação de restauração pontual

Suponha que você faça backups completos do banco de dados uma vez à meia-noite e um backup de log de transações a cada hora. O banco de dados falha às 9:45 da manhã, mas você ainda faz backup dos logs de transação do banco de dados com falha. Você pode escolher entre esses cenários de restauração pontual:

- Restaure o backup completo do banco de dados feito à meia-noite e aceite a perda das alterações feitas posteriormente. (Opção: Nenhuma)
- Restaure o backup completo do banco de dados e aplique todos os backups do log de transações até às 9:45 da manhã (opção: Log até)
- Restaure o backup completo do banco de dados e aplique backups de log de transações, especificando o tempo que você deseja que as transações sejam restauradas a partir do último conjunto de backups de log de transações. (Opção: Por hora específica)

Neste caso, você calcularia a data e a hora em que um determinado erro foi relatado. Quaisquer transações que não tenham sido efetuadas antes da data e hora especificadas são removidas.

Defina uma estratégia de clonagem para o SQL Server

A definição de uma estratégia de clonagem permite clonar seu banco de dados com sucesso.

1. Revise as limitações relacionadas às operações de clone.
2. Decida o tipo de clone que você precisa.

Limitações das operações de clone

Você deve estar ciente das limitações das operações de clone antes de clonar os bancos de dados.

- Se você estiver usando qualquer versão do Oracle de 11.2.0.4 a 12,1.0,1, a operação clone estará no estado suspenso quando você executar o comando *renamedg*. Você pode aplicar o Oracle patch 19544733 para corrigir esse problema.
- A clonagem de bancos de dados de um LUN que está diretamente conectado a um host (por exemplo, usando o Microsoft iSCSI Initiator em um host Windows) para um VMDK ou um LUN RDM no mesmo host Windows, ou outro host Windows, ou vice-versa, não é suportada.
- O diretório raiz do ponto de montagem do volume não pode ser um diretório compartilhado.
- Se você mover um LUN que contém um clone para um novo volume, o clone não poderá ser excluído.

Tipos de operações de clone

Você pode usar o SnapCenter para clonar um backup de banco de dados do SQL Server ou um banco de dados de produção.

- Clonar a partir de um backup de banco de dados

O banco de dados clonado pode servir como uma linha de base para o desenvolvimento de novos aplicativos e ajudar a isolar erros de aplicativos que ocorrem no ambiente de produção. O banco de dados clonado também pode ser usado para recuperação de erros de banco de dados macio.

- Ciclo de vida do clone

Você pode usar o SnapCenter para agendar tarefas de clone recorrentes que ocorrerão quando o banco de dados de produção não estiver ocupado.

Início rápido para instalar o plug-in do SnapCenter para SQL Server

Fornece um conjunto condensado de instruções de instalação para instalar o servidor SnapCenter e o plug-in SnapCenter para Microsoft SQL Server.

Prepare-se para a instalação

Requisitos de domínio e grupo de trabalho

O servidor SnapCenter pode ser instalado em sistemas que estejam em um domínio ou em um grupo de trabalho.


Se você estiver usando um domínio do Active Directory, use um usuário de domínio com direitos de administrador local. O usuário do domínio deve ser membro do grupo Administrador local no host do Windows.

Se estiver a utilizar grupos de trabalho, deve utilizar uma conta local com direitos de administrador local.

Requisitos de licença

O tipo de licenças que você instala depende do seu ambiente.

Licença	Quando necessário
Baseado em controladora padrão da SnapCenter	<p>Necessário para controladores de storage FAS ou AFF</p> <p>A licença padrão da SnapCenter é uma licença baseada em controlador e está incluída como parte do pacote premium. Se você tiver a licença do SnapManager Suite, você também obtém o direito de licença padrão do SnapCenter. Se você quiser instalar o SnapCenter em uma base de avaliação com o storage FAS ou AFF, poderá obter uma licença de avaliação do pacote Premium entrando em Contato com o representante de vendas.</p>
Baseado em capacidade padrão da SnapCenter	<p>Necessário com ONTAP Select e Cloud Volumes ONTAP</p> <p>Se você é um cliente do Cloud Volumes ONTAP ou do ONTAP Select, precisa adquirir uma licença baseada em capacidade por TB com base nos dados gerenciados pelo SnapCenter. Por padrão, o SnapCenter envia uma licença de teste baseada em capacidade padrão SnapCenter de 90 dias e 100 TB incorporada. Para outros detalhes, entre em Contato com o representante de vendas.</p>

Licença	Quando necessário
SnapMirror ou SnapVault	<p>ONTAP</p> <p>A licença SnapMirror ou SnapVault é necessária se a replicação estiver ativada no SnapCenter.</p>
Licenças adicionais (opcional)	"Licenças SnapCenter"Consulte .
Licenças padrão da SnapCenter (opcional)	<p>Destinos secundários</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>É recomendado, mas não obrigatório, que você adicione licenças padrão do SnapCenter a destinos secundários. Se as licenças padrão do SnapCenter não estiverem habilitadas em destinos secundários, você não poderá usar o SnapCenter para fazer backup de recursos no destino secundário após executar uma operação de failover. No entanto, é necessária uma licença FlexClone em destinos secundários para executar operações de clonagem e verificação.</p> </div>

- Requisitos adicionais *

Para obter os requisitos mínimos do ONTAP e do plug-in de aplicativos, consulte ["Ferramenta de Matriz de interoperabilidade"](#)

Hosts	Requisitos mínimos
Sistema operativo (64 bits)	Consulte "Ferramenta de Matriz de interoperabilidade"
CPU	<ul style="list-style-type: none"> • Servidor host: 4 núcleos • Host de plug-in: 1 núcleo
RAM	<ul style="list-style-type: none"> • Servidor anfitrião: 8 GB • Host plug-in: 1 GB

Hosts	Requisitos mínimos
Espaço no disco rígido	<p>Servidor anfitrião:</p> <ul style="list-style-type: none"> • 4 GB para software e logs do servidor SnapCenter • 6 GB para repositório SnapCenter • Cada host de plug-in: 2 GB para instalação de plug-in e logs, isso só é necessário se o plug-in estiver instalado em um host dedicado.
Bibliotecas de terceiros	<p>Necessário no host do servidor SnapCenter e no host de plug-in:</p> <ul style="list-style-type: none"> • Microsoft .NET Framework 4.7.2 ou posterior • Windows Management Framework (WMF) 4,0 ou posterior • PowerShell 4,0 ou posterior
Navegadores	Chrome, Internet Explorer e Microsoft Edge

Tipo de porta	Porta predefinida
Porta SnapCenter	8146 (HTTPS), bidirecional, personalizável, como no URL <i>https://server:8146</i>
Porta de comunicação SnapCenter SMCORE	8145 (HTTPS), bidirecional, personalizável
Banco de dados do repositório	3306 (HTTPS), bidirecional
Hosts de plug-in do Windows	<p>135, 445 (TCP)</p> <p>Além das portas 135 e 445, o intervalo de portas dinâmico especificado pela Microsoft também deve estar aberto. As operações de instalação remota usam o serviço Windows Management Instrumentation (WMI), que procura dinamicamente esse intervalo de portas.</p> <p>Para obter informações sobre o intervalo de portas dinâmico suportado, "Visão geral do serviço e requisitos de porta de rede para Windows" consulte .</p>
Plug-in do SnapCenter para Windows	8145 (HTTPS), bidirecional, personalizável

Tipo de porta	Porta predefinida
Porta de comunicação do cluster ONTAP ou SVM	443 (HTTPS), bidirecional; 80 (HTTP), bidirecional A porta é usada para comunicação entre o host do servidor SnapCenter, o host de plug-in e o SVM ou cluster ONTAP.

Plug-in SnapCenter para requisitos do Microsoft SQL Server

Você deve ter um usuário com Privileges de administrador local com permissões de login local no host remoto. Se você gerenciar nós de cluster, precisará de um usuário com Privileges administrativo para todos os nós do cluster.

Você deve ter um usuário com permissões sysadmin no SQL Server. O plug-in usa o Microsoft VDI Framework, que requer acesso sysadmin.

Instale o servidor SnapCenter

- Baixe e instale o servidor SnapCenter*

Passos

1. Transfira o pacote de instalação do servidor SnapCenter a partir do ["Site de suporte da NetApp"](#) e, em seguida, clique duas vezes no exe.

Depois de iniciar a instalação, todas as pré-verificações são executadas e, se os requisitos mínimos não forem atendidos, as mensagens de erro ou aviso apropriadas serão exibidas. Você pode ignorar as mensagens de aviso e prosseguir com a instalação; no entanto, os erros devem ser corrigidos.

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

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



O caractere especial "%" não é suportado no caminho personalizado para instalação. Se você incluir "%" no caminho, a instalação falhará.

3. Clique em **Instalar agora**.
 - Faça login no SnapCenter*

Passos

1. Inicie o SnapCenter a partir de um atalho na área de trabalho do host ou a partir do URL fornecido pela instalação (<https://server:8146> para a porta padrão 8146 em que o servidor SnapCenter está instalado).
2. Introduza as credenciais.

Para um formato de nome de usuário de administrador de domínio interno, use: `<username>` ou `<username> <username> <domain>` ou `<DomainFQDN>`.

Para um formato de nome de usuário de administrador local integrado, use `<username>`.

3. Clique em **entrar**.

Adicione uma licença baseada em controladora padrão SnapCenter

Passos

1. Faça login no controlador usando a linha de comando ONTAP e digite:

```
system license add -license-code <license_key>
```

2. Verifique a licença:

```
license show
```

Adicione uma licença baseada em capacidade do SnapCenter

Passos

1. No painel esquerdo da GUI do SnapCenter, clique em **Configurações > Software** e, em seguida, na seção Licença, clique em ******.
2. Selecione um dos dois métodos para obter a licença:
 - Introduza as suas credenciais de início de sessão no site de suporte da NetApp para importar licenças.
 - Navegue até a localização do ficheiro de licença do NetApp e clique em **Open**.
3. Na página notificações do assistente, use o limite de capacidade padrão de 90%.
4. Clique em **Finish**.
 - Configurar conexões do sistema de armazenamento*

Passos

1. No painel esquerdo, clique em **istemas de armazenamento > novo**.
2. Na página Adicionar sistema de armazenamento, execute o seguinte:
 - a. Introduza o nome ou endereço IP do sistema de armazenamento.
 - b. Insira as credenciais usadas para acessar o sistema de storage.
 - c. Selecione as caixas de verificação para ativar o sistema de gestão de eventos (EMS) e o AutoSupport.
3. Clique em **mais Opções** se quiser modificar os valores padrão atribuídos à plataforma, protocolo, porta e tempo limite.
4. Clique em **Enviar**.

Instale o plug-in para Microsoft SQL Server

Configurar Executar como credenciais para instalar o plug-in para Microsoft SQL Server

Passos

1. No painel esquerdo, clique em **Definições > credenciais > novo**.
2. Introduza as credenciais.

Para um formato de nome de usuário de administrador de domínio interno, use: *<username>* ou

<username> <username> <domain> ou <DomainFQDN>.

Para um formato de nome de usuário de administrador local integrado, use <username>.

Adicione um host e instale o plug-in para Microsoft SQL Server

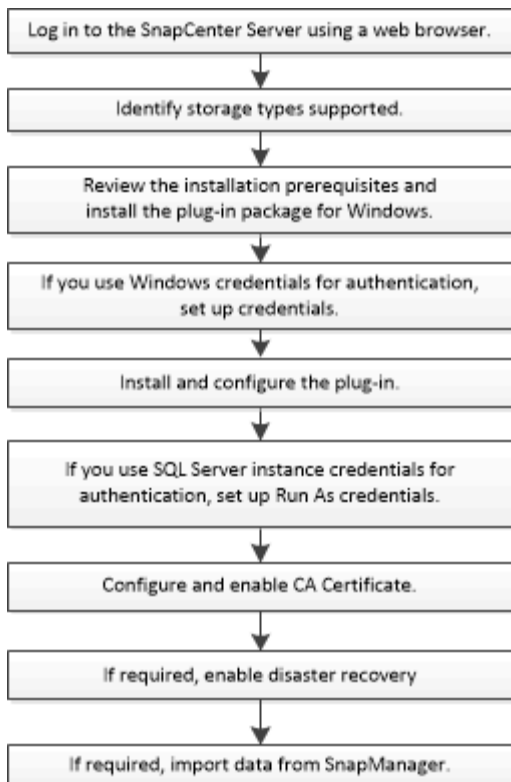
Passos

1. No painel esquerdo da GUI do SnapCenter, clique em **hosts > Managed hosts > Add**.
2. Na página hosts do assistente, execute o seguinte:
 - a. Tipo de host: Selecione o tipo de host do Windows.
 - b. Nome do host: Use o host SQL ou especifique o FQDN de um host dedicado do Windows.
 - c. Credenciais: Selecione o nome da credencial válida do host que você criou ou crie novas credenciais.
3. Na seção Selecionar plug-ins para instalar, selecione **Microsoft SQL Server**.
4. Clique em **mais Opções** para especificar os seguintes detalhes:
 - a. Porta: Guarde o número da porta padrão ou especifique o número da porta.
 - b. Caminho de instalação: O caminho padrão é *C: Arquivos de programas/NetApp/SnapCenter*. Opcionalmente, você pode personalizar o caminho.
 - c. Adicionar todos os hosts no cluster: Marque esta caixa de seleção se estiver usando SQL no WSFC.
 - d. Ignorar verificações de pré-instalação: Marque esta caixa de seleção se você já instalou os plug-ins manualmente ou não deseja validar se o host atende aos requisitos para instalar o plug-in.
5. Clique em **Enviar**.

Prepare-se para instalar o plug-in do SnapCenter para Microsoft SQL Server

Fluxo de trabalho de instalação para o plug-in SnapCenter para Microsoft SQL Server

Você deve instalar e configurar o plug-in do SnapCenter para o Microsoft SQL Server se quiser proteger bancos de dados do SQL Server.



Pré-requisitos para adicionar hosts e instalar o plug-in do SnapCenter para Microsoft SQL Server

Antes de adicionar um host e instalar os pacotes de plug-ins, você deve completar todos os requisitos.

- Se estiver a utilizar iSCSI, o serviço iSCSI tem de estar em execução.
- Você deve ter um usuário com Privileges de administrador local com permissões de login local no host remoto.
- Se você gerenciar nós de cluster no SnapCenter, precisará ter um usuário com Privileges administrativo para todos os nós do cluster.
- Você deve ter um usuário com permissões sysadmin no SQL Server.

O plug-in do SnapCenter para Microsoft SQL Server usa o Microsoft VDI Framework, que requer acesso sysadmin.


["Artigo 2926557: As operações de backup e restauração do SQL Server VDI exigem o sysadmin Privileges"](#)

- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host.
- Se o SnapManager for instalado, você deve ter parado ou desativado o serviço e as programações.
- O host deve ser resolvido para o nome de domínio totalmente qualificado (FQDN) do servidor.

Se o arquivo hosts for modificado para torná-lo resolúvel e se o nome curto e o FQDN forem especificados no arquivo hosts, crie uma entrada no arquivo SnapCenter hosts no seguinte formato: <ip_address> <host_fqdn> <host_name>

Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Windows

Antes de instalar o pacote de plug-ins do SnapCenter para Windows, você deve estar familiarizado com alguns requisitos básicos de espaço do sistema host e requisitos de dimensionamento.

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	5 GB  Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	<ul style="list-style-type: none">• Microsoft .NET Framework 4.7.2 ou posterior• Windows Management Framework (WMF) 4,0 ou posterior• PowerShell 4,0 ou posterior <p>Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".</p> <p>Para obter informações sobre solução de problemas do .NET, "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conectividade com a Internet" consulte .</p>

Configure credenciais para o pacote de plug-ins do SnapCenter para Windows

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter. Você deve criar credenciais para instalar plug-ins do SnapCenter e credenciais adicionais para executar operações de proteção de dados em bancos de dados ou

sistemas de arquivos do Windows.

O que você vai precisar

- Você deve configurar as credenciais do Windows antes de instalar os plug-ins.
- Você deve configurar as credenciais com o Privileges de administrador, incluindo direitos de administrador no host remoto.
- Autenticação SQL em hosts Windows

Você deve configurar credenciais SQL depois de instalar plug-ins.

Se você estiver implantando o plug-in do SnapCenter para o Microsoft SQL Server, deverá configurar credenciais SQL após a instalação dos plug-ins. Configure uma credencial para um usuário com permissões sysadmin do SQL Server.

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

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Clique em **novo**.
4. Na página Credencial (credencial), especifique as informações necessárias para configurar credenciais:

Para este campo...	Faça isso...
Nome da credencial	Introduza um nome para a credencial.

Para este campo...	Faça isso...
Nome de utilizador/Palavra-passe	<p>Introduza o nome de utilizador e a palavra-passe a utilizar para a autenticação.</p> <ul style="list-style-type: none"> Administrador de domínio <p>Especifique o administrador de domínio no sistema no qual você está instalando o plug-in SnapCenter. Os formatos válidos para o campo Nome de usuário são:</p> <ul style="list-style-type: none"> NetBIOS\UserName Domain FQDN\UserName Administrador local (apenas para grupos de trabalho) <p>Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é:</p> <p>UserName</p> <p>Não use aspas duplas (") ou backtick (') nas senhas. Você não deve usar os símbolos menos de (>) e exclamação (!) juntos em senhas. Por exemplo, lessthan!10, lessthan10You!, backtick'12.</p>
Modo de autenticação	<p>Selecione o modo de autenticação que pretende utilizar. Se você selecionar o modo de autenticação SQL, você também deve especificar a instância do servidor SQL e o host onde a instância SQL está localizada.</p>

5. Clique em **OK**.

Depois de concluir a configuração das credenciais, talvez você queira atribuir a manutenção de credenciais a um usuário ou grupo de usuários na página Usuário e Acesso.

Configurar credenciais para um recurso do SQL Server individual

Você pode configurar credenciais para executar tarefas de proteção de dados em recursos individuais do SQL Server para cada usuário. Embora você possa configurar as credenciais globalmente, talvez você queira fazer isso apenas para um recurso

específico.

Sobre esta tarefa

- Se você estiver usando credenciais do Windows para autenticação, você deve configurar sua credencial antes de instalar plug-ins.

No entanto, se você estiver usando uma instância do SQL Server para autenticação, você deve adicionar a credencial após a instalação de plug-ins.

- Se você ativou a autenticação SQL durante a configuração das credenciais, a instância descoberta ou o banco de dados será exibida com um ícone de cadeado de cor vermelha.

Se o ícone de cadeado aparecer, você deve especificar as credenciais da instância ou do banco de dados para adicionar com êxito a instância ou o banco de dados a um grupo de recursos.

- Você deve atribuir a credencial a um usuário de controle de acesso baseado em função (RBAC) sem acesso sysadmin quando as seguintes condições forem atendidas:

- A credencial é atribuída a uma instância SQL.
- A instância ou host SQL é atribuída a um usuário RBAC.



O usuário deve ter o grupo de recursos e o Privileges de backup

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Para adicionar uma nova credencial, clique em **novo**.
4. Na página Credencial (credencial), configure as credenciais:

Para este campo...	Faça isso...
Nome da credencial	Introduza um nome para as credenciais.

Para este campo...	Faça isso...
Nome de usuário	<p>Introduza o nome de utilizador utilizado para a autenticação do SQL Server.</p> <ul style="list-style-type: none"> • O administrador de domínio ou qualquer membro do grupo de administradores especificam o administrador do domínio ou qualquer membro do grupo de administradores no sistema no qual você está instalando o plug-in do SnapCenter. Os formatos válidos para o campo Nome de usuário são: <ul style="list-style-type: none"> ◦ <i>NetBIOS_username</i> ◦ <i>Domain FQDN_username</i> • Administrador local (somente para grupos de trabalho) para sistemas que pertencem a um grupo de trabalho, especifique o administrador local interno no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Username é: <i>Username</i>
Senha	Introduza a palavra-passe utilizada para autenticação.
Modo de autenticação	Selecione o modo de autenticação do SQL Server. Você também pode escolher a autenticação do Windows se o usuário do Windows tiver sysadmin Privileges no servidor SQL.
Anfitrião	Selecione o host.
Instância do SQL Server	Selecione a instância do SQL Server.

5. Clique em **OK** para adicionar a credencial.
6. No painel de navegação esquerdo, clique em **Resources**.
7. Na página recursos, selecione **Instância** na lista **Exibir**.
 - a. Clique  em e selecione o nome do host para filtrar as instâncias.
 - b. Clique  em para fechar o painel de filtro.
8. Na página proteção de instância, proteja a instância e, se necessário, clique em **Configurar credenciais**.

Se o usuário que está conectado ao servidor SnapCenter não tiver acesso ao plug-in do SnapCenter para Microsoft SQL Server, o usuário terá que configurar as credenciais.



A opção credencial não se aplica a bancos de dados e grupos de disponibilidade.

9. Clique em **Atualizar recursos**.

Configure o gMSA no Windows Server 2012 ou posterior

O Windows Server 2012 ou posterior permite criar uma conta de serviço gerenciado de grupo (gMSA) que fornece gerenciamento automatizado de senha de conta de serviço a partir de uma conta de domínio gerenciado.

O que você vai precisar

- Você deve ter um controlador de domínio do Windows Server 2012 ou posterior.
- Você deve ter um host Windows Server 2012 ou posterior, que é um membro do domínio.

Passos

1. Crie uma chave raiz KDS para gerar senhas exclusivas para cada objeto em seu gMSA.
2. Para cada domínio, execute o seguinte comando do controlador de domínio do Windows: Add-KDSRootKey -EffectiveImmediately
3. Crie e configure seu gMSA:
 - a. Crie uma conta de grupo de usuários no seguinte formato:

```
domainName\accountName$  
.. Adicione objetos de computador ao grupo.  
.. Use o grupo de usuários que você acabou de criar para criar o  
gMSA.
```

Por exemplo,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. Execute `Get-ADServiceAccount` o comando para verificar a conta de  
serviço.
```

4. Configure o gMSA em seus hosts:
 - a. Ative o módulo do Active Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

Para fazer isso, execute o seguinte comando do PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. Reinicie o host.
- b. Instale o gMSA em seu host executando o seguinte comando a partir do prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`
- c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`
5. Atribua o Privileges administrativo ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no servidor SnapCenter.

O servidor SnapCenter instalará os plug-ins selecionados no host e o gMSA especificado será usado como a conta de logon de serviço durante a instalação do plug-in.

Instale o plug-in do SnapCenter para Microsoft SQL Server

Adicione hosts e instale o pacote de plug-ins do SnapCenter para Windows

Você deve usar a página SnapCenter **Adicionar host** para adicionar hosts e instalar o pacote de plug-ins. Os plug-ins são instalados automaticamente nos hosts remotos.

O que você vai precisar

- Você deve ser um usuário atribuído a uma função que tenha as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não esteja integrada, desative o UAC no host.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja no estado em execução.
- Se você estiver usando a conta de serviço gerenciado de grupo (gMSA), você deve configurar o gMSA com Privileges administrativo.

["Configurar conta de serviço gerenciado de grupo no Windows Server 2012 ou posterior para SQL"](#)

Sobre esta tarefa

Não é possível adicionar um servidor SnapCenter como um host plug-in a outro servidor SnapCenter.


Você pode adicionar um host e instalar os pacotes de plug-in para um host individual ou para um cluster. Se você estiver instalando os plug-ins em um cluster ou no WSFC (Windows Server failover Clustering), os plug-ins serão instalados em todos os nós do cluster.

Para obter informações sobre como gerenciar hosts, "[Gerenciar hosts](#)" consulte .

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Verifique se a guia **hosts gerenciados** está selecionada na parte superior.
3. Clique em **Add**.
4. Na página hosts, faça o seguinte:


Para este campo...	Faça isso...
Tipo de host	<p>Selecione Windows como o tipo de host. O servidor SnapCenter adiciona o host e, em seguida, instala o plug-in para Windows se o plug-in ainda não estiver instalado no host.</p> <p>Se você selecionar a opção Microsoft SQL Server na página Plug-ins, o servidor SnapCenter instala o plug-in para SQL Server.</p>
Nome do host	<p>Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O endereço IP é suportado para hosts de domínio não confiáveis somente se for resolvido para o FQDN.</p> <p>O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no FQDN.</p> <p>Você pode inserir os endereços IP ou FQDN de um dos seguintes:</p> <ul style="list-style-type: none">• Anfitrião independente• WSFC se você estiver adicionando um host usando o SnapCenter e o host fizer parte de um subdomínio, você deverá fornecer o FQDN.

Para este campo...	Faça isso...
Credenciais	<p>Selecione o nome da credencial que você criou ou crie novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais.</p> <p>Você pode exibir detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você especificou.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar host. </div>

5. Na seção **Select Plug-ins to Install**, selecione os plug-ins a instalar.

6. Clique em **mais opções**.

Para este campo...	Faça isso...
Porta	<p>Guarde o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Se você instalou manualmente os plug-ins e especificou uma porta personalizada, você deve especificar a mesma porta. Caso contrário, a operação falha. </div>
Caminho de instalação	O caminho padrão é C: Arquivos de programas / NetApp / SnapCenter. Opcionalmente, você pode personalizar o caminho.
Adicione todos os hosts no cluster	Marque essa caixa de seleção para adicionar todos os nós de cluster em um WSFC ou um SQL Availability Group. Você deve adicionar todos os nós de cluster selecionando a caixa de seleção de cluster apropriada na GUI se quiser gerenciar e identificar vários grupos de disponibilidade SQL disponíveis em um cluster.
Ignorar as verificações de pré-instalação	Marque essa caixa de seleção se você já instalou os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.

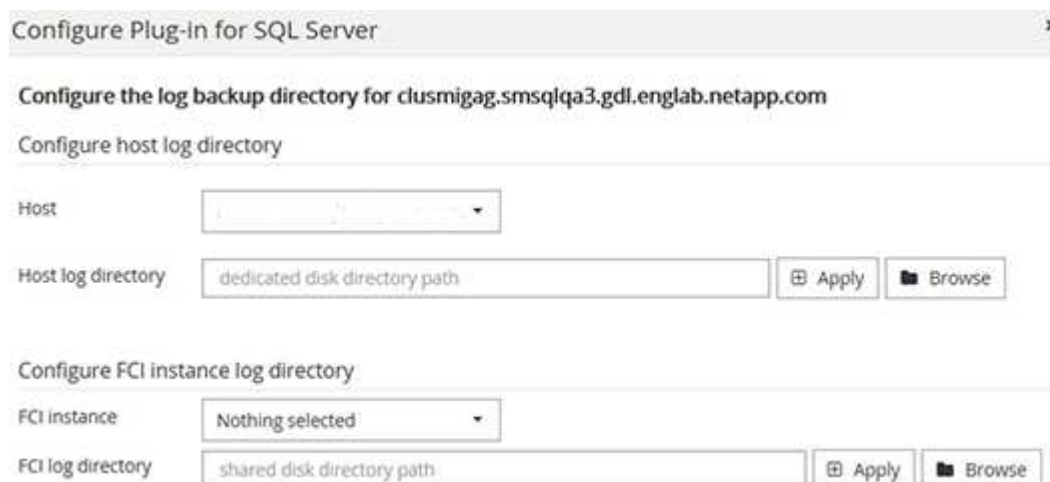
Para este campo...	Faça isso...
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	<p>Marque essa caixa de seleção se quiser usar a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in.</p> <p>Forneça o nome do gMSA no seguinte formato:</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Se o host for adicionado com gMSA e se o gMSA tiver login e sys admin Privileges, o gMSA será usado para se conectar à instância SQL.</p> </div>

7. Clique em **Enviar**.

8. Para o SQL Plug-in, selecione o host para configurar o diretório de log.

- a. Clique em **Configure log Directory** e, na página Configurar diretório de log do host, clique em **Browse** e execute as seguintes etapas:

Apenas os LUNs (unidades) NetApp são listados para seleção. O SnapCenter faz o backup e replica o diretório de log do host como parte da operação de backup.



- i. Selecione a letra da unidade ou ponto de montagem no host onde o log do host será armazenado.
- ii. Escolha um subdiretório, se necessário.
- iii. Clique em **Salvar**.

9. Clique em **Enviar**.

Se você não selecionou a caixa de seleção **Ignorar pré-verificações**, o host será validado para verificar se atende aos requisitos para a instalação do plug-in. O espaço em disco, a RAM, a versão do PowerShell, a versão .NET, a localização (para plug-ins do Windows) e a versão Java (para plug-ins do Linux) são validados de acordo com os requisitos mínimos. Se os requisitos mínimos não forem cumpridos, são apresentadas mensagens de erro ou de aviso adequadas.

Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado no NetApp SnapCenter para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deve corrigir o problema.



Em uma configuração de HA, se você estiver atualizando o arquivo web.config, será necessário atualizar o arquivo em ambos os nós.

10. Monitorize o progresso da instalação.

Instale o plug-in do SnapCenter para Microsoft SQL Server em vários hosts remotos usando cmdlets

Você pode instalar o plug-in do SnapCenter para Microsoft SQL Server em vários hosts simultaneamente usando o cmdlet `Install-SmHostPackage` PowerShell.

O que você vai precisar

Você deve ter feito login no SnapCenter como um usuário de domínio com direitos de administrador local em cada host no qual deseja instalar o pacote de plug-in.

Passos

1. Inicie o PowerShell.
2. No host do servidor SnapCenter, estabeleça uma sessão usando o cmdlet `Open-SmConnection` e insira suas credenciais.
3. Instale o plug-in do SnapCenter para Microsoft SQL Server em vários hosts remotos usando o cmdlet `Install-SmHostPackage` e os parâmetros necessários.

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

Você pode usar a opção `-skipprecheck` quando já tiver instalado os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.

4. Insira suas credenciais para instalação remota.

Instale o plug-in do SnapCenter para Microsoft SQL Server silenciosamente a partir da linha de comando

Você deve instalar o plug-in do SnapCenter para Microsoft SQL Server a partir da interface de usuário do SnapCenter. No entanto, se você não puder por algum motivo, você pode executar o Plug-in para o programa de instalação do SQL Server sem supervisão no modo silencioso a partir da linha de comando do Windows.

O que você vai precisar

- Você deve excluir a versão anterior do plug-in do SnapCenter para Microsoft SQL Server antes de instalar.

Para obter mais informações, ["Como instalar um plug-in do SnapCenter manualmente e diretamente do host do plug-in"](#) consulte .

Passos

1. Valide se a pasta `C: /Temp` existe no host do plug-in e o usuário conectado tem acesso total a ela.
2. Faça o download do plug-in para o software do SQL Server a partir do repositório

C:/ProgramData/NetApp/SnapCenter/Package.

Este caminho é acessível a partir do host onde o servidor SnapCenter está instalado.

3. Copie o arquivo de instalação para o host no qual você deseja instalar o plug-in.
4. Em um prompt de comando do Windows no host local, navegue até o diretório para o qual você salvou os arquivos de instalação do plug-in.
5. Instale o plug-in para o software SQL Server:

```
"snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"  
/log"Log_Path" BI_SNAPCENTER_PORT=Num  
SUITE_INSTALLDIR="Install_Directory_Path"  
BI_SERVICEACCOUNT=domain\\administrator BI_SERVICEPWD=password  
ISFeatureInstall=SCW,SCSQL
```

Substitua os valores do marcador de posição pelos dados

- Debug_Log_Path é o nome e a localização do arquivo de log do instalador do pacote.
- Log_Path é o local dos logs de instalação dos componentes do plug-in (SCW, SCSQL e SMCORE).
- Num é a porta na qual o SnapCenter se comunica com o SMCORE
- Install_Directory_Path é o diretório de instalação do pacote de plug-in do host.
- Domínio/administrador é a conta do serviço Web do SnapCenter Plug-in para Microsoft Windows.
- Senha é a senha para a conta de serviço da Web do SnapCenter Plug-in para Microsoft Windows. E

```
"snapcenter_windows_host_plugin.exe"/silent  
/debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\ " BI_SNAPCENTER_PORT=8145  
SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"  
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=SCW,SCSQL
```



Todos os parâmetros passados durante a instalação do Plug-in para SQL Server são sensíveis a maiúsculas e minúsculas.

6. Monitore o agendador de tarefas do Windows, o arquivo de log de instalação principal C: Installdebug.log e os arquivos de instalação adicionais em C: Temp.
7. Monitore o diretório %temp% para verificar se os instaladores do msie.exe estão instalando o software sem erros.








A instalação do plug-in para SQL Server registra o plug-in no host e não no servidor SnapCenter. Você pode registrar o plug-in no servidor SnapCenter adicionando o host usando a GUI do SnapCenter ou cmdlet do PowerShell. Depois que o host é adicionado, o plug-in é descoberto automaticamente.

Monitore o status da instalação do Plug-in para SQL Server

Pode monitorizar o progresso da instalação do pacote de plug-ins do SnapCenter utilizando a página trabalhos. Você pode querer verificar o andamento da instalação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

-  Em curso
-  Concluído com êxito
-  Falha
-  Preenchido com avisos ou não foi possível iniciar devido a avisos
-  Em fila de espera

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **trabalhos**.
3. Na página trabalhos, para filtrar a lista de modo a que apenas as operações de instalação de plug-in sejam listadas, faça o seguinte:
 - a. Clique em **filtro**.
 - b. Opcional: Especifique a data de início e fim.
 - c. No menu suspenso tipo, selecione **Instalação Plug-in**.
 - d. No menu suspenso Status, selecione o status da instalação.
 - e. Clique em **aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Configurar certificado CA

Gerar arquivo CSR do certificado CA

Você pode gerar uma solicitação de assinatura de certificado (CSR) e importar o certificado que pode ser obtido de uma autoridade de certificação (CA) usando a CSR gerada. O certificado terá uma chave privada associada a ele.

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

Para obter informações sobre como gerar um CSR, "[Como gerar o arquivo CSR do certificado CA](#)" consulte .



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

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

Importar certificados CA

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

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File > Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola > certificados – computador local > autoridades de Certificação raiz fidedignas > certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" e selecione **todas as tarefas > Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente...	Faça o seguinte...
Importar chave privada	Selecione a opção Yes , importe a chave privada e clique em Next .
Importar formato de ficheiro	Não faça alterações; clique em seguinte .
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em Avançar .
Concluir o Assistente de importação de certificados	Revise o resumo e clique em Finish para iniciar a importação.



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

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

Obtenha a impressão digital do certificado CA

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

Passos

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

e. Remova os espaços entre os números hexadecimais.

Por exemplo, se a impressão digital for: "A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 B0 0d 42 77 A3 2a 7b", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:

a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

```
Get-ChildItem -Path Cert: LocalMachine/My
```

b. Copie a impressão digital.

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

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

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

Passos

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

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

Por exemplo:

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

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

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

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
appid="$guid"
```

Por exemplo:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

Ative certificados de CA para plug-ins

Você deve configurar os certificados de CA e implantar os certificados de CA no servidor SnapCenter e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

O que você vai precisar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet `RUN Set-SmCertificateSettings`.
- Você pode exibir o status do certificado para os plug-ins usando as `Get-SmCertificateSettings`.





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

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **hosts gerenciados**.
3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

Depois de terminar

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

-  ** Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.
-  ** Indica que o certificado da CA foi validado com êxito.
-  ** Indica que o certificado da CA não pôde ser validado.
-  ** indica que as informações de conexão não puderam ser recuperadas.



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

Configurar a recuperação de desastres

Recuperação de desastres do plug-in SnapCenter para SQL Server

Quando o plug-in do SnapCenter estiver inativo, mude para um host SQL diferente e recupere os dados executando algumas etapas.

O que você vai precisar

- O host secundário deve ter o mesmo sistema operacional, aplicativo e nome de host que o host principal.
- Envie o plug-in do SnapCenter para SQL Server para um host alternativo usando a página **Adicionar host** ou **Modificar host**.

Passos

1. Selecione o host na página **hosts** para modificar e instalar o plug-in do SnapCenter para SQL Server.
2. (Opcional) substitua o plug-in do SnapCenter para arquivos de configuração do SQL Server do backup de recuperação de desastres (DR) para a nova máquina.
3. Importe programações do Windows e SQL da pasta do plug-in do SnapCenter para SQL Server do backup de DR.

Para obter mais informações, consulte o "[APIs de recuperação de desastres](#)" vídeo.

Recuperação de desastres de storage (DR) para plug-in SnapCenter para SQL Server

Você pode recuperar o plug-in do SnapCenter para armazenamento do SQL Server habilitando o modo DR para armazenamento na página Configurações globais.

O que você vai precisar

- Certifique-se de que os plug-ins estão no modo de manutenção.
- Quebre a relação SnapMirror/SnapVault. "[Quebrando relacionamentos SnapMirror](#)"
- Conecte o LUN do secundário à máquina host com a mesma letra de unidade.
- Certifique-se de que todos os discos estejam conectados usando as mesmas letras de unidade usadas antes do DR.
- Reinicie o serviço de servidor MSSQL.
- Certifique-se de que os recursos SQL estão novamente online.

Sobre esta tarefa

A recuperação de desastres (DR) não é compatível com configurações VMDK e RDM.

Passos

1. Na página Configurações, navegue até **Configurações > Configurações globais > recuperação de desastres**.
2. Selecione **Ativar recuperação de desastres**.
3. Clique em **aplicar**.
4. Verifique se a tarefa DR está ativada ou não clicando em **Monitor > jobs**.

Depois de terminar

- Se novos bancos de dados forem criados após o failover, os bancos de dados estarão no modo não DR.
Os novos bancos de dados continuarão operando como antes do failover.
- Os novos backups criados no modo DR serão listados em SnapMirror ou SnapVault (secundário) na página topologia.

Um ícone "i" é exibido ao lado dos novos backups para indicar que esses backups foram criados durante o modo DR.

- Você pode excluir o plug-in do SnapCenter para backups do SQL Server criados durante o failover usando a IU ou o cmdlet a seguir: `Remove-SmBackup`
- Após o failover, se você quiser que alguns dos recursos estejam em modo não DR, use o seguinte cmdlet: `Remove-SmResourceDRMode`

Para obter mais informações, consulte "[Guia de referência de cmdlet do software SnapCenter](#)".

- O servidor SnapCenter gerenciará os recursos de storage individuais (bancos de dados SQL) que estão no modo DR ou não DR, mas não o grupo de recursos com recursos de storage que estão no modo DR ou no modo não DR.

Failback do plug-in do SnapCenter para storage secundário do SQL Server para storage primário

Depois que o plug-in do SnapCenter para o armazenamento primário do SQL Server estiver novamente on-line, você deve fazer o failback para o storage primário.

O que você vai precisar

- Coloque o plug-in do SnapCenter para SQL Server no modo **Manutenção** na página hosts gerenciados.
- Desconecte o storage secundário do host e conecte-se ao storage primário.
- Para fazer o failback para o storage primário, verifique se a direção da relação permanece a mesma antes do failover executando a operação de resincronização reversa.

Para manter as funções de armazenamento primário e secundário após a operação de resincronização reversa, execute novamente a operação de resincronização reversa.

Para obter mais informações, consulte "[Reverter a resincronização das relações de espelho](#)".

- Reinicie o serviço de servidor MSSQL.
- Certifique-se de que os recursos SQL estão novamente online.



Durante o failover ou failback do plug-in, o status geral do plug-in não é atualizado imediatamente. O status geral do host e do plug-in é atualizado durante a operação de atualização subsequente do host.

Passos

1. Na página Configurações, navegue até **Configurações > Configurações globais > recuperação de desastres**.
2. Desmarque **Ativar recuperação de desastres**.
3. Clique em **aplicar**.
4. Verifique se a tarefa DR está ativada ou não clicando em **Monitor > jobs**.

Depois de terminar

- Você pode excluir o plug-in do SnapCenter para backups do SQL Server criados durante o failover usando a IU ou o cmdlet a seguir: `Remove-SmDRFailoverBackups`

Instale o plug-in do SnapCenter para VMware vSphere

Se seu banco de dados estiver armazenado em máquinas virtuais (VMs) ou se você quiser proteger VMs e datastores, será necessário implantar o plug-in do SnapCenter para o dispositivo virtual VMware vSphere.

Para obter informações sobre como implantar, "[Visão geral da implantação](#)" consulte .

Implantar certificado CA

Para configurar o certificado CA com o plug-in SnapCenter para VMware vSphere, "[Criar ou importar certificado SSL](#)" consulte .

Configure o arquivo CRL

O plug-in do SnapCenter para VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL para o plug-in do SnapCenter para VMware vSphere é `/opt/NetApp/config/crl`.

Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Preparar-se para a proteção de dados

Pré-requisitos para usar o plug-in do SnapCenter para Microsoft SQL Server

Antes de começar a usar o plug-in para SQL Server, o administrador do SnapCenter deve instalar e configurar o servidor SnapCenter e executar tarefas pré-requisitos.

- Instalar e configurar o servidor SnapCenter.
- Inicie sessão no SnapCenter.
- Configure o ambiente SnapCenter adicionando ou atribuindo conexões do sistema de storage e criando credenciais.



O SnapCenter não é compatível com vários SVMs com o mesmo nome em clusters diferentes. Cada SVM com suporte do SnapCenter precisa ter um nome exclusivo.

- Adicione hosts, instale os plug-ins, descubra (atualize) os recursos e configure os plug-ins.
- Mova um banco de dados existente do Microsoft SQL Server de um disco local para um LUN NetApp ou vice-versa executando `invoke-SmConfigureResources`.

Para obter informações sobre como executar o cmdlet, consulte "[Guia de referência de cmdlet do software SnapCenter](#)"

- Se você estiver usando o servidor SnapCenter para proteger bancos de dados SQL que residem em LUNs ou VMDKs do VMware RDM, você deverá implantar o plug-in do SnapCenter para VMware vSphere e Registrar o plug-in com o SnapCenter. A documentação do plug-in do SnapCenter para VMware vSphere tem mais informações.

["Plug-in do SnapCenter para documentação do VMware vSphere"](#)

- Execute o provisionamento de storage no lado do host usando o plug-in do SnapCenter para Microsoft Windows.
- Configure as relações do SnapMirror e do SnapVault, se quiser fazer backup da replicação.

Para obter detalhes, consulte informações de instalação do SnapCenter.

Para usuários do SnapCenter 4.1.1, a documentação do plug-in do SnapCenter para VMware vSphere 4.1.1 tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos. Para usuários do SnapCenter 4,2.x, o Agente de dados do NetApp 1,0 e 1,0.1, a documentação tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o plug-in do SnapCenter para VMware vSphere fornecido pelo dispositivo virtual NetApp Data Broker baseado em Linux (formato Open Virtual Appliance). Para usuários do SnapCenter 4,3.x, a documentação do plug-in do SnapCenter para VMware vSphere 4,3 tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o plug-in SnapCenter baseado no Linux para o dispositivo virtual VMware vSphere (formato Open Virtual Appliance).

["Plug-in do SnapCenter para documentação do VMware vSphere"](#)

Como recursos, grupos de recursos e políticas são usados para proteger o SQL Server

Antes de usar o SnapCenter, é útil entender conceitos básicos relacionados às operações de backup, clonagem e restauração que você deseja executar. Você interage com recursos, grupos de recursos e políticas para diferentes operações.

- Os recursos geralmente são bancos de dados, instâncias de banco de dados ou grupos de disponibilidade do Microsoft SQL Server que você faz backup ou clone com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host ou cluster.

Quando você executa uma operação em um grupo de recursos, executa essa operação nos recursos definidos no grupo de recursos de acordo com a programação especificada para o grupo de recursos.

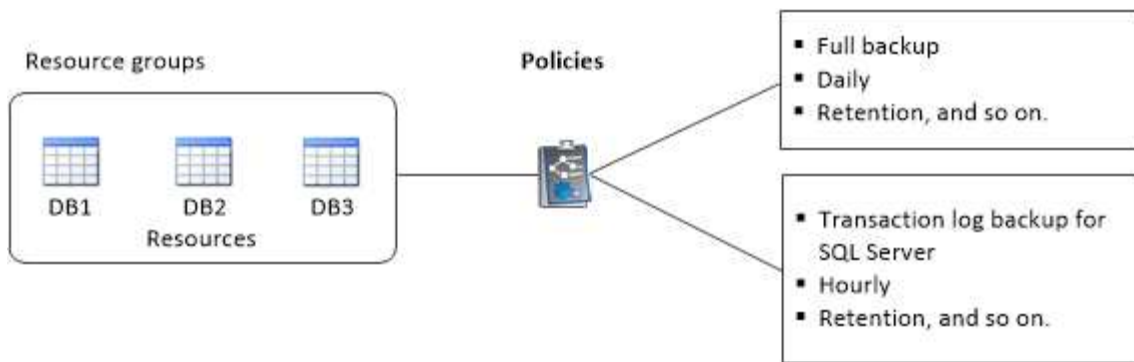
Você pode fazer backup sob demanda de um único recurso ou de um grupo de recursos. Você também pode executar backups programados para recursos únicos e grupos de recursos.

- As políticas especificam a frequência de backup, retenção de cópia, replicação, scripts e outras características das operações de proteção de dados.

Ao criar um grupo de recursos, você seleciona uma ou mais políticas para esse grupo. Você também pode selecionar uma política quando você executa um backup sob demanda para um único recurso.

Pense em um grupo de recursos como definindo *o que* você quer proteger e quando você quer protegê-lo em termos de dia e tempo. Pense em uma política como definindo *como* você quer protegê-la. Se você estiver fazendo backup de todos os bancos de dados ou fazendo backup de todos os sistemas de arquivos de um host, por exemplo, você pode criar um grupo de recursos que inclua todos os bancos de dados ou todos os sistemas de arquivos no host. Em seguida, você pode anexar duas políticas ao grupo de recursos: Uma política diária e uma política por hora. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diário e outro agendamento que executa backups de log por hora.

A imagem a seguir ilustra a relação entre recursos, grupos de recursos e políticas para bancos de dados:



Faça backup do banco de dados do SQL Server, instância ou grupo de disponibilidade

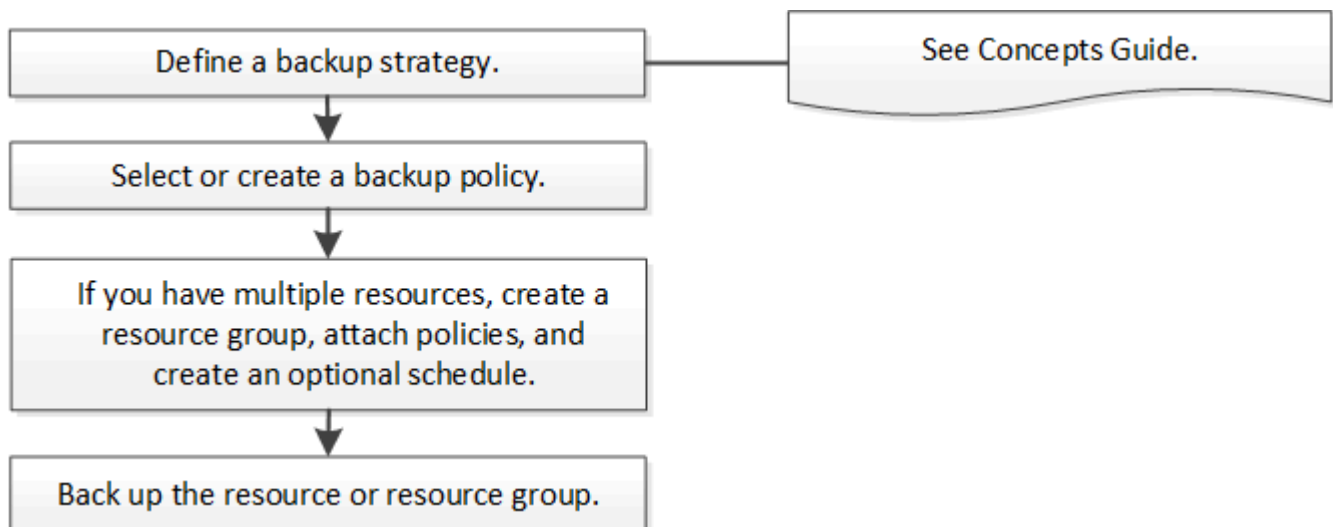
Fluxo de trabalho de backup

Ao instalar o plug-in do SnapCenter para Microsoft SQL Server em seu ambiente, você pode usar o SnapCenter para fazer backup dos recursos do SQL Server.

Você pode agendar vários backups para serem executados em servidores simultaneamente.

As operações de backup e restauração não podem ser executadas simultaneamente no mesmo recurso.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar as operações de backup:



As opções fazer backup agora, restaurar, gerenciar backups e clonar na página recursos serão desativadas se você selecionar um LUN que não seja NetApp, um banco de dados corrompido ou um banco de dados que está sendo restaurado.

Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração, recuperação, verificação e clone. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet SnapCenter ou consulte o ["Guia de referência de cmdlet do software SnapCenter"](#)

Como o SnapCenter faz backup de bancos de dados

O SnapCenter usa a tecnologia de cópia Snapshot para fazer backup dos bancos de dados do SQL Server que residem em LUNs ou VMDKs. O SnapCenter cria o backup criando cópias Snapshot dos bancos de dados.

Quando você seleciona um banco de dados para um backup completo do banco de dados na página recursos, o SnapCenter seleciona automaticamente todos os outros bancos de dados que residem no mesmo volume de storage. Se o LUN ou VMDK armazenar apenas um único banco de dados, você pode limpar ou re selecionar o banco de dados individualmente. Se o LUN ou VMDK contiver vários bancos de dados, você deve limpar ou re selecionar os bancos de dados como um grupo.

O backup de todos os bancos de dados que residem em um único volume é realizado simultaneamente, usando cópias Snapshot. Se o número máximo de bancos de dados de backup simultâneos for 35 e se mais de 35 bancos de dados residirem em um volume de storage, o número total de cópias Snapshot criadas será igual ao número de bancos de dados dividido por 35.



Você pode configurar o número máximo de bancos de dados para cada cópia Snapshot na política de backup.

Quando o SnapCenter cria uma cópia Snapshot, todo o volume do sistema de storage é capturado na cópia Snapshot. No entanto, o backup é válido apenas para o servidor host SQL para o qual o backup foi criado.

Se os dados de outros servidores host SQL residirem no mesmo volume, esses dados não poderão ser restaurados a partir da cópia Snapshot.

Encontre mais informações

["Faça backup de recursos usando cmdlets do PowerShell"](#)

["Operações de quiesce ou agrupamento de recursos falham"](#)

Determine se os recursos estão disponíveis para backup

Os recursos são bancos de dados, instâncias de aplicativos, grupos de disponibilidade e componentes semelhantes que são mantidos pelos plug-ins instalados. Você pode adicionar esses recursos a grupos de recursos para que você possa executar tarefas de proteção de dados, mas primeiro você deve identificar quais recursos você tem disponíveis. A determinação dos recursos disponíveis também verifica se a instalação do plug-in foi concluída com êxito.

O que você vai precisar

- Você já deve ter concluído tarefas como instalar o servidor SnapCenter, adicionar hosts, criar conexões do sistema de storage e adicionar credenciais.
- Para descobrir os bancos de dados Microsoft SQL, uma das seguintes condições deve ser atendida.
 - O usuário que foi usado para adicionar o host de plug-in ao servidor SnapCenter deve ter as permissões necessárias (sysadmin) no Microsoft SQL Server.
 - Se a condição acima não for atendida, no servidor SnapCenter você deve configurar o usuário que tem as permissões necessárias (sysadmin) no Microsoft SQL Server. O usuário deve ser configurado no nível de instância do Microsoft SQL Server e o usuário pode ser um usuário SQL ou Windows.

- Para descobrir os bancos de dados Microsoft SQL em um cluster do Windows, você deve desbloquear a porta TCP/IP de instância de cluster de failover (FCI).
- Se os bancos de dados residirem em LUNs ou VMDKs do VMware RDM, você deverá implantar o plug-in do SnapCenter para VMware vSphere e Registrar o plug-in no SnapCenter.

Para obter mais informações, consulte "[Implante o plug-in do SnapCenter para VMware vSphere](#)"

- Se o host for adicionado com gMSA e se o gMSA tiver login e administrador do sistema Privileges, o gMSA será usado para se conectar à instância SQL.

Sobre esta tarefa

Não é possível fazer backup de bancos de dados quando a opção **Status Geral** na página Detalhes estiver definida como não disponível para backup. A opção **Estado geral** está definida como não disponível para cópia de segurança quando qualquer uma das seguintes situações for verdadeira:

- Os bancos de dados não estão em um LUN NetApp.
- Os bancos de dados não estão no estado normal.

Os bancos de dados não estão no estado normal quando estão offline, restaurando, recuperando pendente, suspeitando, etc.

- Os bancos de dados não têm Privileges suficientes.

Por exemplo, se um usuário tiver acesso somente à base de dados, os arquivos e propriedades do banco de dados não podem ser identificados e, portanto, não podem ser copiados.



O SnapCenter só pode fazer backup do banco de dados principal se você tiver uma configuração de grupo de disponibilidade no SQL Server Standard Edition.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Instância** ou **Grupo de disponibilidade** na lista suspensa **Exibir**.

Clique e selecione o nome do host e a instância do SQL Server para filtrar os recursos. Em seguida, pode clicar para fechar o painel de filtro.

3. Clique em **Atualizar recursos**.

Os recursos recém-adicionados, renomeados ou excluídos são atualizados para o inventário do servidor SnapCenter.



Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

Os recursos são exibidos juntamente com informações como tipo de recurso, nome de host ou cluster, grupos de recursos associados, tipo de backup, políticas e status geral.

- Se o banco de dados estiver em um armazenamento não NetApp, Not available for backup será exibido na coluna **Estado geral**.

Não é possível executar operações de proteção de dados em um banco de dados que esteja em um storage que não seja NetApp.

- Se o banco de dados estiver em um armazenamento NetApp e não estiver protegido, `Not protected` será exibido na coluna **Estado geral**.
- Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido, a interface do usuário exibirá `Backup not run` a mensagem na coluna **Estado geral**.
- Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido e se o backup for acionado para o banco de dados, a interface do usuário exibirá `Backup succeeded` a mensagem na coluna **Estado geral**.



Se você ativou uma autenticação SQL ao configurar as credenciais, a instância descoberta ou banco de dados será exibida com um ícone de cadeado vermelho. Se o ícone de cadeado aparecer, você deve especificar as credenciais da instância ou do banco de dados para adicionar com êxito a instância ou o banco de dados a um grupo de recursos.

Depois que o administrador do SnapCenter atribuir os recursos a um usuário do RBAC, o usuário do RBAC deve fazer login e clicar em **Atualizar recursos** para ver o status geral mais recente dos recursos.

Migrar recursos para o sistema de storage NetApp

Depois de ter provisionado o sistema de armazenamento NetApp usando o plug-in SnapCenter para Microsoft Windows, você pode migrar seus recursos para o sistema de armazenamento NetApp ou de um LUN NetApp para outro LUN NetApp usando a interface gráfica do usuário (GUI) do SnapCenter ou usando os cmdlets do PowerShell.

O que você vai precisar


- Você deve ter adicionado sistemas de storage ao servidor SnapCenter.
- Você deve ter atualizado (descoberto) os recursos do SQL Server.

A maioria dos campos nessas páginas do assistente são auto-explicativos. As informações a seguir descrevem alguns dos campos para os quais você pode precisar de orientação.

Passos


1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Instância** na lista suspensa **Exibir**.
3. Selecione o banco de dados ou a instância na lista e clique em **Migrate**.
4. Na página recursos, execute as seguintes ações:

Para este campo...	Faça isso...
Nome do banco de dados (opcional)	Se você selecionou uma instância para migração, você deve selecionar os bancos de dados dessa instância na lista suspensa bancos de dados .

Para este campo...	Faça isso...
Escolha Destinos	<p>Selecione o local de destino para dados e arquivos de log.</p> <p>Os ficheiros de dados e de registo são movidos para a pasta dados e Registo, respetivamente, sob a unidade NetApp selecionada. Se qualquer pasta na estrutura de pastas não estiver presente, uma pasta será criada e o recurso será migrado.</p>
Mostrar detalhes do arquivo de banco de dados (opcional)	<p>Selecione esta opção quando quiser migrar vários arquivos de um único banco de dados.</p> <div style="display: flex; align-items: center;">  <p>Esta opção não é exibida quando você seleciona o recurso Instância.</p> </div>
Opções	<p>Selecione Excluir cópia do banco de dados migrado no local original para excluir a cópia do banco de dados da origem.</p> <p>Opcional: EXECUTE ESTATÍSTICAS DE ATUALIZAÇÃO em tabelas antes de desanexar o banco de dados.</p>

5. Na página verificar, execute as seguintes ações:

Para este campo...	Faça isso...
Opções de verificação de consistência de banco de dados	<p>Selecione Executar antes para verificar a integridade do banco de dados antes da migração. Selecione Executar após para verificar a integridade do banco de dados após a migração.</p>

Para este campo...	Faça isso...
<ul style="list-style-type: none"> • DBCC CHECKDB opções* 	<ul style="list-style-type: none"> • Selecione a opção PHYSICAL_only para limitar a verificação de integridade à estrutura física do banco de dados e para detetar páginas rasgadas, falhas na soma de verificação e falhas comuns de hardware que afetam o banco de dados. • Selecione a opção NO_INFOMSGS para suprimir todas as mensagens informativas. • Selecione a opção All_ERRORMSGs para exibir todos os erros relatados por objeto. • Selecione a opção NOINDEX se não quiser verificar índices não agrupados. <p>O banco de dados do SQL Server usa o Microsoft SQL Server Database Consistency Checker (DBCC) para verificar a integridade física e lógica dos objetos no banco de dados.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>Você pode querer selecionar essa opção para diminuir o tempo de execução.</p> </div> <ul style="list-style-type: none"> • Selecione TABLOCK opção para limitar as verificações e obter bloqueios em vez de usar uma cópia Snapshot do banco de dados interno.

6. Revise o resumo e clique em **concluir**.

Criar políticas de backup para bancos de dados do SQL Server

Você pode criar uma política de backup para o recurso ou para o grupo de recursos antes de usar o SnapCenter para fazer backup de recursos do SQL Server ou criar uma política de backup no momento em que criar um grupo de recursos ou fazer backup de um único recurso.

O que você vai precisar

- Você precisa ter definido sua estratégia de proteção de dados.
- Você precisa se preparar para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, identificar recursos e criar conexões do sistema de storage.
- Você deve ter configurado o diretório de log do host para o backup de log.
- Você deve ter atualizado (descoberto) os recursos do SQL Server.
- Se você estiver replicando cópias Snapshot em um espelhamento ou cofre, o administrador do SnapCenter deverá ter atribuído as máquinas virtuais de storage (SVMs) para os volumes de origem e de destino a você.

Para obter informações sobre como os administradores atribuem recursos aos usuários, consulte as informações de instalação do SnapCenter.

- Se você quiser executar os scripts do PowerShell em prescripts e postscripts, defina o valor do parâmetro usePowershellProcessforScripts como true no arquivo web.config.

O valor padrão é false

Sobre esta tarefa

- Uma política de backup é um conjunto de regras que regem como você gerencia e retém backups e com que frequência o backup do recurso ou do grupo de recursos é feito. Além disso, você pode especificar as configurações de replicação e script. Especificar opções em uma política economiza tempo quando você deseja reutilizar a política para outro grupo de recursos.
- O SCRIPT_PATH é definido usando a chave PredefinedWindowsScriptsDirectory localizada no arquivo SMCOREServiceHost.exe.Config do host do plug-in.

Se necessário, você pode alterar esse caminho e reiniciar o serviço SMcore. É recomendável usar o caminho padrão para segurança.


O valor da chave pode ser exibido do swagger através da API: API /4,7/configsettings


Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.

- A maioria dos campos nessas páginas do assistente são auto-explicativos. As informações a seguir descrevem alguns dos campos para os quais você pode precisar de orientação.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **políticas**.
3. Clique em **novo**.
4. Na página Nome, insira o nome e a descrição da política.
5. Na página tipo de backup, execute as seguintes etapas:
 - a. Escolha o tipo de cópia de segurança:

Se você quiser...	Faça isso...
Faça backup dos arquivos de banco de dados e logs de transação e trancar os logs de transação	<ol style="list-style-type: none">i. Selecione cópia de segurança completa e cópia de segurança de registro.ii. Insira o número máximo de bancos de dados que devem ser copiados para cada cópia Snapshot. <div style="display: flex; align-items: center; margin-top: 10px;"><p>Você deve aumentar esse valor se quiser executar várias operações de backup simultaneamente.</p></div>

Se você quiser...	Faça isso...
Faça uma cópia de segurança dos ficheiros da base de dados	i. Selecione cópia de segurança completa . ii. Insira o número máximo de bancos de dados que devem ser copiados para cada cópia Snapshot. O valor padrão é 100  <p>Você deve aumentar esse valor se quiser executar várias operações de backup simultaneamente.</p>
Faça backup dos logs de transação	Selecione Log backup .


- b. Se você estiver fazendo backup de seus recursos usando outro aplicativo de backup, selecione **Backup somente cópia**.

Manter os logs de transação intactos permite que qualquer aplicativo de backup restaure os bancos de dados. Você normalmente não deve usar a opção somente cópia em nenhuma outra circunstância.



O Microsoft SQL não suporta a opção **cópia apenas de backup** juntamente com a opção **backup completo e backup de log** para armazenamento secundário.

- c. Na seção Configurações do Grupo de disponibilidade, execute as seguintes ações:

Para este campo...	Faça isso...
Backup apenas na réplica de backup preferencial	Selecione esta opção para fazer backup apenas na réplica de backup preferida. A réplica de backup preferida é decidida pelas preferências de backup configuradas para o AG no SQL Server.
Selecione réplicas para backup	Escolha a réplica AG primária ou a réplica AG secundária para o backup.
Prioridade de backup (prioridade mínima e máxima de backup)	Especifique um número mínimo de prioridade de backup e um número máximo de prioridade de backup que decida a réplica AG para backup. Por exemplo, você pode ter uma prioridade mínima de 10 e uma prioridade máxima de 50. Neste caso, todas as réplicas AG com uma prioridade superior a 10 e inferior a 50 são consideradas para backup.  <p>Por padrão, a prioridade mínima é 1 e a prioridade máxima é 100.</p>



Nas configurações de cluster, os backups são retidos em cada nó do cluster de acordo com as configurações de retenção definidas na política. Se o nó proprietário do AG for alterado, os backups serão feitos de acordo com as configurações de retenção e os backups do nó proprietário anterior serão mantidos. A retenção para AG é aplicável apenas no nível do nó.

- d. Se você quiser agendar o backup que deseja criar com esta política, especifique o tipo de agendamento selecionando **on Demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.

Você pode selecionar um tipo de agendamento para uma política.

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

- On demand
- Hourly
- Daily
- Weekly
- Monthly



Você pode especificar a programação (data de início, data de término e frequência) para a operação de backup ao criar um grupo de recursos. Isso permite que você crie grupos de recursos que compartilham a mesma política e frequência de backup, mas permite atribuir diferentes programações de backup a cada política.





Se você tiver agendado para as 2:00 da manhã, o horário não será acionado durante o horário de verão (DST).

6. Na página retenção, dependendo do tipo de backup selecionado na página tipo de backup, execute uma ou mais das seguintes ações:

- a. Na seção Configurações de retenção para a operação de restauração de até o minuto, execute uma das seguintes ações:

Se você quiser...	Faça isso...
Reter apenas um número específico de cópias Snapshot	Selecione a opção manter backups de log aplicáveis aos últimos dias do <number> e especifique o número de dias a serem retidos. Se você estiver perto desse limite, talvez queira excluir cópias mais antigas.
Guarde as cópias de backup por um número específico de dias	Selecione a opção manter backups de log aplicáveis aos últimos dias do <number> de backups completos e especifique o número de dias para manter as cópias de backup de log.

- b. Na seção **Configurações completas de retenções de backup** para as configurações de retenção sob demanda, execute as seguintes ações:

Para este campo...	Faça isso...
<p>Total de cópias Snapshot a serem mantidas</p>	<p>Se você quiser especificar o número de cópias snapshot a serem mantidas, selecione Total de cópias snapshot a serem mantidas.</p> <p>Se o número de cópias Snapshot exceder o número especificado, as cópias snapshot serão excluídas com as cópias mais antigas excluídas primeiro.</p> <div data-bbox="898 583 954 636" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">  <p>O valor máximo de retenção é 1018 para recursos no ONTAP 9.4 ou posterior e 254 para recursos no ONTAP 9.3 ou anterior. Os backups falharão se a retenção for definida para um valor maior do que o que a versão subjacente do ONTAP suporta.</p> </div> <div data-bbox="898 940 954 993" style="border: 1px solid #ccc; padding: 5px;">  <p>Por padrão, o valor da contagem de retenção é definido como 2. Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque a primeira cópia Snapshot é a cópia Snapshot de referência para a relação SnapVault até que uma cópia Snapshot mais recente seja replicada para o destino.</p> </div>
<p>Manter cópias Snapshot durante</p>	<p>Se você quiser especificar o número de dias para os quais deseja manter as cópias Snapshot antes de excluí-las, selecione manter cópias snapshot para.</p>

- c. Na seção **Configurações completas de retenções de backup** para as configurações de retenção horária, diária, semanal e mensal, especifique as configurações de retenção para o tipo de agendamento selecionado na página tipo de backup.

Para este campo...	Faça isso...
Total de cópias Snapshot a serem mantidas	<p>Se você quiser especificar o número de cópias snapshot a serem mantidas, selecione Total de cópias snapshot a serem mantidas. Se o número de cópias Snapshot exceder o número especificado, as cópias snapshot serão excluídas com as cópias mais antigas excluídas primeiro.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>Você deve definir a contagem de retenção como 2 ou superior, se quiser habilitar a replicação do SnapVault. Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque a primeira cópia Snapshot é a cópia Snapshot de referência para a relação SnapVault até que uma cópia Snapshot mais recente seja replicada para o destino.</p> </div>
Manter cópias Snapshot durante	<p>Se você quiser especificar o número de dias para os quais deseja manter as cópias Snapshot antes de excluí-las, selecione manter cópias snapshot para.</p>

A retenção de cópia Snapshot do log é definida como 7 dias por padrão. Use o cmdlet Set-SmPolicy para alterar a retenção de cópia Snapshot do log.


Este exemplo define a retenção de cópia Snapshot do log como 2:

```
Set-SmPolicy -PolicyName 'newpol' -PolicyType 'Backup' -PluginPolicyType
'SCSQL' -sqlbackuptype 'FullBackupAndLogBackup' -RetentionSettings
@{BackupType='DATA';ScheduleType='Hourly';RetentionCount=2},{BackupType
='LOG_SNAPSHOT';ScheduleType='None';RetentionCount=2},{BackupType='LOG'
;ScheduleType='Hourly';RetentionCount=2} -schedulescheduletype 'Hourly'
```

+ "O SnapCenter retém cópias Snapshot do banco de dados"

7. Na página replicação, especifique a replicação para o sistema de storage secundário:

Para este campo...	Faça isso...
Atualize o SnapMirror depois de criar uma cópia Snapshot local	<p>Selecione esta opção para criar cópias espelhadas de conjuntos de backup em outro volume (SnapMirror).</p>

Para este campo...	Faça isso...
Atualize o SnapVault depois de criar uma cópia Snapshot	Selecione esta opção para executar a replicação de backup de disco para disco.
Etiqueta de política secundária	<p>Selecione uma etiqueta Snapshot.</p> <p>Dependendo do rótulo da cópia Snapshot selecionado, o ONTAP aplica a política de retenção da cópia snapshot secundária que corresponde ao rótulo.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> Se você selecionou Atualizar SnapMirror depois de criar uma cópia Snapshot local, você pode especificar opcionalmente o rótulo de política secundária. No entanto, se você selecionou Atualizar SnapVault depois de criar uma cópia Snapshot local, especifique o rótulo de política secundária.</p> </div>
Contagem de tentativas de erro	Insira o número de tentativas de replicação que devem ocorrer antes que o processo pare.

8. Na página Script, insira o caminho e os argumentos do prescript ou postscript que devem ser executados antes ou depois da operação de backup, respectivamente.

Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas e enviar logs.



O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.



Você deve configurar a política de retenção SnapMirror no ONTAP para que o storage secundário não atinja o limite máximo de cópias Snapshot.

9. Na página Verificação, execute as seguintes etapas:
- a. Na seção Executar verificação para as seguintes programações de backup, selecione a frequência de agendamento.
 - b. Na seção Opções de verificação consistência de banco de dados, execute as seguintes ações:

Para este campo...	Faça isso...
Limitar a estrutura de integridade à estrutura física do banco de dados (FÍSICO_SOMENTE)	Selecione Limit a estrutura de integridade à estrutura física do banco de dados (PHYSICAL_only) para limitar a verificação de integridade à estrutura física do banco de dados e para detetar páginas rasgadas, falhas de checksum e falhas comuns de hardware que afetam o banco de dados.
Suprima todas as mensagens de informação (NO_INFOMSGS)	Selecione Suprima todas as mensagens de informação (NO_INFOMSGS) para suprimir todas as mensagens informativas. Selecionado por predefinição.
Exibir todas as mensagens de erro reportadas por objeto (ALL_ERRORMSGs)	Selecione Exibir todas as mensagens de erro relatadas por objeto (ALL_ERRORMSGs) para exibir todos os erros relatados por objeto.
Não verificar índices não agrupados (NOINDEX)	Selecione não verifique índices não agrupados (NOINDEX) se você não quiser verificar índices não agrupados. O banco de dados do SQL Server usa o Microsoft SQL Server Database Consistency Checker (DBCC) para verificar a integridade física e lógica dos objetos no banco de dados.
Limitar as verificações e obter os bloqueios em vez de usar uma cópia Snapshot do banco de dados interno (TABLOCK)	Selecione Limit as verificações e obtenha os bloqueios em vez de usar uma cópia Snapshot do banco de dados interno (TABLOCK) para limitar as verificações e obter bloqueios em vez de usar uma cópia Snapshot do banco de dados interno.

- c. Na seção **Backup de log**, selecione **verificar backup de log após a conclusão** para verificar o backup de log após a conclusão.
- d. Na seção **Configurações do script de verificação**, insira o caminho e os argumentos do prescriitor ou postscript que devem ser executados antes ou depois da operação de verificação, respetivamente.



O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.

10. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas para o SQL Server

Um grupo de recursos é um contentor ao qual você adiciona recursos que deseja fazer backup e proteger juntos. Um grupo de recursos permite fazer backup de todos os dados associados a um determinado aplicativo simultaneamente. Um grupo de recursos é necessário para qualquer trabalho de proteção de dados. Você também deve anexar

uma ou mais políticas ao grupo de recursos para definir o tipo de tarefa de proteção de dados que deseja executar.

Você pode proteger recursos individualmente sem criar um novo grupo de recursos. Você pode fazer backups no recurso protegido.


Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** na lista **Exibir**.



Se você recentemente adicionou um recurso ao SnapCenter, clique em **Atualizar recursos** para exibir o recurso recém-adicionado.

3. Clique em **novo grupo de recursos**.
4. Na página Nome, execute as seguintes ações:

Para este campo...	Faça isso...
Nome	Introduza o nome do grupo de recursos.  O nome do grupo de recursos não deve exceder 250 caracteres.
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar HR como uma tag a vários grupos de recursos, poderá encontrar mais tarde todos os grupos de recursos associados à tag HR.
Use o formato de nome personalizado para cópia Snapshot	Opcional: Insira o nome e o formato da cópia Snapshot personalizada. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, um carimbo de data/hora é anexado ao nome da cópia Snapshot.

5. Na página recursos, execute as seguintes etapas:
 - a. Selecione o nome do host, o tipo de recurso e a instância do SQL Server nas listas suspensas para filtrar a lista de recursos.



Se você tiver adicionado recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois de atualizar sua lista de recursos.


- b. Para mover recursos da seção **recursos disponíveis** para a seção recursos selecionados, execute uma das seguintes etapas:
 - Selecione **seleção automática de todos os recursos no mesmo volume de armazenamento** para mover todos os recursos no mesmo volume para a seção recursos selecionados.

- Selecione os recursos na seção **recursos disponíveis** e clique na seta para a direita para movê-los para a seção **recursos selecionados**.


6. Na página políticas, execute as seguintes etapas:

- a. Selecione uma ou mais políticas na lista suspensa.



Você também pode criar uma política clicando em  .

Na seção Configurar agendas para políticas selecionadas, as políticas selecionadas são listadas.

- b. Na seção Configurar agendas para políticas selecionadas, clique em  na coluna Configurar agendas para a política para a qual você deseja configurar o agendamento.

- c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação especificando a data de início, data de expiração e frequência e clique em **OK**.

Você deve fazer isso para cada frequência listada na política. As programações configuradas são listadas na coluna agendas aplicadas na seção **Configurar programações para políticas selecionadas**.

- d. Selecione o agendador do Microsoft SQL Server.

Você também deve selecionar uma instância do agendador para associar à política de agendamento.

Se você não selecionar o agendador do Microsoft SQL Server, o padrão é o agendador do Microsoft Windows.

As agendas de backup de terceiros não são suportadas quando sobrepõem-se às agendas de backup do SnapCenter. Você não deve modificar as programações e renomear a tarefa de backup criada no Windows Scheduler ou no SQL Server Agent.


7. Na página Verificação, execute as seguintes etapas:

- a. Selecione o servidor de verificação na lista suspensa **servidor de verificação**.

A lista inclui todos os servidores SQL adicionados no SnapCenter. Você pode selecionar vários servidores de verificação (host local ou host remoto).





A versão do servidor de verificação deve corresponder à versão e edição do servidor SQL que está hospedando o banco de dados principal.

- a. Clique em **Load Locators** para carregar os volumes SnapMirror e SnapVault para executar a verificação no armazenamento secundário.
- b. Selecione a política para a qual pretende configurar o seu agendamento de verificação e, em seguida, clique em * *  .
- c. Na caixa de diálogo Adicionar agendamentos de verificação *policy_name* , execute as seguintes ações:

Se você quiser...	Faça isso...
Execute a verificação após a cópia de segurança	Selecione Executar verificação após backup .
Marque uma verificação	Selecione Executar verificação agendada .

d. Clique em **OK**.

As programações configuradas são listadas na coluna agendas aplicadas. Pode rever e editar clicando

em  * ou eliminar clicando em *  .

8. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. Se quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar Relatório de trabalho**.



Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando PowerShell SET-SmtpServer.

9. Revise o resumo e clique em **Finish**.

Encontre mais informações

["Criar políticas de backup para bancos de dados do SQL Server"](#)

Requisitos para fazer backup de recursos SQL

Antes de fazer backup de um recurso SQL, você deve garantir que vários requisitos sejam atendidos.

- Você precisa ter migrado um recurso de um sistema de storage que não seja da NetApp para um sistema de storage da NetApp.
- Você deve ter criado uma política de backup.
- Se você quiser fazer backup de um recurso que tenha uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "SnapMirror All". No entanto, se você estiver usando a função "vsadmin", o privilégio "SnapMirror all" não será necessário.
- A operação de backup iniciada por um usuário de diretório ativo (AD) falha se a credencial de instância SQL não for atribuída ao usuário ou grupo do AD. Você deve atribuir a credencial da instância SQL ao usuário ou grupo do AD na página **Configurações > Acesso do usuário**.
- Você deve ter criado um grupo de recursos com uma política anexada.
- Se um grupo de recursos tiver vários bancos de dados de hosts diferentes, a operação de backup em alguns hosts pode ser acionada tarde devido a problemas de rede. Você deve configurar o valor de FMaxRetryForUninitializedHosts em web.config usando o cmdlet Set-SmConfigSettings PS.

Faça backup de recursos SQL

Se um recurso ainda não fizer parte de qualquer grupo de recursos, você poderá fazer backup do recurso na página recursos.

Sobre esta tarefa

- Para autenticação de credenciais do Windows, você deve configurar sua credencial antes de instalar os plug-ins.
- Para autenticação de instância do SQL Server, você deve adicionar a credencial após a instalação dos plug-ins.
- Para autenticação gMSA, você deve configurar o gMSA enquanto Registra o host com o SnapCenter na página **Adicionar host** ou **Modificar host** para ativar e usar o gMSA.
- Se o host for adicionado com gMSA e se o gMSA tiver login e administrador do sistema Privileges, o gMSA será usado para se conectar à instância SQL.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados**, ou **Instância** ou **Grupo de disponibilidade** na lista suspensa **Exibir**.

- a. Selecione o banco de dados, instância ou grupo de disponibilidade que você deseja fazer backup.

Quando você faz um backup de uma instância, as informações sobre o último status de backup ou o carimbo de data/hora dessa instância não estarão disponíveis na página recursos.

Na visualização de topologia, não é possível diferenciar se o status do backup, o carimbo de data/hora ou o backup é para uma instância ou um banco de dados.

3. Na página recursos, marque a caixa de seleção **formato de nome personalizado para cópia Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome da cópia Snapshot.


Por exemplo, customtext_policy_hostname ou resource_hostname. Por padrão, um carimbo de data/hora é anexado ao nome da cópia Snapshot.

4. Na página políticas, execute as seguintes tarefas:

- a. Na seção políticas, selecione uma ou mais políticas na lista suspensa.

Pode criar uma política clicando em  para iniciar o assistente de política.

Na seção **Configurar programações para políticas selecionadas**, as políticas selecionadas são listadas.

- b. Clique em  ** na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.
- c. Na caixa de diálogo **Adicionar agendas para política** policy_name, configure a programação e clique em **OK**.

`policy_name` Aqui está o nome da política que você selecionou.

As programações configuradas são listadas na coluna **programações aplicadas**.

- a. Selecione o **Use o agendador do Microsoft SQL Server** e selecione a instância do agendador na lista suspensa **Instância do Agendador** associada à política de agendamento.


5. Na página Verificação, execute as seguintes etapas:

- a. Selecione o servidor de verificação na lista suspensa **servidor de verificação**.

Você pode selecionar vários servidores de verificação (host local ou host remoto).



A versão do servidor de verificação deve ser igual ou superior à versão da edição do servidor SQL que está hospedando o banco de dados principal.

- a. Selecione **carregar localizadores secundários para verificar backups no secundário** para verificar seus backups no sistema de armazenamento secundário.
- b. Selecione a política para a qual pretende configurar o seu agendamento de verificação e, em seguida, clique em **  .
- c. Na caixa de diálogo Adicionar agendas de verificação *policy_name*, execute as seguintes ações:

Se você quiser...	Faça isso...
Execute a verificação após a cópia de segurança	Selecione Executar verificação após cópia de segurança .
Marque uma verificação	Selecione Executar verificação agendada .



Se o servidor de verificação não tiver uma conexão de armazenamento, a operação de verificação falhará com erro: Falha ao montar o disco.

- d. Clique em **OK**.

As programações configuradas são listadas na coluna agendas aplicadas.

6. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. Se quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar Relatório de trabalho**.



Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando PowerShell SET-SmtpServer.

7. Revise o resumo e clique em **Finish**.

A página de topologia do banco de dados é exibida.

8. Clique em **fazer backup agora**.

9. Na página Backup, execute as seguintes etapas:

- a. Se você tiver aplicado várias políticas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.

Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

- b. Selecione **Verify after backup** para verificar o backup.

- c. Clique em **Backup**.



Você não deve renomear a tarefa de backup criada no Windows Scheduler ou no SQL Server Agent.

Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

Um grupo de recursos implícito é criado. Pode ver isto selecionando o respectivo utilizador ou grupo na página Acesso ao Utilizador. O tipo de grupo de recursos implícito é "recurso".

10. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

Depois de terminar

- Nas configurações do MetroCluster, o SnapCenter pode não ser capaz de detetar uma relação de proteção após um failover.

["Não é possível detetar a relação SnapMirror ou SnapVault após o failover do MetroCluster"](#)

- Se você estiver fazendo backup de dados de aplicativos em VMDKs e o tamanho de heap Java para o plug-in SnapCenter para VMware vSphere não for grande o suficiente, o backup pode falhar. Para aumentar o tamanho do heap Java, localize o arquivo de script `/opt/NetApp/init_scripts/scvservice`. Nesse script, o `do_start method` comando inicia o serviço de plug-in SnapCenter VMware. Atualize esse comando para o seguinte: `Java -jar -Xmx8192M -Xms4096M`.

Encontre mais informações

["Criar políticas de backup para bancos de dados do SQL Server"](#)

["Faça backup de recursos usando cmdlets do PowerShell"](#)

["Operações de backup falha com erro de conexão MySQL devido ao atraso no TCP_TIMEOUT"](#)

["A cópia de segurança falha com o erro do programador do Windows"](#)

["Operações de quiesce ou agrupamento de recursos falham"](#)



Fazer backup de grupos de recursos do SQL Server

Você pode fazer backup de um grupo de recursos sob demanda na página recursos. Se

um grupo de recursos tiver uma política anexada e uma programação configurada, os backups ocorrerão automaticamente de acordo com a programação.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Grupo de recursos** na lista **Exibir**.

Você pode pesquisar o grupo de recursos inserindo o nome do grupo de recursos na caixa de pesquisa ou clicando em  e, em seguida, selecionando a tag. Em seguida, pode clicar em  * para fechar o painel do filtro.

3. Na página grupos de recursos, selecione o grupo de recursos que deseja fazer backup e clique em **fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
 - a. Se você associou várias políticas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.

Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.
 - b. Após o backup, selecione **Verify** para verificar o backup sob demanda.

A opção **Verify** na política aplica-se apenas a trabalhos agendados.
 - c. Clique em **Backup**.
5. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

Encontre mais informações

["Criar políticas de backup para bancos de dados do SQL Server"](#)

["Crie grupos de recursos e anexe políticas para o SQL Server"](#)

["Faça backup de recursos usando cmdlets do PowerShell"](#)

["Operações de backup falha com erro de conexão MySQL devido ao atraso no TCP_TIMEOUT"](#)

["A cópia de segurança falha com o erro do programador do Windows"](#)

Monitorar operações de backup







Monitore operações de backup de recursos SQL na página de tarefas do SnapCenter

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Você pode querer verificar o progresso para determinar quando ele está concluído ou se há um problema.


Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado correspondente das


operações:

-  Em curso
-  Concluído com êxito
-  Falha
-  Preenchido com avisos ou não foi possível iniciar devido a avisos
-  Em fila de espera
-  Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **trabalhos**.
3. Na página trabalhos, execute as seguintes etapas:
 - a. Clique  para filtrar a lista de modo a que apenas as operações de cópia de segurança sejam listadas.
 - b. Especifique as datas de início e fim.
 - c. Na lista suspensa **Type**, selecione **Backup**.
 - d. Na lista suspensa **Status**, selecione o status da cópia de segurança.
 - e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione um trabalho de cópia de segurança e clique em **Detalhes** para ver os detalhes do trabalho.



Embora o status do trabalho de backup seja exibido  , quando você clica nos detalhes do trabalho, você pode ver que algumas das tarefas secundárias da operação de backup ainda estão em andamento ou marcadas com sinais de aviso.

5. Na página Detalhes da tarefa, clique em **Exibir logs**.


O botão **View logs** exibe os logs detalhados para a operação selecionada.

Monitore operações de proteção de dados em recursos SQL no painel atividade

O painel atividade exibe as cinco operações mais recentes executadas. O painel atividade também é exibido quando a operação foi iniciada e o status da operação.

O painel atividade exibe informações sobre operações de backup, restauração, clone e backup agendadas. Se você estiver usando Plug-in para SQL Server ou Plug-in para Exchange Server, o painel atividade também exibirá informações sobre a operação de Reseed.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Clique  no painel atividade para visualizar as cinco operações mais recentes.

Quando clica numa das operações, os detalhes da operação são listados na página Detalhes da tarefa.

Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell

Você deve criar uma conexão de máquina virtual de armazenamento (SVM) e uma credencial antes de usar cmdlets do PowerShell para executar operações de proteção de dados.

O que você vai precisar

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

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

- Os nomes do sistema de armazenamento devem ser exclusivos.

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

Passos

1. Inicie uma sessão de conexão do PowerShell usando o cmdlet `Open-SmConnection`.

Este exemplo abre uma sessão do PowerShell:

```
PS C:\> Open-SmConnection
```

2. Crie uma nova conexão com o sistema de armazenamento usando o cmdlet `Add-SmStorageConnection`.

Este exemplo cria uma nova conexão de sistema de armazenamento:

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol https  
-Timeout 60
```

3. Crie uma nova credencial usando o cmdlet `Add-SmCredential`.

Este exemplo cria uma nova credencial chamada `FinanceAdmin` com credenciais do Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

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

Faça backup de recursos usando cmdlets do PowerShell

Você pode usar os cmdlets do PowerShell para fazer backup de bancos de dados do SQL Server ou sistemas de arquivos do Windows. Isso incluiria o backup de um banco de dados do SQL Server ou sistema de arquivos do Windows inclui estabelecer uma conexão com o servidor SnapCenter, descobrir as instâncias de banco de dados do SQL Server ou sistemas de arquivos do Windows, adicionar uma política, criar um grupo de recursos de backup, fazer backup e verificar o backup.

O que você vai precisar

- Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.
- Você deve ter adicionado a conexão do sistema de armazenamento e criado uma credencial.
- Você deve ter adicionado hosts e recursos descobertos.

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o cmdlet `Open-SmConnection`.

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

É apresentado o aviso de nome de utilizador e palavra-passe.

2. Crie uma política de backup usando o cmdlet `Add-SmPolicy`.

Este exemplo cria uma nova política de backup com um tipo de backup SQL de fullbackup:

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy  
-PluginPolicyType SCSQL -PolicyType Backup  
-SqlBackupType FullBackup -Verbose
```

Este exemplo cria uma nova política de backup com um tipo de backup do sistema de arquivos do Windows `CrashConsistent`:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy  
-PluginPolicyType SCW -PolicyType Backup  
-ScwBackupType CrashConsistent -Verbose
```

3. Descubra os recursos do host usando o cmdlet `Get-SmResources`.

Este exemplo descobre os recursos do plug-in Microsoft SQL no host especificado:

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

Este exemplo descobre os recursos para sistemas de arquivos do Windows no host especificado:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Adicione um novo grupo de recursos ao SnapCenter usando o cmdlet Add-SmResourceGroup.

Este exemplo cria um novo grupo de recursos de backup de banco de dados SQL com a política e os recursos especificados:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

Este exemplo cria um novo grupo de recursos de backup do sistema de arquivos do Windows com a política e os recursos especificados:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Inicie uma nova tarefa de backup usando o cmdlet New-SmBackup.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Exiba o status da tarefa de backup usando o cmdlet Get-SmBackupReport.

Este exemplo exibe um relatório de resumo de todos os trabalhos executados na data especificada:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

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

Cancele o plug-in do SnapCenter para operações de backup do Microsoft SQL Server

Você pode cancelar operações de backup em execução, na fila ou sem resposta. Quando você cancela uma operação de backup, o servidor SnapCenter interrompe a operação e remove todas as cópias Snapshot do armazenamento se o backup criado não estiver registrado no servidor SnapCenter. Se o backup já estiver registrado no servidor SnapCenter, ele não reverterá a cópia Snapshot já criada mesmo após o cancelamento ser acionado.

O que você vai precisar


- Você deve estar logado como administrador do SnapCenter ou proprietário da tarefa para cancelar as operações de restauração.
- Você pode cancelar apenas as operações de log ou backup completo que estão na fila ou em execução.
- Não é possível cancelar a operação após a verificação ter sido iniciada.

Se cancelar a operação antes da verificação, a operação é cancelada e a operação de verificação não será executada.

- Pode cancelar uma operação de cópia de segurança a partir da página Monitor ou do painel atividade.
- Além de usar a GUI do SnapCenter, você pode usar cmdlets do PowerShell para cancelar operações.
- O botão **Cancelar trabalho** está desativado para operações que não podem ser canceladas.
- Se você selecionou **todos os membros desta função podem ver e operar em objetos de outros membros** na página usuários/grupos ao criar uma função, você pode cancelar as operações de backup em fila de outros membros enquanto usa essa função.

Passo

Execute uma das seguintes ações:

A partir do...	Ação
Página do monitor	<ol style="list-style-type: none">1. No painel de navegação esquerdo, clique em Monitor > trabalhos.2. Selecione o trabalho e clique em Cancelar trabalho.
Painel da atividade	<ol style="list-style-type: none">1. Depois de iniciar o trabalho de cópia de segurança, clique  no painel atividade para ver as cinco operações mais recentes.2. Selecione a operação.3. Na página Detalhes da tarefa, clique em Cancelar tarefa.

Resultado

A operação é cancelada e o recurso é revertido para o estado anterior. Se a operação cancelada não for

responsiva no estado de cancelamento ou execução, você deverá executar `Cancel-SmJob -JobID <int> -Force` o cmdlet para interromper a operação de backup com força.




Veja os backups e clones do SQL Server na página topologia

Ao se preparar para fazer backup ou clonar um recurso, talvez seja útil exibir uma representação gráfica de todos os backups e clones no storage primário e secundário.

Sobre esta tarefa

Na página topologia, você pode ver todos os backups e clones disponíveis para o grupo de recursos ou recursos selecionado. Você pode visualizar os detalhes desses backups e clones e, em seguida, selecioná-los para executar operações de proteção de dados.

Você pode revisar os ícones a seguir na exibição **Gerenciar cópias** para determinar se os backups e clones estão disponíveis no storage primário ou secundário (cópias espelhadas ou cópias do Vault).

-  Exibe o número de backups e clones disponíveis no storage primário.
-  Exibe o número de backups e clones espelhados no storage secundário usando a tecnologia SnapMirror.
-  Exibe o número de backups e clones replicados no storage secundário usando a tecnologia SnapVault.
 - O número de backups exibidos inclui os backups excluídos do armazenamento secundário.

Por exemplo, se você criou backups 6 usando uma política para reter apenas 4 backups, o número de backups exibidos é 6.



Os clones de um backup de um espelhamento flexível de versão em um volume do tipo cofre-espelho são exibidos na visualização de topologia, mas a contagem de backup espelhado na visualização de topologia não inclui o backup flexível de versão.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione o recurso ou o grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso na exibição de detalhes do recurso ou na exibição de detalhes do grupo de recursos.

Se o recurso selecionado for um banco de dados clonado, proteja o banco de dados clonado, a origem do clone será exibida na página topologia. Clique em **Detalhes** para visualizar o backup usado para clonar.

Se o recurso estiver protegido, a página topologia do recurso selecionado é exibida.
4. Revise o cartão de resumo para ver um resumo do número de backups e clones disponíveis no storage primário e secundário.

A seção **cartão de resumo** exibe o número total de backups e clones.

Clicar no botão **Refresh** inicia uma consulta do armazenamento para exibir uma contagem precisa.


5. Na exibição **Gerenciar cópias**, clique em **backups** ou **clones** do armazenamento primário ou secundário para ver detalhes de um backup ou clone.

Os detalhes dos backups e clones são exibidos em um formato de tabela.

6. Selecione o backup na tabela e clique nos ícones de proteção de dados para executar operações de restauração, clonagem, renomeação e exclusão.



Não é possível renomear ou excluir backups que estão no armazenamento secundário.

7. Selecione um clone da tabela e clique em **Clone Split**.
8. Se quiser excluir um clone, selecione-o na tabela e clique  em .

Remova backups usando cmdlets do PowerShell

Você pode usar o cmdlet `Remove-SmBackup` para excluir backups se não precisar mais deles para outras operações de proteção de dados.

Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.

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

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o cmdlet `Open-SmConnection`.

```
Open-SmConnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. Exclua um ou mais backup usando o cmdlet `Remove-SmBackup`.

Este exemplo exclui dois backups usando suas IDs de backup:

```
Remove-SmBackup -BackupIds 3,4
Remove-SmBackup
Are you sure want to remove the backup(s) .
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):
```

Limpe a contagem de backup secundária usando cmdlets do PowerShell

Você pode usar o cmdlet `Remove-SmBackup` para limpar a contagem de backup para

backups secundários que não têm cópias Snapshot. Você pode querer usar este cmdlet quando as cópias Snapshot totais exibidas na topologia Gerenciar cópias não corresponderem à configuração de retenção de cópia Snapshot do storage secundário.

Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.

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

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o cmdlet `Open-SmConnection`.

```
Open-SmConnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. Limpe a contagem de backups secundários usando o parâmetro `-CleanupSecondaryBackups`.

Este exemplo limpa a contagem de backup para backups secundários sem cópias Snapshot:

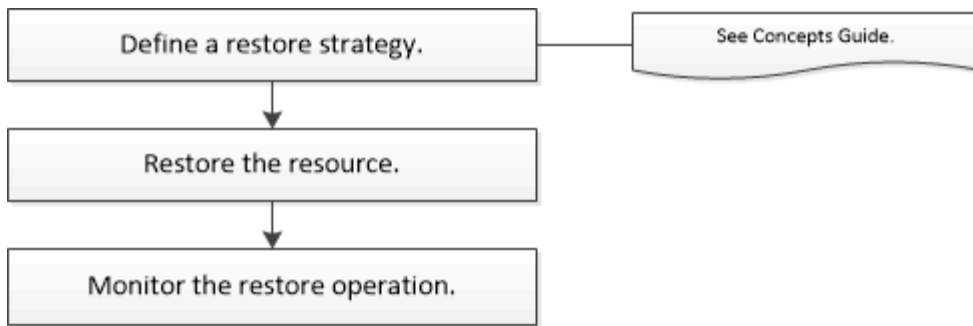
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s) .
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):
```

Restaurar recursos do SQL Server

Restaure o fluxo de trabalho

Você pode usar o SnapCenter para restaurar bancos de dados SQL Server restaurando os dados de um ou mais backups para o seu sistema de arquivos ativo e, em seguida, recuperando o banco de dados. Você também pode restaurar bancos de dados que estão em grupos de disponibilidade e, em seguida, adicionar os bancos de dados restaurados ao Grupo de disponibilidade. Antes de restaurar um banco de dados do SQL Server, você deve executar várias tarefas preparatórias.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar as operações de restauração de banco de dados:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração, recuperação, verificação e clone. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet SnapCenter ou consulte o ["Guia de referência de cmdlet do software SnapCenter 4,4"](#)

Encontre mais informações

["Restaure um banco de dados SQL Server a partir do armazenamento secundário"](#)

["Restaure e recupere recursos usando cmdlets do PowerShell"](#)

["A operação de restauração pode falhar no Windows 2008 R2"](#)

Requisitos para restaurar um banco de dados

Antes de restaurar um banco de dados SQL Server a partir de um plug-in do SnapCenter para backup do Microsoft SQL Server, você deve garantir que vários requisitos sejam atendidos.

- A instância do SQL Server de destino deve estar on-line e em execução antes de poder restaurar um banco de dados.

Isso se aplica às operações de restauração de banco de dados do usuário e às operações de restauração de banco de dados do sistema.

- As operações do SnapCenter que estão agendadas para serem executadas com base nos dados do SQL Server que você está restaurando devem ser desativadas, incluindo quaisquer tarefas agendadas em servidores de gerenciamento remoto ou verificação remota.
- Se os bancos de dados do sistema não estiverem funcionais, você deve primeiro reconstruir os bancos de dados do sistema usando um utilitário SQL Server.
- Se você estiver instalando o plug-in, certifique-se de conceder permissões para outras funções para restaurar os backups do Grupo de disponibilidade (AG).

A restauração de AG falha quando uma das seguintes condições for atendida:

- Se o plug-in for instalado pelo usuário do RBAC e um administrador tentar restaurar um backup AG
- Se o plug-in for instalado por um administrador e um usuário RBAC tentar restaurar um backup AG
- Se você estiver restaurando backups de diretório de log personalizados para um host alternativo, o servidor SnapCenter e o host do plug-in devem ter a mesma versão do SnapCenter instalada.
- Você deve ter instalado o hotfix da Microsoft, KB2887595. O site de suporte da Microsoft contém mais informações sobre o KB2887595.

["Artigo de suporte da Microsoft 2887595: Pacote cumulativo de atualizações do Windows RT 8,1, Windows 8,1 e Windows Server 2012 R2: Novembro de 2013"](#)

- Você deve ter feito backup dos grupos de recursos ou banco de dados.
- Se você estiver replicando cópias Snapshot em um espelhamento ou cofre, o administrador do SnapCenter deverá ter atribuído a você as máquinas virtuais de storage (SVMs) para os volumes de origem e de destino.

Para obter informações sobre como os administradores atribuem recursos aos usuários, consulte as informações de instalação do SnapCenter.

- Todos os trabalhos de cópia de segurança e clone têm de ser interrompidos antes de restaurar a base de dados.
- A operação de restauração pode ter tempo limite se o tamanho do banco de dados estiver em terabytes (TB).

Você deve aumentar o valor do parâmetro RESTTimeout do servidor SnapCenter para 20000000 ms executando o seguinte comando: `Set-SmConfigSettings -Agent -configSettings [20000000]`. De acordo com o tamanho do banco de dados, o valor de tempo limite pode ser alterado e o valor máximo que você pode definir é de 86400000 ms.

Se você quiser restaurar enquanto os bancos de dados estiverem on-line, a opção de restauração on-line deve estar habilitada na página Restaurar.

Restaure backups de banco de dados do SQL Server

Você pode usar o SnapCenter para restaurar bancos de dados do SQL Server com backup. Restauração de banco de dados é um processo multifásico que copia todos os dados e páginas de log de um backup especificado do SQL Server para um banco de dados especificado.

Sobre esta tarefa

- Você pode restaurar os bancos de dados do SQL Server com backup para uma instância diferente do SQL Server no mesmo host onde o backup foi criado.

Você pode usar o SnapCenter para restaurar os bancos de dados do SQL Server com backup para um caminho alternativo, de modo que você não substitua uma versão de produção.

- O SnapCenter pode restaurar bancos de dados em um cluster do Windows sem colocar o grupo de cluster do SQL Server offline.
- Se ocorrer uma falha de cluster (uma operação de movimentação de grupo de cluster) durante uma operação de restauração (por exemplo, se o nó que possui os recursos for desativado), você deverá se reconectar à instância do SQL Server e reiniciar a operação de restauração.
- Não é possível restaurar o banco de dados quando os usuários ou as tarefas do SQL Server Agent estão acessando o banco de dados.
- Não é possível restaurar os bancos de dados do sistema para um caminho alternativo.
- O `SCRIPT_PATH` é definido usando a chave `PredefinedWindowsScriptsDirectory` localizada no arquivo `SMCoreServiceHost.exe.Config` do host do plug-in.

Se necessário, você pode alterar esse caminho e reiniciar o serviço `SMcore`. É recomendável usar o

caminho padrão para segurança.

O valor da chave pode ser exibido do swagger através da API: API /4,7/configsettings


Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.

- A maioria dos campos nas páginas do assistente Restaurar são auto-explicativos. As informações a seguir descrevem os campos para os quais você pode precisar de orientação.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione a base de dados ou o grupo de recursos na lista.

A página de topologia é exibida.


4. No modo de exibição Gerenciar cópias, selecione **backups** no sistema de armazenamento.
5. Selecione a cópia de segurança na tabela e, em seguida, clique no  ícone.



Backup Name	End Date
rg1_scipr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM


6. Na página Restaurar escopo, selecione uma das seguintes opções:

Opção	Descrição
Restaure o banco de dados para o mesmo host onde o backup foi criado	Selecione esta opção se quiser restaurar o banco de dados para o mesmo servidor SQL em que os backups são feitos.

Opção	Descrição
Restaurar o banco de dados para um host alternativo	<p>Selecione esta opção se quiser que o banco de dados seja restaurado para um servidor SQL diferente no mesmo ou em um host diferente no qual os backups são feitos.</p> <p>Selecione um nome de host, forneça um nome de banco de dados (opcional), selecione uma instância e especifique os caminhos de restauração.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p>A extensão de arquivo fornecida no caminho alternativo deve ser igual à extensão de arquivo do arquivo de banco de dados original.</p> </div> <p>Se a opção Restaurar o banco de dados para um host alternativo não for exibida na página Restaurar escopo, limpe o cache do navegador.</p>
Restaurar o banco de dados usando arquivos de banco de dados existentes	<p>Selecione esta opção se quiser que o banco de dados seja restaurado para um SQL Server alternativo no mesmo host ou diferente em que os backups são feitos.</p> <p>Os arquivos de banco de dados já devem estar presentes nos caminhos de arquivo existentes fornecidos. Selecione um nome de host, forneça um nome de banco de dados (opcional), selecione uma instância e especifique os caminhos de restauração.</p>

7. Na página âmbito de recuperação, selecione uma das seguintes opções:

Opção	Descrição
Nenhum	Selecione nenhum quando precisar restaurar somente o backup completo sem nenhum log.
Todos os backups de log	Selecione todos os backups de log operação de restauração de backup atualizada para restaurar todos os backups de log disponíveis após o backup completo.
Por backup de log até	Selecione por backups de log para executar uma operação de restauração pontual, que restaura o banco de dados com base em logs de backup até o log de backup com a data selecionada.

Opção	Descrição
Por data específica até	<p>Selecione por data específica até para especificar a data e a hora após as quais os logs de transação não são aplicados ao banco de dados restaurado.</p> <p>Esta operação de restauração pontual interrompe a restauração de entradas de log de transações que foram registradas após a data e hora especificadas.</p>
Use o diretório de log personalizado	<p>Se tiver selecionado todos os backups de log, por backups de log ou por data específica até e os logs estiverem localizados em um local personalizado, selecione usar diretório de log personalizado e especifique o local do log.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>O diretório de log personalizado não é suportado para o banco de dados do grupo de disponibilidade.</p> </div>

8. Na página Pré-operações, execute as seguintes etapas:

a. Na página Opções de pré restauração, selecione uma das seguintes opções:

- Selecione **Substituir o banco de dados com o mesmo nome durante a restauração** para restaurar o banco de dados com o mesmo nome.
- Selecione **reter configurações de replicação do banco de dados SQL** para restaurar o banco de dados e manter as configurações de replicação existentes.
- Selecione **criar backup de log de transações antes de restaurar** para criar um log de transações antes do início da operação de restauração.
- Selecione **Sair da restauração se o backup do log de transações antes da restauração falhar** para cancelar a operação de restauração se o backup do log de transações falhar.

b. Especifique scripts opcionais a serem executados antes de executar um trabalho de restauração.

Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas, enviar logs e assim por diante.



O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.

9. Na página Pós-operações, execute as seguintes etapas:

a. Na seção escolher estado do banco de dados após a conclusão da restauração, selecione uma das seguintes opções:

- Selecione **operacional, mas indisponível para restaurar logs de transação adicionais** se você estiver restaurando todos os backups necessários agora.

Esse é o comportamento padrão, que deixa o banco de dados pronto para uso, revertendo as transações não confirmadas. Não é possível restaurar registros de transações adicionais até criar uma cópia de segurança.

- Selecione **não operacional, mas disponível para restaurar logs transacionais adicionais** para deixar o banco de dados não operacional sem reverter as transações não comprometidas.

Logs de transação adicionais podem ser restaurados. Você não pode usar o banco de dados até que ele seja recuperado.

- Selecione **modo somente leitura, disponível para restaurar logs transacionais adicionais** para deixar o banco de dados no modo somente leitura.

Essa opção desfaz transações não confirmadas, mas salva as ações desfeitas em um arquivo de espera para que os efeitos de recuperação possam ser revertidos.

Se a opção Desfazer diretório estiver ativada, mais logs de transações serão restaurados. Se a operação de restauração do log de transações não for bem-sucedida, as alterações podem ser revertidas. A documentação do SQL Server contém mais informações.

- b. Especifique scripts opcionais a serem executados após a execução de um trabalho de restauração.

Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas, enviar logs e assim por diante.



O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.

10. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail.

11. Revise o resumo e clique em **Finish**.
12. Monitorize o processo de restauro utilizando a página **Monitor > trabalhos**.

Encontre mais informações

["Restaure e recupere recursos usando cmdlets do PowerShell"](#)

["Restaure um banco de dados SQL Server a partir do armazenamento secundário"](#)

Restaure um banco de dados SQL Server a partir do armazenamento secundário

É possível restaurar os bancos de dados SQL Server com backup dos LUNs físicos (RDM, iSCSI ou FCP) em um sistema de storage secundário. O recurso Restaurar é um processo multifásico que copia todos os dados e as páginas de log de um backup especificado do SQL Server residente no sistema de storage secundário para um banco de dados especificado.

O que você vai precisar


- Você precisa ter replicado as cópias Snapshot do sistema de storage primário para o secundário.
- Você deve garantir que o servidor SnapCenter e o host do plug-in possam se conectar ao sistema de storage secundário.

- A maioria dos campos nas páginas do assistente de restauração são explicados no processo de restauração básico. As informações a seguir descrevem alguns dos campos para os quais você pode precisar de orientação.

Passos

1. No painel de navegação à esquerda, clique em **Resources** e selecione **SnapCenter Plug-in para SQL Server** na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista suspensa **Exibir**.
3. Selecione o banco de dados ou o grupo de recursos.

A página de topologia do banco de dados ou do grupo de recursos é exibida.

4. Na seção Gerenciar cópias, selecione **backups** no sistema de armazenamento secundário (espelhado ou Vault).
5. Selecione a cópia de segurança na lista e clique  em .
6. Na página localização, escolha o volume de destino para restaurar o recurso selecionado.
7. Conclua o assistente de restauração, revise o resumo e clique em **Finish**.

Se você restaurou um banco de dados para um caminho diferente que é compartilhado por outros bancos de dados, você deve executar uma verificação completa de backup e backup para confirmar que seu banco de dados restaurado está livre de corrupção no nível físico.

Reseed Availability Group Databases

Reseed é uma opção para restaurar bancos de dados do Availability Group (AG). Se um banco de dados secundário ficar fora de sincronização com o banco de dados primário em um AG, você poderá fazer a semente novamente do banco de dados secundário.

O que você vai precisar

- Você deve ter criado o backup do banco de dados AG secundário que você deseja restaurar.
- O servidor SnapCenter e o host do plug-in devem ter a mesma versão do SnapCenter instalada.

Sobre esta tarefa

- Não é possível executar a operação de semente em bancos de dados primários.
- Não é possível executar uma operação de semente novamente se o banco de dados de réplica for removido do grupo de disponibilidade. Quando a réplica é removida, a operação de reseed falha.
- Ao executar a operação de reseed no banco de dados SQL Availability Group, você não deve acionar backups de log nos bancos de dados de réplica desse banco de dados de grupo de disponibilidade. Se você acionar backups de log durante a operação de reseed, a operação de reseed falha com o banco de dados espelhado, "database_name" tem dados de log de transação insuficientes para preservar a cadeia de backup de log da mensagem de erro principal do banco de dados.

Passos

1. No painel de navegação à esquerda, clique em **Resources** e selecione **SnapCenter Plug-in para SQL Server** na lista.

2. Na página recursos, selecione **Banco de dados** na lista **Exibir**.
3. Selecione a base de dados AG secundária na lista.
4. Clique em **Reseed**.
5. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

Restaure recursos usando cmdlets do PowerShell

A restauração de um backup de recurso inclui iniciar uma sessão de conexão com o servidor SnapCenter, listar os backups e recuperar informações de backup e restaurar um backup.

Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o cmdlet `Open-SmConnection`.

```
Open-smconnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando os cmdlets `Get-SmBackup` e `Get-SmBackupReport`.

Este exemplo exibe informações sobre todos os backups disponíveis:

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM

Este exemplo exibe informações detalhadas sobre o backup de 29th 2015 de janeiro a 3rd de fevereiro de 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId         : 2032
StartDateTime   : 2/2/2015 6:57:03 AM
EndDateTime     : 2/2/2015 6:57:11 AM
Duration        : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName      : Vault
SmPolicyId      : 18
BackupName      : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId         : 2183
StartDateTime   : 2/2/2015 1:02:41 PM
EndDateTime     : 2/2/2015 1:02:38 PM
Duration        : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName      : Vault
SmPolicyId      : 18
BackupName      : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restaure dados do backup usando o cmdlet Restore-SmBackup.


```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :

```

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







Monitorar operações de restauração de recursos SQL

Pode monitorizar o progresso de diferentes operações de restauro do SnapCenter utilizando a página trabalhos. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um problema.


Sobre esta tarefa

os estados pós-restauração descrevem as condições do recurso após uma operação de restauração e quaisquer outras ações de restauração que você possa executar.

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:


-  Em curso
-  Concluído com êxito
-  Falha
-  Preenchido com avisos ou não foi possível iniciar devido a avisos
-  Em fila de espera
-  Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **trabalhos**.
3. Na página trabalhos, execute as seguintes etapas:
 - a. Clique  para filtrar a lista de modo que apenas as operações de restauração sejam listadas.
 - b. Especifique as datas de início e fim.
 - c. Na lista suspensa **Type**, selecione **Restore**.
 - d. Na lista suspensa **Status**, selecione o status de restauração.
 - e. Clique em **Apply** para ver as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para exibir os detalhes do trabalho.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

O botão **View logs** exibe os logs detalhados para a operação selecionada.



Após a operação de restauração baseada em volume, os metadados do backup são excluídos do repositório do SnapCenter, mas as entradas do catálogo de backup permanecem no catálogo do SAP HANA. Embora o status do trabalho de restauração seja exibido , você deve clicar nos detalhes do trabalho para ver o sinal de aviso de algumas das tarefas secundárias. Clique no sinal de aviso e elimine as entradas do catálogo de cópias de segurança indicadas.

Cancelar operações de restauração de recursos SQL

Você pode cancelar trabalhos de restauração que estão na fila.

Você deve estar logado como administrador do SnapCenter ou proprietário da tarefa para cancelar as operações de restauração.

Sobre esta tarefa

- Você pode cancelar uma operação de restauração em fila na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de restauração em execução.
- Você pode usar a GUI do SnapCenter, cmdlets do PowerShell ou os comandos CLI para cancelar as operações de restauração em fila.
- O botão **Cancelar trabalho** está desativado para operações de restauração que não podem ser canceladas.

- Se você selecionou **todos os membros desta função podem ver e operar em outros objetos membros** na página usuários/grupos ao criar uma função, você pode cancelar as operações de restauração em fila de outros membros enquanto usa essa função.

Passo

Execute uma das seguintes ações:

A partir do...	Ação
Página do monitor	<ol style="list-style-type: none"> 1. No painel de navegação esquerdo, clique em Monitor > trabalhos. 2. Selecione o trabalho e clique em Cancelar trabalho.
Painel da atividade	<ol style="list-style-type: none"> 1. Depois de iniciar a operação de restauração, clique  no painel atividade para exibir as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes da tarefa, clique em Cancelar tarefa.

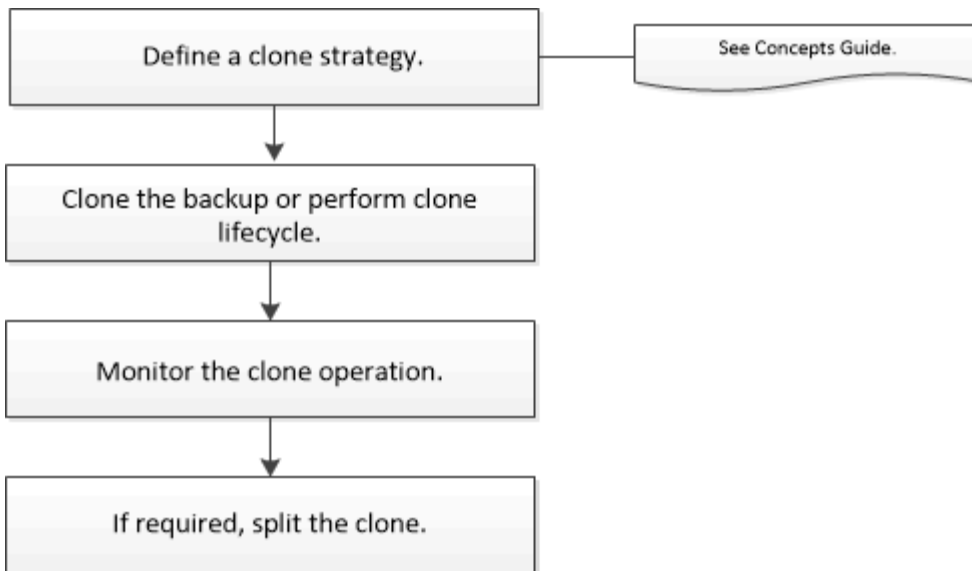
Clonar recursos de banco de dados do SQL Server

Fluxo de trabalho clone

É necessário executar várias tarefas usando o servidor SnapCenter antes de clonar os recursos do banco de dados a partir de um backup. Clonagem de banco de dados é o processo de criação de uma cópia pontual de um banco de dados de produção ou de seu conjunto de backup. Você pode clonar bancos de dados para testar a funcionalidade que precisa ser implementada usando a estrutura e o conteúdo atuais do banco de dados durante os ciclos de desenvolvimento de aplicativos, para usar as ferramentas de extração e manipulação de dados ao preencher data warehouses ou para recuperar dados que foram excluídos ou alterados erroneamente.

Uma operação de clonagem de banco de dados gera relatórios com base nas IDs de tarefa.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar as operações de clonagem:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração, recuperação, verificação e clone. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet SnapCenter ou consulte o. ["Guia de referência de cmdlet do software SnapCenter"](#)

Encontre mais informações

["Clone de um backup de banco de dados do SQL Server"](#)

["Execute o ciclo de vida do clone"](#)

["A operação de clone pode falhar ou levar mais tempo para ser concluída com o valor padrão TCP_TIMEOUT"](#)

Clone de um backup de banco de dados do SQL Server

Você pode usar o SnapCenter para clonar um backup de banco de dados do SQL Server. Se quiser acessar ou restaurar uma versão mais antiga dos dados, você pode clonar backups de bancos de dados sob demanda.

O que você vai precisar

- Você deve se preparar para a proteção de dados concluindo tarefas como adicionar hosts, identificar recursos e criar conexões do sistema de storage.
- Você deve ter feito backup de bancos de dados ou grupos de recursos.
- O tipo de proteção, como espelho, cofre ou espelho-Vault para LUN de dados e LUN de log, deve ser o mesmo para descobrir localizadores secundários durante a clonagem para um host alternativo usando backups de log.
- Se a unidade de clone montada não puder ser encontrada durante uma operação de clone do SnapCenter, você deve alterar o parâmetro CloneRetryTimeout do servidor SnapCenter para 300.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de storage (SVM).

Sobre esta tarefa

- Durante a clonagem para uma instância de banco de dados autônoma, verifique se o caminho do ponto de montagem existe e se ele é um disco dedicado.
- Durante a clonagem para uma instância de cluster de failover (FCI), certifique-se de que os pontos de montagem existem, é um disco compartilhado e o caminho e o FCI devem pertencer ao mesmo grupo de recursos SQL.
- Verifique se há apenas um iniciador VFC ou FC conectado a cada host. Isso ocorre porque o SnapCenter suporta apenas um iniciador por host.
- Se o banco de dados de origem ou a instância de destino estiver em um volume compartilhado de cluster (csv), o banco de dados clonado estará no csv.
- O SCRIPT_PATH é definido usando a chave PredefinedWindowsScriptsDirectory localizada no arquivo SMCoreServiceHost.exe.Config do host do plug-in.

Se necessário, você pode alterar esse caminho e reiniciar o serviço SMcore. É recomendável usar o caminho padrão para segurança.

O valor da chave pode ser exibido do swagger através da API: API /4,7/configsettings

Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.



Para ambientes virtuais (VMDK/RDM), verifique se o ponto de montagem é um disco dedicado.


Passos

1. No painel de navegação à esquerda, clique em **Resources** e selecione **SnapCenter Plug-in para SQL Server** na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.



A clonagem de um backup de uma instância não é suportada.

Passos

1. Selecione o banco de dados ou o grupo de recursos.
2. Na página de exibição Gerenciar cópias, selecione o backup no sistema de storage primário ou secundário (espelhado ou abobadado).
3. Selecione a cópia de segurança e, em seguida, clique em  *.
4. Na página Opções de clones, execute as seguintes ações:

Para este campo...	Faça isso...
Servidor clone	Escolha um host no qual o clone deve ser criado.
Instância de clone	Escolha uma instância clone para a qual você deseja clonar o backup do banco de dados. Essa instância SQL deve estar localizada no servidor clone especificado.

Para este campo...	Faça isso...
Sufixo clone	<p>Insira um sufixo que será anexado ao nome do arquivo clone para identificar que o banco de dados é um clone.</p> <p>Por exemplo, <i>db1_clone</i>. Se você estiver clonando para o mesmo local do banco de dados original, forneça um sufixo para diferenciar o banco de dados clonado do banco de dados original. Caso contrário, a operação falha.</p>
Atribuir automaticamente o ponto de montagem ou atribuir automaticamente o ponto de montagem do volume sob o caminho	<p>Escolha se deseja atribuir automaticamente um ponto de montagem ou um ponto de montagem de volume sob um caminho.</p> <p>Atribuir automaticamente ponto de montagem de volume sob caminho: O ponto de montagem sob um caminho permite que você forneça um diretório específico. Os pontos de montagem serão criados dentro desse diretório. Antes de escolher essa opção, você deve garantir que o diretório esteja vazio. Se houver um banco de dados no diretório, o banco de dados estará em um estado inválido após a operação de montagem.</p>

5. Na página Logs, selecione uma das seguintes opções:

Para este campo...	Faça isso...
Nenhum	Escolha esta opção quando quiser clonar apenas o backup completo sem quaisquer logs.
Todos os backups de log	Escolha esta opção para clonar todos os backups de log disponíveis datados após o backup completo.
Por backup de log até	Escolha esta opção para clonar o banco de dados com base nos logs de backup que foram criados até o log de backup com a data selecionada.
Por data específica até	<p>Especifique a data e a hora após as quais os logs de transação não são aplicados ao banco de dados clonado.</p> <p>Esse clone pontual interrompe o clone das entradas do log de transações que foram registradas após a data e hora especificadas.</p>

6. Na página Script, insira o tempo limite do script, o caminho e os argumentos do prescript ou postscript que devem ser executados antes ou depois da operação clone, respectivamente.

Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas, enviar logs e assim por diante.



O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.

O tempo limite padrão do script é de 60 segundos.

7. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. Se quiser anexar o relatório da operação clone executada, selecione **Anexar Relatório de trabalho**.



Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando PowerShell SET-SmtpServer.

Para EMS, pode consultar "[Gerir a recolha de dados EMS](#)"

8. Revise o resumo e clique em **Finish**.
9. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

Depois de terminar

Depois que o clone é criado, você nunca deve renomeá-lo.

Encontre mais informações

["Faça backup do banco de dados do SQL Server, instância ou grupo de disponibilidade"](#)

["Clonar backups usando cmdlets do PowerShell"](#)

["A operação de clone pode falhar ou levar mais tempo para ser concluída com o valor padrão TCP_TIMEOUT"](#)

["O clone do banco de dados de instância do cluster de failover falha"](#)

Clonar backups usando cmdlets do PowerShell

O fluxo de trabalho do clone inclui Planejamento, execução da operação do clone e monitoramento da operação.

Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. Liste os backups que podem ser clonados usando o cmdlet Get-SmBackup ou Get-SmResourceGroup.

Este exemplo exibe informações sobre todos os backups disponíveis:

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

Este exemplo exibe informações sobre um grupo de recursos especificado, seus recursos e políticas associadas:

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

```
Description :  
CreationTime : 8/4/2015 3:44:05 PM  
ModificationTime : 8/4/2015 3:44:05 PM  
EnableEmail : False  
EmailSMTPServer :  
EmailFrom :  
EmailTo :  
EmailSubject :  
EnableSysLog : False  
ProtectionGroupType : Backup  
EnableAsupOnFailure : False  
Policies : {FinancePolicy}  
HostResourceMapping : {}  
Configuration : SMCOREContracts.SmCloneConfiguration  
LastBackupStatus :  
VerificationServer :  
EmailBody :  
EmailNotificationPreference : Never  
VerificationServerInfo : SMCOREContracts.SmVerificationServerInfo  
SchedulerSQLInstance :  
CustomText :  
CustomSnapshotFormat :  
SearchResources : False  
ByPassCredential : False  
IsCustomSnapshot :  
MaintenanceStatus : Production  
PluginProtectionGroupTypes : {SMSQL}  
Name : Payrolldataset
```



```
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeout : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
```

```

SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCOREContracts.SmAuth
IsClone : False

```

3. Inicie uma operação de clone a partir de um backup existente usando o cmdlet New-SmClone.

Este exemplo cria um clone a partir de um backup especificado com todos os logs:

```

PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy

```

Este exemplo cria um clone para uma instância especificada do Microsoft SQL Server:

```

PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"

```

4. Exiba o status da tarefa clone usando o cmdlet Get-SmCloneReport.

Este exemplo exibe um relatório de clone para a ID de tarefa especificada:

```

PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper_clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}

```

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

Execute o ciclo de vida do clone

Com o SnapCenter, você pode criar clones de um grupo de recursos ou banco de dados. Você pode executar um clone sob demanda ou agendar operações de clone recorrentes de um grupo de recursos ou banco de dados. Se você clonar um backup periodicamente, poderá usar o clone para desenvolver aplicativos, preencher dados ou recuperar dados.

O SnapCenter permite que você programe várias operações de clone para serem executadas simultaneamente em vários servidores.

O que você vai precisar

- Durante a clonagem para uma instância de banco de dados autônoma, verifique se o caminho do ponto de montagem existe e se ele é um disco dedicado.
- Durante a clonagem para uma instância de cluster de failover (FCI), certifique-se de que os pontos de montagem existem, é um disco compartilhado e o caminho e o FCI devem pertencer ao mesmo grupo de recursos SQL.
- Se o banco de dados de origem ou a instância de destino estiver em um volume compartilhado de cluster (csv), o banco de dados clonado estará no csv.



Para ambientes virtuais (VMDK/RDM), verifique se o ponto de montagem é um disco dedicado.

Sobre esta tarefa

- O SCRIPT_PATH é definido usando a chave PredefinedWindowsScriptsDirectory localizada no arquivo SMCoreServiceHost.exe.Config do host do plug-in.

Se necessário, você pode alterar esse caminho e reiniciar o serviço SMcore. É recomendável usar o caminho padrão para segurança.

O valor da chave pode ser exibido do swagger através da API: API /4,7/configsettings

Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.

- A maioria dos campos nas páginas do assistente Clone Lifecycle são auto-explicativos. As informações a seguir descrevem os campos para os quais você pode precisar de orientação.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o grupo de recursos ou banco de dados e clique em **Clone Lifecycle**.
4. Na página Opções, execute as seguintes ações:

Para este campo...	Faça isso...
Clone o nome da tarefa	Especifique o nome da tarefa do ciclo de vida do clone que ajuda a monitorar e modificar a tarefa do ciclo de vida do clone.
Servidor clone	Escolha o host no qual o clone deve ser colocado.
Instância de clone	Escolha a instância clone para a qual você deseja clonar o banco de dados. Essa instância SQL deve estar localizada no servidor clone especificado.
Sufixo clone	Digite um sufixo que será anexado ao banco de dados clone para identificar que é um clone. Cada instância SQL usada para criar um grupo de recursos clone deve ter um nome de banco de dados exclusivo. Por exemplo, se o grupo de recursos clone contiver um banco de dados de origem "d.B1" de uma instância SQL "inst1" e se "d.B1" for clonado para "inst1", então o nome do banco de dados clone deve ser "d.B1clone". "clone" é um sufixo obrigatório definido pelo usuário porque o banco de dados é clonado para a mesma instância. Se "d.B1" for clonado para a instância SQL "inst2", então o nome do banco de dados clone pode permanecer "d.B1" (o sufixo é opcional) porque o banco de dados é clonado para uma instância diferente.

Para este campo...	Faça isso...
Atribuir automaticamente o ponto de montagem ou atribuir automaticamente o ponto de montagem do volume sob o caminho	Escolha se deseja atribuir automaticamente um ponto de montagem ou um ponto de montagem de volume sob um caminho. Escolher atribuir automaticamente um ponto de montagem de volume sob um caminho permite fornecer um diretório específico. Os pontos de montagem serão criados dentro desse diretório. Antes de escolher essa opção, você deve garantir que o diretório esteja vazio. Se houver um banco de dados no diretório, o banco de dados estará em um estado inválido após a operação de montagem.

- Na página local, selecione um local de armazenamento para criar um clone.
- Na página Script, insira o caminho e os argumentos do prescriitor ou postscript que devem ser executados antes ou depois da operação clone, respetivamente.

Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas, enviar logs e assim por diante.



O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.

O tempo limite padrão do script é de 60 segundos.

- Na página Agendar, execute uma das seguintes ações:
 - Selecione **Executar agora** se quiser executar a tarefa clone imediatamente.
 - Selecione **Configurar agendamento** quando quiser determinar com que frequência a operação de clone deve ocorrer, quando a programação de clones deve ser iniciada, em que dia a operação de clone deve ocorrer, quando a programação deve expirar e se os clones devem ser excluídos após a expiração da programação.
- Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. Se quiser anexar o relatório da operação clone executada, selecione **Anexar Relatório de trabalho**.



Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando PowerShell SET-SmtpServer.

Para EMS, pode consultar "[Gerir a recolha de dados EMS](#)"

- Revise o resumo e clique em **Finish**.

Deve monitorizar o processo de clonagem utilizando a página **Monitor > trabalhos**.







Monitorar operações de clone de banco de dados SQL

Você pode monitorar o andamento das operações de clone do SnapCenter usando a


página tarefas. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

-  Em curso
-  Concluído com êxito
-  Falha
-  Preenchido com avisos ou não foi possível iniciar devido a avisos
-  Em fila de espera
-  Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **trabalhos**.
3. Na página trabalhos, execute as seguintes etapas:
 - a. Clique  para filtrar a lista para que apenas operações de clone sejam listadas.
 - b. Especifique as datas de início e fim.
 - c. Na lista suspensa **Type**, selecione **Clone**.
 - d. Na lista suspensa **Status**, selecione o status do clone.
 - e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione a tarefa clone e clique em **Detalhes** para exibir os detalhes da tarefa.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Cancelar operações de clone de recursos SQL

Você pode cancelar as operações de clone que estão na fila.


Você deve estar logado como administrador do SnapCenter ou proprietário da tarefa para cancelar operações de clone.

Sobre esta tarefa

- Você pode cancelar uma operação de clone na fila a partir da página **Monitor** ou do painel **atividade**.
- Não é possível cancelar uma operação de clone em execução.
- Você pode usar a GUI do SnapCenter, cmdlets do PowerShell ou os comandos CLI para cancelar as operações de clone na fila.
- Se você selecionou **todos os membros desta função podem ver e operar em outros objetos membros** na página usuários/grupos enquanto cria uma função, você pode cancelar as operações de clone em fila de outros membros enquanto usa essa função.

Passo

Execute uma das seguintes ações:

A partir do...	Ação
Página do monitor	<ol style="list-style-type: none">1. No painel de navegação esquerdo, clique em Monitor > trabalhos.2. Selecione a operação e clique em Cancelar trabalho.
Painel da atividade	<ol style="list-style-type: none">1. Depois de iniciar a operação clone, clique  no painel atividade para exibir as cinco operações mais recentes.2. Selecione a operação.3. Na página Detalhes da tarefa, clique em Cancelar tarefa.

Divida um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido torna-se independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clones em um clone intermediário.

Por exemplo, depois de criar clone1 a partir de um backup de banco de dados, você pode criar um backup de clone1 e clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e não é possível executar a operação de divisão de clones no clone1. No entanto, você pode executar a operação de divisão de clones no clone2.

Depois de dividir clone2, você pode executar a operação de divisão de clones no clone1 porque clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e as tarefas de clone do clone são excluídas.
- Para obter informações sobre limitações de operação de divisão de clones, "[Guia de gerenciamento de storage lógico do ONTAP 9](#)" consulte .
- Certifique-se de que o volume ou o agregado no sistema de storage esteja on-line.


Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicativos de banco de dados	Selecione Banco de dados na lista Exibir.
Para sistemas de arquivos	Selecione caminho na lista Exibir.

3. Selecione o recurso apropriado na lista.

A página de topologia do recurso é exibida.

4. No modo de exibição Gerenciar cópias, selecione o recurso clonado (por exemplo, o banco de dados ou LUN) e clique em .
5. Revise o tamanho estimado do clone que deve ser dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

A operação de divisão de clones deixa de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clones e tentar novamente a operação de divisão de clones.

Se você quiser um tempo de enquete mais longo ou menor para verificar se o clone está dividido ou não, você pode alterar o valor do parâmetro *CloneSplitStatusCheckPollTime* no arquivo *SMCoreServiceHost.exe.config* para definir o intervalo de tempo para que o SMCore busque o status da operação de divisão de clones. O valor é em milissegundos e o valor padrão é de 5 minutos.

Por exemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

A operação de inicialização dividida de clone falhará se o backup, a restauração ou outra divisão de clones estiver em andamento. Você deve reiniciar a operação de divisão de clones somente depois que as operações em execução estiverem concluídas.

Encontre mais informações

["O clone ou a verificação do SnapCenter falha com o agregado não existe"](#)

Informações sobre direitos autorais

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

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

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

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

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

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

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

Informações sobre marcas comerciais

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